МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

# ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Приложение

№14 Сентябрь 2021

Зарегистрирован в Федеральной службе по надзору
в сфере связи и массовых коммуникаций

Свидетельство о регистрации ПИ № ФС 77-50702 от 17 июля 2012 г.

**ТРУДЫ**
**XX Международной конференции**
**«Сибирская научная школа-семинар**
**“Компьютерная безопасность и криптография” — SIBECRYPT’21»**
**имени Г. П. Агибалова**
**(Новосибирск, 6—11 сентября 2021 г.)**

**УЧРЕДИТЕЛЬ**
**Томский государственный университет**



**Адрес редакции:** 634050, г. Томск, пр. Ленина, 36
**E-mail:** pank@mail.tsu.ru

XX Международная конференция «Сибирская научная школа-семинар “Компьютерная безопасность и криптография” — SIBECRYPT’21» имени Г. П. Агибалова проведена Новосибирским государственным университетом и Международным математическим центром в Академгородке в сотрудничестве с Национальным исследовательским Томским государственным университетом и Академией криптографии РФ с 6 по 11 сентября 2021 г. в Новосибирске при финансовой поддержке Международного математического центра в Академгородке (соглашение с Министерством науки и высшего образования РФ № 075-15-2019-1613).

**Теоретические основы прикладной дискретной математики**
**Дискретные функции**
**Математические методы криптографии**
**Математические основы компьютерной безопасности**
**Прикладная теория кодирования и графов**
**Математические основы информатики и программирования**
**Вычислительные методы в дискретной математике**

Редактор Н. И. Шидловская
Верстка И. А. Панкратовой

Подписано к печати 12.08.2021. Формат 60 x 84₈. Усл. п. л. 24,25. Тираж 300 экз.
Заказ № 4749. Цена свободная. Дата выхода в свет 19.08.2021.

Отпечатано на оборудовании
Издательства Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел.: 8(3822)53-15-28, 52-98-49

СОДЕРЖАНИЕ

**ВОСПОМИНАНИЯ КОЛЛЕГ И УЧЕНИКОВ О ГЕННАДИИ ПЕТРОВИЧЕ АГИБАЛОВЕ** 6

Секция 1

**ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ**

**Болтнев Ю. Ф., Новоселов С. А., Осипов В. А.** О построении максимальных гиперэллиптических кривых рода 3 . . . . . 24

**Меженная Н. М., Михайлов В. Г.** Центральная предельная теорема для U -статистик от цепочек меток вершин на полном графе ..... 30

**Фомичёв В. М.** О наибольшем порядке подстановок заданной степени ..... 32

Секция 2

**ДИСКРЕТНЫЕ ФУНКЦИИ**

**Атутова Н. Д.** Гибридный подход к поиску булевых функций с высокой алгебраической иммунностью на основе эвристических методов ..... 37

**Зюбина Д. А., Токарева Н. Н.** S-блоки с максимальной компонентной алгебраической иммунностью от малого числа переменных ..... 40

**Куценко А. В.** О некоторых свойствах самодуальных обобщённых бент-функций ..... 42

**Муха Н., Коломеец Н. А., Ахтямов Д. А., Сутормин И. А., Панферов М. А., Титова К. М., Бонич Т. А., Ищукова Е. А., Токарева Н. Н., Жантуликов Б. Ф.** О свойствах разностных характеристик XOR по модулю $2^n$ . . . . . 46

**Панков К. Н.** Улучшенные оценки для числа k-эластичных и корреляционноиммунных двоичных отображений ..... 48

**Фомин Д. Б.** О способе построения дифференциально 25-равномерных подстановок на $F_{2^{2m}}$ 51

**Черемушкин А. В.** Условие однозначности разложения в произведение функций p-значной логики при линейной замене переменных ..... 55

**Шапоренко А. С.** О производных булевых бент-функций ..... 57

Секция 3

**МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ**

**Агиевич С. В.** XS-схемы: скрытие тактовых оракулов..... 59

**Бахарев А. О.** Разработка и анализ оракула для гибридной атаки на криптографическую систему NTRU с использованием алгоритма квантового поиска ..... 62

**Бердникова Н. Ю., Панкратова И. А.** Криптоаналитическая обратимость функций двух аргументов..... 67

**Бобровский Д. А., Задорожный Д. И., Коренева А. М., Набиев Т. Р., Фомичёв В. М.** Экспериментальное исследование характеристик одного способа контроля целостности при хранении данных большого объёма ..... 71

**Бобровский Д. А., Набиев Т. Р., Фомичёв В. М.** Об алгоритме дополнения блоков большого размера в системах контроля целостности ..... 74

**Колегов Д. Н., Халниязова Ю. Р.** Пороговая схема протокола Диффи — Хеллмана 79

**Колегов Д. Н., Халниязова Ю. Р.** Использование российских криптографических алгоритмов в протоколе безопасности сетевого уровня WireGuard ..... 81

**Куценко А. В., Атутова Н. Д., Зюбина Д. А., Маро Е. А., Филиппов С. Д.** Алгебраический криптоанализ низкоресурсных шифров Simon и Speck ..... 84

**Медведева Н. В., Титов С. С.** К задаче описания минимальных по включению совершенных шифров ..... 91

**Набоков Д. А.** Постквантовое электронное голосование на основе решёток при участии нескольких кандидатов ..... 95

**Погорелов Б. А., Пудовкина М. А.** Об ARX-подобных шифрсистемах на базе различных кодировок неабелевых регулярных 2-групп с циклической подгруппой индекса 2 . 100

**Семёнов А. А., Антонов К. В., Грибанова И. А.** Порождение дополнительных ограничений в задачах алгебраического криптоанализа при помощи SAT- оракулов ..... 104

**Kosolapov Y. V., Turchenko O. Y.** Choosing parameters for one IND-CCA2 secure McEliece modification in the standard model ..... 110

**Roman'kov V. A.** An improvement of cryptographic schemes based on the conjugacy search problem 114

Секция 4

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

**Ахметзянова Л. Р., Бабуева А. А., Кяжин С. Н., Попов В. А.** О конфиденциальности транзакций в децентрализованных системах учёта токенов ..... 119

**Девянин П. Н., Леонова М. А.** О приемах по доработке согласованного описания МРОСЛ ДП-модели для ОС и СУБД с целью его верификации инструментами Rodin и ProB ..... 126

**Кондырев Д. О.** Метод обеспечения конфиденциальности данных на основе zk-SNARK .. 132

**Лебедев В. В.** Деобфускация Control Flow Flattening средствами символьного исполнения 134

**Лебедев Р. К., Корякин И. А.** Применение расширений архитектуры x86 в защите программного кода ..... 138

**Недяк М. С.** Повышение эффективности поиска уязвимостей с использованием технологии фаззинга в виртуальных машинах JavaScript ..... 140

**Николаев А. А.** Расширение и исследование метода сокрытия информации Deep Steganography 146

**Никулин В. С.** Адаптация метода Розенблатта — Парзена для экспериментальной оценки надёжности вычислительной системы ..... 148

Секция 5

## ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ И ГРАФОВ

**Геут К. Л., Титов С. С.** Базисы над полем GF(2), порождённые при помощи операции Шура — Адамара.....154

**Косолапов Ю. В., Лелюк Е. А.** О разложимости произведения Шура — Адамара суммы тензорных произведений кодов Рида — Маллера ..... 158

**Лобов А. А., Абросимов М. Б.** Регулярное вершинное 1-расширение двухмерных решёток 161

**Пантелеев Р. И., Жаркова А. В.** Об аттракторах в одной дискретной двоичной динамической системе с двудольным графом зависимостей ..... 163

**Разумовский П. В., Абросимов М. Б.** Схемы построения минимальных вершинных 1-расширений полных двухцветных графов ..... 165

**Nagy G. P., El Khalfaoui S.** Towards the security of McEliece's cryptosystem based on Hermitian subfield subcodes ..... 168

Секция 6

## МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

**Егорушкин О. И., Колбасина И. В., Сафонов К. В.** О решении полиномиальных грамматик и общего алгебраического уравнения ..... 176

**Рыбалов А. Н.** О генерической сложности проблемы изоморфизма конечных полугрупп . 178

Секция 7

## ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

**Коврижных М. А., Фомин Д. Б.** Об эвристическом подходе к построению биективных векторных булевых функций с заданными криптографическими характеристиками ..... 181

**Кузнецов А. А., Кузнецова А. С.** О некоторых подгруппах бернсайдовой группы $B_0(2, 5)$ 184

**Ткачев А. В., Калгин К. В.** DPLL-подобный решатель задачи выполнимости над системой уравнений в АНФ ..... 187

СВЕДЕНИЯ ОБ АВТОРАХ ..... 191

АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ ..... 196

# ВОСПОМИНАНИЯ КОЛЛЕГ И УЧЕНИКОВ О ГЕННАДИИ ПЕТРОВИЧЕ АГИБАЛОВЕ

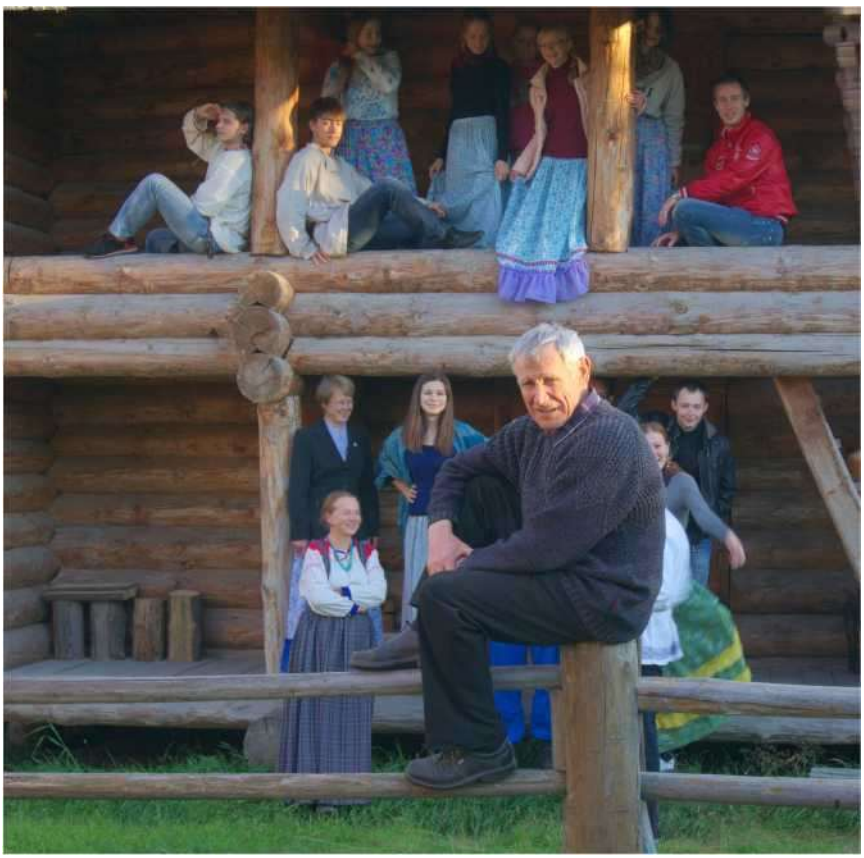
Дорогие друзья!

Вы держите в руках сборник трудов юбилейной XX школы-семинара SIBECRYPT. Юбилейной — и первой без её основателя и бессменного руководителя с 2002 г. Геннадия Петровича Агибалова, ушедшего от нас 16 декабря 2020 г.

С этого года наша конференция будет носить его имя. Едва ли сам Геннадий Петрович одобрил бы это — настолько чуждо было его натуре всякое «официальное» признание его заслуг. Но оргкомитет принял такое решение, признавая, что все организационные вопросы и характер проведения, тематика лекций и докладов, наполненность утренней и вечерней программ, все положительные моменты, душевный стиль и внимательное отношение к молодёжи, составляющие главные черты и отличительные особенности данной конференции, были заложены и реализованы именно благодаря задумкам, усилиям и таланту Геннадия Петровича.

В конце прошлого года мы обратились к соратникам, друзьям и ученикам Геннадия Петровича с предложением прислать свои воспоминания и впечатления о встречах с ним. Откликнулись очень многие, не только в России и не только те, к кому мы обращались. Мы публикуем эти заметки как дань памяти замечательному человеку и как первое знакомство с ним тех, кому не посчастливилось встретиться с Геннадием Петровичем лично.

Воспоминания публикуются в алфавитном порядке фамилий их авторов.



SIBECRYPT’13, с. Парабель Томской области

**Абросимов М. Б.** (профессор Саратовского государственного университета)

Не знаю, насколько я могу оставлять воспоминания о Геннадии Петровиче, так

как встречался с ним достаточно редко — не чаще одного раза в год. С другой стороны, я знаю его почти половину своей жизни, и он достаточно сильно повлиял на то, как она сложилась.

Впервые я встретился с Геннадием Петровичем в 2000 г. в Томске на конференции «Новые информационные технологии в исследовании дискретных структур», будучи аспирантом второго года. Мне сразу запомнилась какая-то безграничная энергия Геннадия Петровича, желание во всём разобраться, желание преобразовать пространство вокруг себя в творческую атмосферу научной вовлечённости. Потом появилась школа- семинар SIBECRYPT, при организации которой Геннадий Петрович создал особенную среду: он всё сделал для того, чтобы участники могли сконцентрироваться на конференции, не отвлекаясь ни на что постороннее: эти конференции обычно проводились в удалённых и уединённых местах, иногда в достаточно спартанских условиях. Эта школа-семинар стала для меня любимой, и при малейшей возможности я старался на неё попасть.

Геннадий Петрович был многогранным и сложным, невозможно описать его в нескольких словах, но, наверное, все, кто был с ним знаком, видели, что это необычный, особенный Человек, который со всей своей энергией и страстью отдавался любому делу, за которое брался, будь то исполнение гимна криптографов вместе со студентами и аспирантами, покорение водопадов на Телецком озере или обсуждение научных проблем. Таким он мне и запомнится.

Агиевич С. В. (зав. лаб. БГУ, Минск)

Образ Геннадия Петровича в моей голове абсолютно светлый: с улыбкой, с драйвом, с интересом, с желанием создавать. Правильный образ. Значит, всё было правильно и будет хорошо.

Бутузова Т. В. (преподаватель профессионального английского языка для студентов кафедры защиты информации и криптографии (ЗИК) Томского государственного университета)

Для меня Геннадий Петрович прежде всего харизматичный человек. Человек-борец, много сил и времени отдававший кафедре. Я хочу поделиться своими впечатлениями, связанными с ним и с кафедрой.

Для меня было необычно то, что на кафедре всегда были студенты: кто-то сдавал темы, кто-то приходил с вопросами, могли и чай попить: всё, как в большой семье. На стенах фотографии всех выпускников. Была хорошая традиция встречаться в начале учебного года с первокурсниками в неофициальной обстановке, за чаепитием. Сначала Геннадий Петрович представлял преподавателей, а затем каждый первокурсник рассказывал о себе.

Была ещё одна хорошая традиция: 7 апреля праздновать День рождения кафедры! К этому дню готовились все: и студенты, и преподаватели. Когда я первый раз была приглашена на этот праздник, меня потрясло то, что Геннадий Петрович ещё и стихи пишет. Не стишки, а **стихи**. И как он читал! Читал сердцем! Эти стихи были о его малой Родине. Он сумел передать все свои чувства! О своём детстве, о друзьях, о природе. И о своём сожалении, что редко туда возвращается.

Сохраним добрую память о Геннадии Петровиче!

Городилова А. А. (к.ф.м.н., Новосибирск)

Удивительный человек! Уверена, в каждом, кто когда-либо знал его, он останется в памяти преданным, душевным, честным человеком.

Девянин П. Н. (профессор, член-корр. Академии криптографии РФ, Москва)

Это был замечательный человек, широчайшей души, настоящий ученый, педагог, энтузиаст науки. Всегда буду его помнить.

Жаркова А. В. (к.ф.м.н., Саратов)

Геннадий Петрович был прекрасным специалистом, сколько идей и их воплощений! Замечательный человек, всегда весёлый, жизнерадостный и воодушевляющий всех вокруг!

Колегов Д. Н. (выпускник кафедры ЗИК, затем коллега Геннадия Петровича)

Геннадий Петрович Агибалов — профессор, энтузиаст криптографии и компьютерной безопасности, хакер и идейный вдохновитель. Под его началом была основана специальность «Компьютерная безопасность» и создана кафедра защиты информации и криптографии в ТГУ, научная конференция SIBECRYPT, ставшая и оставшаяся одной из немногих научных конференций в России, журнал «Прикладная дискретная математика», CTF-команда SiBears, лаборатория компьютерной криптографии. По его идее на кафедре защиты информации и криптографии, а затем в лаборатории компьютерной криптографии силами студентов и аспирантов велись работы над возрождением специализированного безопасного языка программирования ЛЯПАС и операционной системы на его основе.

Геннадий Петрович всегда работал только над масштабными проблемами: если делать язык программирования, то в интересах безопасности России, не меньше; если разрабатывать операционную систему, то для критически важных систем управления; если создавать криптографические алгоритмы, то для квантовых компьютеров, даже если их ещё нет.

Для меня и многих моих коллег и студентов всегда было удивительно, когда в процессе научных семинаров кафедры Геннадий Петрович мог вникнуть в сложную механику компьютерных систем, протоколов и уязвимостей, о которых он слышал впервые, а мы занимались годами, перевести эти процессы на свой язык — язык математики — и затем, размышляя в рамках созданной им модели, вести разговор с нами, молодыми специалистами, на равных, а часто и лучше нас понимать, в чём на самом деле проблема и что нужно сделать для её решения.

Геннадий Петрович был и остаётся человеком-легендой. Когда мы были студентами первого курса, глядя на Геннадия Петровича, все видели в нём человека, окутанного романтикой разведки, шифровок и тайн криптографии. Ходило много легенд о том, кто он, чем занимается и чему нас научит. Геннадий Петрович в лекциях всегда оперировал термином «враг», рассказывая об атаках на криптографические протоколы и шифры, и в те моменты создавалось стойкое ощущение, что враг никогда не сможет преодолеть криптографические барьеры, созданные с использованием математического аппарата. Можно сказать точно, что многие первокурсники, побывавшие на лекциях Геннадия Петровича и познакомившиеся с ним лично, мечтали стать хакерами или криптоаналитиками.

С тех пор прошло 20 лет. Многое, о чём говорили студенты, оказалось вымыслом, очень мало тех, кто связал свою жизнь с криптографией, кафедры защиты информации и криптографии в ТГУ уже нет, но одно сказать можно точно: Геннадий Петрович своим примером через всё то время, что я его знал, показал, что есть настоящая наука, что не стоит никого и ничего бояться, что нужно заниматься тем, во что ты веришь, и идти до конца.

Колесникова С. И. (д.т.н., Санкт-Петербург)

### Агибалов Г. П. и его отражение в нас

О моральных качествах АГП и его интеллектуальных достижениях (а «последние зависят от величия характера в значительно большей степени, чем это обычно принято считать» (А. Эйнштейн)) могут много сказать его ближайшие коллеги и ученики. Во мне АГП отразился как Учитель в самом прекрасном смысле этого слова

с редкой увлечённостью своим Делом и учениками, в которых вместе с криптографическими и математическими тонкостями впечатывал преданность и любовь к России. Точнее, чем Л. Н. Толстой, трудно подобрать ассоциативные формулировки для определения понятия «учитель»:

«Если учитель имеет только любовь к делу, он будет хороший учитель.
Если учитель имеет только любовь к ученику, как отец, мать, — он будет лучше того учителя, который прочёл все книги, но не имеет любви ни к делу, ни к ученикам.
Если учитель соединяет в себе любовь к делу и к ученикам, он — совершенный учитель».

Коренева А. М. (к.ф.м.н., Москва)

Я познакомилась с Геннадием Петровичем в 2012 г. на своей первой конференции SIBECRYPT, где оказалась благодаря научному руководителю, профессору В. М. Фомичёву. С тех пор я не пропустила ни одной поездки в Сибирь, так сильно меня впечатлила ни на что не похожая, по-домашнему тёплая и удивительная атмосфера этой сибирской конференции. У SIBECRYPT особенная энергетика и дух, которые во многом сформировались под влиянием идей, личности и энтузиазма Геннадия Петровича. Его любовь к Родине и российской науке, интерес к масштабным проблемам и научные споры, глубокие рассуждения и потрясающие стихотворения — без этого не проходила ни одна конференция SIBECRYPT.

Геннадий Петрович был и остаётся ярким примером безусловно талантливого Человека с большой буквы. Искреннего и преданного своим ценностям, своему делу жизни — становлению и развитию российской криптографической науки. Я ценю, что мне посчастливилось обсуждать с ним научные проблемы и результаты. Он обладал очень ясным умом и редкой энергией, всегда искусно добирался до самой сути каждого доклада.

Воспоминаний очень много: как играли в волейбол, сидели у костра, репетировали номера для творческого вечера. Как ездили на экскурсии, где приобщались к сибирской природе и русской истории. Как собирались в большом зале и обсуждали, где встретимся в очередной раз.

Геннадий Петрович восхищал своей прекрасной спортивной формой. Особенно хорошо помню, как в 2017 г. в горном парке «Бобровый лог» (Красноярск) они на пару с Ириной Анатольевной Панкратовой легко забежали на вершину горы, быстрее и бодрее всей молодёжи.

Геннадий Петрович был добрым человеком с русской душой, значительную часть которой он вложил в молодых учёных, в своих воспитанников. Так и во мне продолжает жить частичка его души.

Крылов П. А. (профессор, заведующий кафедрой алгебры ТГУ)

На протяжении многих лет у меня случались нечастые встречи с Геннадием Петровичем Агибаловым по каким-то поводам и на разного рода мероприятиях. Всегда чувствовалась цельность его натуры. У него были независимые суждения и собственная точка зрения на различные события и особенно на процессы, происходящие на факультете и в университете.

Обращало на себя внимание заинтересованное отношение Геннадия Петровича ко всему, что было связано с кафедрой защиты информации и криптографии, заведующим которой он был долгое время. Прежде всего это относилось к учебным делам и научной составляющей деятельности кафедры. Кафедра защиты информации и криптографии всегда привлекала внимание абитуриентов, обычно был конкурс и хорошие наборы. Студенты кафедры регулярно занимали призовые места на соревнованиях по

защите информации и компьютерной безопасности. Геннадий Петрович стремился сохранить и развить на кафедре научное направление в области криптографии. Он неоднократно говорил об этом в разговорах. В последние годы Геннадий Петрович высказывал и предпринимал определённые действия по реализации ряда идей, касающихся будущего кафедры. В частности, обсуждался переход кафедры на механико-математический факультет. Со мной он говорил о создании на кафедре алгебры совместной магистратуры по специальности, связанной с криптографией. К сожалению, в силу различных, часто трудно преодолимых препятствий эти планы не удалось реализовать. Отсутствовали также интерес и серьёзная поддержка этого руководителей разных уровней.

Геннадию Петровичу в своё время удалось добиться открытия в ТГУ диссертационного совета по двум специальностям, связанным с защитой информации и компьютерной безопасностью. И он был заместителем председателя этого совета (председатель — президент ТГУ Г. В. Майер). Помню (а я был членом этого совета) интересные и содержательные выступления Геннадия Петровича в дискуссиях на различные темы, близкие к защищаемой диссертации.

Геннадий Петрович более 20 лет также был членом с момента открытия кандидатского, а затем докторского советов, функционировавших на механико-математическом факультете. Он представлял специальность 01.01.06 — «Математическая логика, алгебра и теория чисел». Относился очень ответственно к обязанностям члена совета, занимал активную позицию на защитах. В 2019 г. Геннадий Петрович вошёл и в новый диссертационный совет, после того как ТГУ получил право самостоятельно присуждать ученые степени.

Геннадий Петрович Агибалов был неординарным талантливым человеком. Он внёс достойный вклад в образование и науку.

Мурин Д. М. (к.ф.м.н., Ярославль)

Я мало знал Геннадия Петровича. Он производил впечатление очень сильного человека, готового брать на себя ответственность, и за которым бы хотелось идти.

В моей жизни очень мало таких людей. Я всегда буду помнить его лихой подъём на гору на Байкале.

Панкратов И. В. (выпускник кафедры ЗИК)

Мне довелось не только учиться у Геннадия Петровича, но и писать курсовые и дипломную работы под его руководством. Кроме этого, я был «заочно знаком» с ним по маминым рассказам. После выпуска мы периодически виделись на конференциях или я просто забегал на кафедру по старой памяти.

Мне всегда казалось естественным, что у студента есть кафедра, куда можно практически в любой момент зайти и обратиться с какими-то своими проблемами или даже просто попить чайку. Как позже оказалось, это не у всех так, а даже почти совсем ни у кого, кроме нашей кафедры. У нас же было заведено и, вероятно, именно Геннадием Петровичем, что студенты и преподаватели общались по различным вопросам и имели тёплые, почти семейные отношения. И Геннадий Петрович всегда готов был выслушать любого студента, относился к нам по-отечески. Большинство из нас отвечало ему взаимностью.

В 2012 г. на конференции в Иркутске я заболел, причём как-то достаточно внезапно и сильно, пришлось даже вызвать скорую. Студентом я тогда уже, конечно, не был, и Агибалов не нёс за меня вообще никакой ответственности, но он отложил все дела, коих имелось огромное количество — всё-таки первый день конференции, и занимался мной добрую половину утра, пока не убедился, что дальше я сам справлюсь. Не мог он оставить человека в беде, никогда.

Однажды в рамках курсовой работы я получил несколько неожиданный результат, но сколько ни проверял, результат подтверждался и никак не хотел опровергаться. Немного озадаченный, я пришёл с этим к Геннадию Петровичу. Первая реакция была категоричной: «Это ерунда какая-то, ищи ошибку в доказательстве!» Через некоторое время мне удалось убедить Геннадия Петровича в правильности доказательства, мы некоторое время обсуждали теоретические стороны вопроса, а в конце беседы Геннадий Петрович совершенно буднично заявил: «Так ведь это же очевидно!»

Где-то в 2004 г. у Геннадия Петровича стали болеть колени во время бега, а бегать он любил и бегал довольно много, несмотря на уже весьма солидный возраст. После некоторого обсуждения этой проблемы мы с одногруппниками решили подарить Агибалову роликовые коньки на приближающийся день рождения. Выяснили втихаря размер ноги, пошли в спорттовары и купили коньки, которые нам показались самыми подходящими. Уже дома увидели крупную надпись на коробке «Ролики подростковые», повеселились, но решили, что это ничего не меняет. Когда ролики были торжественно вручены прямо на кафедре, Геннадий Петрович, тоже посмеявшись над «подростковыми роликами», надел их и поехал кататься по кафедре. Позже мы узнали, что он катался на них чуть ли не каждое утро и колени чувствовали себя при этом вполне уютно.

Что меня всегда поражало и восхищало в Агибалове, так это его стойкость и иногда даже жёсткость в отстаивании всего того, что он считал правильным, и борьбе со всякой профанацией. Почему-то я всегда был уверен, что он никогда не сделает выбор в пользу чего-то, что было бы выгодно ему лично, но «неправильно» в целом или вредило бы его Делу. А своим Делом, насколько я понимаю, он считал служение Отечеству, в том числе воспитание молодого поколения образованных и патриотичных (в правильном смысле этого слова) людей. И делал он это всеми доступными методами: и личным примером, и влиянием на окружающих взрослых. К сожалению, борьба за правое дело — не самое безопасное и выгодное занятие, поэтому Геннадий Петрович имел немало проблем на работе, но они его никогда не останавливали и, похоже, вообще не принимались в расчёт.

Панкратова И. А. (ученица, затем коллега Геннадия Петровича)

С Геннадием Петровичем я работала всю свою жизнь, начиная с защиты диплома.

Помню, как после окончания ФПМК мы с Ирой Верёвкиной пришли работать в лабораторию синтеза дискретных автоматов (ЛСДА) СФТИ, которой Геннадий Петрович тогда руководил. Сидим на семинаре, слушаем докладчика, ничего не понимаем. Пока Геннадий Петрович не говорит: «Стоп. Давайте очистим задачу» — и не начинает задавать вопросы (это обычно случалось быстро — минут через 5 после начала доклада). И в ответах докладчика на вопросы и комментариях Геннадия Петровича выясняется, что всё просто и понятно!

Это умение Геннадия Петровича быстро уловить суть дела, очистить его «от шелухи» и преподнести так, чтобы и слушатели, и сам докладчик поняли, о чём на самом деле речь, проявлялось не только при обсуждении курсовых работ студентов и диссертаций начинающих исследователей, но и докладов маститых учёных.

Конец 1990-х, очередной семинар ЛСДА. Геннадий Петрович тогда уже задумал открывать новую специальность в ТГУ, но мы об этом не знали и о криптографии ничего не слышали. Семинар начинается так: «Вот я сейчас с Быковой (Светлана Васильевна, ближайший соратник и сподвижник Геннадия Петровича во всех делах) на глазах у всех договорюсь об общем секрете, и вы никогда его не узнаете!» Всё! Мы заинтересованы навсегда! А сам доклад был посвящён схеме Диффи — Хеллмана открытого обмена секретными ключами, которую, я думаю, все участники того

семинара, даже никогда больше не встречавшиеся с криптографией, помнят до сих пор.

В Издательстве ТГУ появилась новая сотрудница-экономист. Прихожу со своим учебным пособием, она начинает считать, сколько будет стоить его издание, говорит — надо редакторам отнести. Я в растерянности — про редакторов не знала. Тут в кабинет заглядывает Клара Григорьевна Шилько (главный редактор Издательства), спрашивает меня: «Геннадий Петрович пособие читал?» «Да, читал, правил, много». Клара Григорьевна поворачивается к сотруднице: «Запомните этих людей! У них берём всё, что они приносят. Лучше Агибалова мы всё равно не сделаем». В итоге на пособии написано «в авторской редакции», по факту — в редакции Геннадия Петровича.

Это вообще характерно — у учеников Геннадия Петровича, включая студентов, почти нет работ, написанных в соавторстве с ним, даже когда основной вклад в написание работы был сделан Геннадием Петровичем. А вот обратное случалось часто: Геннадий Петрович работает над большой статьёй, что-то иногда со мной обсуждает. Малейшее моё замечание-предложение-дополнение, и бац! — я в соавторах. Говорю: «Зачем? Тут же нет моих результатов». Ответ: «А как может быть иначе??»

Уже в зрелом возрасте Геннадий Петрович увлёкся лыжами, освоил технически сложный коньковый ход, азартно участвовал в соревнованиях, иногда выигрывал. Запомнился такой случай. Первенство среди сотрудников вузов Томска, возрастная группа 70+ (самая многочисленная, потому что без верхней границы). На старте, в том числе, мастера спорта по лыжным гонкам, лыжному ориентированию, «полупрофессионалы» — и сейчас работающие тренерами, «в боевой раскраске» — пёстрых гоночных костюмах и на хороших лыжах. Дают старт — и Геннадий Петрович «выкашивает» стартовую поляну (уходит с неё лидером). Потом его, конечно, обогнали — не все; по- моему, он занял тогда третье место; но понравилась фраза на финише: «Были бы лыжные забеги на 100 метров — я бы выиграл!»

А наша кафедра, родная 109-я аудитория второго корпуса ТГУ, где мы проводили большую и лучшую часть своей жизни! Там всё, начиная от «пробивания» помещения для кафедры в ректорате и до закрашивания огрехов на стенах, оставленных нерадивыми ремонтниками — установщиками окон, сделано Геннадием Петровичем. Первое, что он принёс и повесил на стену в 109-й, — флаг и гимн Российской Федерации. Запомнилась картина — два профессора (Геннадий Петрович и Александр Михайлович Оранов) ползают на коленках под шифоньером, подкручивая ножки, — для выравнивания. И ни одному не пришла в голову фраза «в мои должностные обязанности это не входит», которую довелось услышать от вчерашнего выпускника ТГУ в ответ на просьбу унести что-то в главный корпус.

А как мы ехали на конференцию в Иркутск в 2004 году! Примерно 10 студентов, столько же сотрудников, все в одном плацкартном вагоне. Стали по ролям читать «Федота-стрельца» Л. Филатова; царь, конечно, — Геннадий Петрович. Постепенно в отделении, где происходила читка, собрался весь вагон — и свои, и просто пассажиры. Потом этого «Стрельца», адаптированного всякий раз по-новому на злобу дня, мы показывали и на Днях кафедры, и на Всероссийской конференции SIBECRYPT.

Многие знают о «сложных» отношениях Геннадия Петровича с начальством. К сожалению, ситуация типична для выдающихся российских учёных (а скорее, не только российских и не только учёных) — Сеченов, Менделеев, Лобачевский, . . . (список можно продолжать бесконечно) испытывали гонения со стороны чиновников, борясь с косностью, бюрократизмом и непониманием. Увы, слабое утешение в том,

что случилось — закрытие в ТГУ специализации «Математические методы защиты информации» (трижды признанной независимыми экспертами одной из лучших в России), уничтожение кафедры (признанной Госдумой РФ в 2015 г. лучшим образовательным центром года в области информационной безопасности); всё это — «выстрелы в сердце» Геннадию Петровичу, произведённые властями ТГУ.

Зато студентами Геннадий Петрович был любим бесконечно! Нет, не «был» — есть! Все, кому посчастливилось учиться у него, на всю жизнь сохранят в душе этот чистый исток, с которого начался их путь.

И все мы, бесконечно грустя о невосполнимой потере, будем всё же радоваться, что в нашей жизни был такой Человек, как Геннадий Петрович.

Пономарева В. Н. (сокурсница Геннадия Петровича, неоднократно участвовала вместе с ним в туристических походах)

Хорошо помню такой эпизод. Двигаясь в Киргизии по горному хребту Сусамыр-тау Внутреннего Тянь-Шаня, мы вышли к месту, где этот хребет прорывает ущелье горной реки Чичкан. Моста, конечно, не было, но кто-то натянул над этим бурным и широким горным потоком канат с карабином. Однако спасительный карабин застрял как раз в центре каната и, казалось, был нам совершенно недоступен. Ситуация безвыходная, и мы в отчаянии. . . И тогда в схватку с неожиданной преградой вступил наш гимнаст Гена Агибалов! Виртуозно прогнувшись, он повис на канате и, перебирая руками, быстро и ловко добрался до карабина. Сделав над бушующей бездной невероятно красивый переворот, Гена пристегнулся к карабину и так же быстро вернулся к нам. Мы в полнейшем восторге и восхищении любовались нашим бесстрашным, ловким и сильным спасителем! Как я сама оказалась на другом берегу, не помню. Ведь высоко висеть над ревущим потоком, даже пристегнувшись к карабину, было очень страшно. . .

Поттосин Ю. В. (доцент БГУ, Минск)

Мы с Геннадием Петровичем учились на одном факультете, но на разных курсах. Хотя, когда нам, нескольким пятикурсникам, продлили срок обучения на полгода и усадили с четверокурсниками слушать лекции по двум спецкурсам, мы оказались с ним «на одной студенческой скамье». Более близко мы познакомились, работая в одном небольшом научном коллективе, руководимом Аркадием Дмитриевичем Закревским. Там были сотрудники проблемной лаборатории, каким был я, а также аспиранты и преподаватели, каким был Геннадий Петрович (почти никого из них уже нет). У нас, молодых тогда людей, установились дружеские отношения. Стали совместно совершенствовать свой разговорный английский язык, понимая, что читать научные статьи на английском трудно без навыков разговорной речи. В своих воспоминаниях Геннадий Петрович тепло отзывался о Максе Хановиче Курмане, который вёл наш кружок английского языка. Понимали мы тогда, что без знаний основ дискретной математики, которую нам, радиофизикам, не читали, невозможно вести исследования в выбранной нами области. В то время вышла книга К. Бержа «Теория графов и её применения», и мы из неё стали совместно набирать знания по дискретной математике. Для этого создали что-то вроде семинара, где каждому была определена глава, которую он должен разобрать и доложить на заседании. Так мы вместе занимались и английским языком, и теорией графов. Сейчас, кстати, я преподаю именно дискретную математику студентам Белорусского государственного университета информатики и радиоэлектроники.

Было у нас тогда такое правило: если ты написал статью или даже диссертацию, перед тем как куда-то подавать, дай её почитать кому-нибудь из своих товарищей на предмет конструктивной критики. Когда я написал черновик своей кандидатской

диссертации, я попросил Гену почитать ее. Он согласился. Какие были замечания, я не помню, но когда я его попросил быть вторым оппонентом (он уже имел степень кандидата, а тогда одному из оппонентов разрешалось быть из той же организации, где работает соискатель), с работой он уже познакомился и также согласился. Хорошо выступил на защите, высоко оценил мою работу. Когда Геннадий Петрович уезжал в командировку, то просил меня прочитать за него лекции студентам по его предмету. Можно сказать, так он вовлёк меня в преподавательскую деятельность, которой я занимаюсь по совместительству по сей день, о чём уже упомянул. Однажды, приехав из Москвы, он связал меня с редакцией реферативного журнала «Математика», и я с 1970 по 2017 г. реферировал статьи по теории графов. Какую-то пользу я от этого, конечно, получил.

Случилось так, что я уехал из Томска, но дружеские отношения с Геннадием Петровичем не прекратились. Я много раз приезжал в Томск и обязательно встречался с Геной, если он не был в отъезде во время отпуска. Будучи в Минске, он также заходил ко мне. В разное время встречался с ним на конференциях в разных городах. С большим удовольствием участвовал в организуемых им конференциях, если имел на это возможность. Мне нравилась обстановка, в которой они проходили. Последний раз я встречался с ним в Томске в 2018 г., а по телефону разговаривал с ним в мае 2020 г. Не мог предположить, что это были последняя встреча и последний разговор.

Для меня уход Геннадия Петровича — большая потеря. С ним у меня связаны самые приятные воспоминания. Храню его поздравление в стихах, которое он мне прислал когда-то по случаю моего юбилея. Буду помнить всегда о нём, как о верном друге, хорошем человеке.

Романьков В. А. (профессор ОмГУ, Омск)

Познакомился с Геннадием Петровичем в Шушенском на SIBECRYPT 2006 г., куда меня уговорил поехать мой друг — Рашид Тагирович Файзуллин (к сожалению, уже ушедший). Встречался с ним только на конференциях. Но впечатление такое, что знал его давно и хорошо. Знал о его трудном военном детстве, более кратко о дальнейшей учёбе, видел его отношение к делу, великое трудолюбие. Этот человек был мне близок во многих отношениях: к жизни, работе, журналу, стихам. Стихи — вот что произвело на меня неизгладимое впечатление, вот откуда мои представления о нём. Геннадий Петрович был искренним человеком, не стеснялся своего деревенского происхождения, отношения к родной земле, всегдашнего свитера. Не приукрашивался. Ни в стихах, ни в жизни. Не был благолепным, мог отчитать, не согласиться с тобой, но всё равно оставался близким человеком. Я выпросил у него файлы со стихами, где вся его жизнь, трогательные воспоминания о прошлом и тяжкие думы о настоящем. Геннадий Петрович в его неприятии многого в нашей нынешней действительности не был наблюдателем, как её записные критики. Это были представления человека, занятого трудом, активного исследователя, редактора, преподавателя, учителя, физически крепкого человека, вкладывающего во все свои дела частицы души. Большая и невосполнимая потеря.

Семенов А. А. (зав. лаб. ИДСТУ, Иркутск)

Не стало Геннадия Петровича Агибалова. Человека, стоявшего у истоков эпохи дискретной математики и криптографии в Томске. Эпохи, начатой Аркадием Дмитриевичем Закревским и продолженной Геннадием Петровичем. Им была создана одна из сильнейших на территории России научных школ в области криптографии и компьютерной безопасности. Организованная им в 2002 г. ежегодная конференция SIBECRYPT (школа-семинар в понимании самого Геннадия Петровича) стала настоящей

кузницей молодых кадров в области приложений дискретной математики к проблемам информационной и компьютерной безопасности. Было бы интересно представить статистику по защищённым диссертациям участников школы за почти 20 лет её активной работы. Геннадий Петрович как-то приводил подобные данные, но, по-моему, детальной ретроспективы на всю историю школы в этом плане не было.

В общении с Геннадием Петровичем не всегда было легко — в научных спорах он воспринимал только точные, математически обоснованные аргументы. Я был знаком с Геннадием Петровичем более 20 лет, и всё это время, да я так полагаю, что и всю жизнь, он был одержим (в хорошем смысле) своими идеями — как научными, так и организаторскими, и при их продвижении мог занимать весьма жёсткую позицию. Неизменным, однако, оставалось его всегда доброе и внимательное отношение к молодёжи. Про его понимание роли образования (как в целом, так и в области криптографии в частности) в развитии России хорошо написал Денис Колегов. К этим словам добавить по существу нечего. Геннадий Петрович всегда болел за страну и всеми силами пытался внести свой вклад в развитие направлений, в которых был экспертом, а в некоторых и основоположником. И ведь получалось! Нетерпимость Геннадия Петровича к халтуре в любой форме создавала ему много трудностей в общении с начальством. Но эти трудности его не пугали. Он всегда оставался верным своим принципам и не шёл ни на какие компромиссы.

С бескомпромиссностью Геннадия Петровича связан целый ряд историй, среди которых есть немало весёлых — по крайней мере, с позиции моего, допускаю, весьма своеобразного чувства юмора. Одну такую историю, рассказанную как-то им самим, я и хочу привести здесь. Я присутствовал при этом рассказе, однако сразу скажу, что не могу поручиться за точность всех деталей, поскольку времени прошло довольно много.

Насколько я помню, дело происходило не в ТГУ, а в каком-то другом вузе (честно говоря, даже не знаю в каком), где Геннадий Петрович согласился прочитать курс лекций по криптографии. Я так полагаю, что в основе этих лекций, скорее всего, лежали его «Избранные теоремы начального курса криптографии». Данная книга — это, с моей точки зрения, выдающееся явление на просторах российского образования. Книгу нельзя назвать лёгкой для чтения, и я бы даже не назвал её учебным пособием, поскольку вряд ли обычный студент сможет разобраться во всех её разделах без помощи лектора. Но зато студент, полностью усвоивший представленный в ней материал (который весьма обширен, несмотря на небольшой объём в страницах), как мне кажется, может спокойно поступать в аспирантуру и начинать исследовательскую работу в области криптографии.

Так вот, семестр закончился и пришла пора экзаменов. Однажды Геннадий Петрович задержался в аудитории, оформляя результаты принятого экзамена. Кто-то постучал в дверь. «Входите, открыто!» Перед Геннадием Петровичем предстала колоритная дама, скажем так, нетипичной для города внешности. В руках у неё была зачётная книжка. Далее состоялся примерно следующий диалог:

— Простите, Вы кто?

— Так мы студенты ваши!

— Какие ещё студенты? Я Вас впервые вижу!

— Так а мы с Колпашева! Вот, приехали сдавать вам криптографию!

Ошарашенный Геннадий Петрович, выглянув в коридор, обнаружил там ещё с десяток подобных персонажей, покорно ожидающих своей участи. Выяснилось, что всё это время вуз вёл видеозаписи его лекций, которые затем транслировались в один

из многочисленных филиалов, расположенных в различных населённых пунктах области. В обязанности студентов, заплативших, естественно, деньги за такое «обучение», входили приезд в Томск и сдача экзамена. Причём, что особенно интересно, Геннадий Петрович был полностью не в курсе того, что данный вуз задействует его в рамках такой «модели образования».

Финалом этой истории стало заявление от Геннадия Петровича на увольнение по собственному желанию. В ответ на вопрос руководства: «А в чём, собственно, дело?» — Геннадий Петрович изрёк свою бессмертную фразу: «Миша (не ручаюсь за точность имени)! Я не хочу участвовать в чужих преступлениях!»

**Сибирякова В. А.** (коллега Геннадия Петровича)

Говорить о Геннадии Петровиче в прошедшем времени — невыносимо. По моему мнению, такие люди должны жить долго-долго.

Геннадий Петрович, несомненно, — гениальный математик, физик, логик, блестящий педагог, эрудит во многих областях, человек, создавший из 0 и 1 целый мир, мир криптографии. Это его замечательные слова: «В мире ничего не существует, кроме 0 и 1!» Его вклад в развитие компьютерной безопасности в университете, городе, всей стране, да и во всём мире неоценим. Его ученики защищают информацию во многих частях света.

Но для меня Геннадий Петрович, в первую очередь, Человек с большой буквы: внимательный, добрый, отзывчивый, всесторонне развитый, готовый прийти на помощь в любой момент, не жалея сил и средств.

Несколько фактов.

Несмотря на свою колоссальную занятость, он приходил к больной коллеге справиться о здоровье, поговорить, оказать финансовую помощь.

Потрясает его уважительное отношение к своим родным. Ему пришлось и с мамой, и с папой быть рядом в последние дни и проводить их в последний путь на родину. В 2017 г. он ездил в Хакассию, на родину. Был в Абакане, где я находилась со своей престарелой мамой. Так Геннадий Петрович подошел к дивану, где она лежала, встал на колени, обнял и сказал одобрительно: «Ничего не слабая, как хорошо выглядит, какая молодец!»

Шуточный случай. Однажды Геннадий Петрович пришёл на кафедру и сказал, что он был на дне рождения великого человека. Спросили, почему. Потому что он родился между Гитлером и Лениным. Тогда я, смеясь, сказала: и я такая же. Он запомнил и каждый год поздравлял меня в этот день.

А кафедральные праздники 7 апреля — всё держалось на его идее и инициативе: спортивные соревнования, олимпиады по математике, информатике между курсами, праздничный концерт и чай! К месту следует заметить, что неоценимой помощницей ему была Ирина Анатольевна Панкратова.

**Соколов С.** (выпускник кафедры ЗИК)

На первом курсе у нас был семестр введения в математику. Геннадий Петрович рассказывал не столько о математике, сколько о математическом мышлении. Я очень ярко и отчётливо помню тот день, когда в моей голове повернулись шестерёнки и я понял про логичность и последовательность высказываний, про импликацию и эквивалентность, что это всё применимо и вне математики. Это была самая важная лекция, которая многое поменяла в моей жизни. С тех пор стал больше изучать рациональность и математическое мышление. Вот так Геннадий Петрович навсегда перевернул моё мировоззрение, за что я ему безмерно благодарен.

**Тимошевская Н. Е.** (ученица, затем коллега Геннадия Петровича)

«По утрам кошка ко мне на колени запрыгнет, мы с ней посидим пару минут, и только тогда я уже готов вставать. . . » — от этой простой фразы запало какое-то чувство душевной теплоты.

Поездка на конференцию в Шушенское в 2006 г. для меня ознаменовалась острой ушной болью. Боль в ухе стала нарастать ещё в поезде и концу второго дня была почти невыносимой.

— Геннадий Петрович, так и так, боюсь, мне надо ехать обратно домой срочно.

— Не выдумывайте, завтра с утра что-нибудь придумаем.

На следующее утро до начала первого дня конференции, когда у организаторов обычно дел по горло, мы вместе идём в местную поликлинику, ну как идём — ГП идёт, а я полубегу, стараясь не отстать. По дороге он объясняет, что уже позвонил и обо всем договорился, он знает там врачей ещё с былых времен. Позже выяснилось, что у меня был разрыв барабанной перепонки, выписанные лекарства сделали своё дело, и к третьему дню я была в состоянии сделать доклад. Другой мог бы отмахнуться или перепоручить кому-то, и без того забот. . . но не Геннадий Петрович.

Токарева Н. Н. (к.ф.м.н., Новосибирск)

Мы познакомились с Геннадием Петровичем почти пятнадцать лет назад. Смелость, упорство и полная самоотдача, с которыми жил и работал Геннадий Петрович, поражают. Во многом благодаря личному примеру Геннадия Петровича, мы стали пробовать развивать криптографию у себя в Новосибирске. Наши преподаватели, студенты и аспиранты стали приезжать на SIBECRYPT, ни одного года не пропуская. Эта школа-конференция сразу запоминается своей душевностью, сосредоточенностью на главном, возможностью прямых разговоров о науке и её проблемах, разговоров честных и без пафоса. Безусловно, такой её создал Геннадий Петрович.

То, что сделал Геннадий Петрович, не оценено, не понято ещё до конца, сделать это только предстоит. Как факт — созданная Геннадием Петровичем уникальная кафедра защиты информации и криптографии, на которой глубокое системное образование сочеталось с серьёзной исследовательской работой, стала первой и долгое время единственной за Уралом группой в области криптографии — на многие-многие километры просторов нашей Родины до самой Камчатки не было больше ничего. И Геннадий Петрович не только такую группу создал, но и сделал её одной из сильнейших в России. Геннадий Петрович глубоко и остро чувствовал свою ответственность. Конечно же, он помнил знаменитые слова М. Ломоносова: «Российское могущество прирастать будет Сибирью и Северным океаном», как помнил и другие, менее знаменитые слова госсекретаря США М. Олбрайт: «Ни о какой мировой справедливости не может быть и речи, пока такой территорией, как Сибирь, владеет одна страна».

Из остроты переживаний Геннадия Петровича за судьбу своей Родины возникла и SIBECRYPT — Сибирская криптографическая конференция, и кафедра защиты информации и криптографии — «Есть такая профессия — информацию защищать», и свой, отечественный, язык программирования Ляпас. Возникли и стихи Геннадия Петровича, пронзительные, а иной раз полные горечи, и крепкая дружба со студентами, авторитет и глубокое уважение к Геннадию Петровичу в среде специалистов. Даже поклонение. Хотя трудно себе представить, что оно было нужно Геннадию Петровичу. Он всегда был прост и поразительно скромен, у него болела душа. Для меня Геннадий Петрович всегда останется в памяти необыкновенным человеком. В одном строю с В. М. Шукшиным и В. С. Высоцким. Светлая память.

*Томашев В. Ф.* (дипломник Геннадия Петровича, РФФ ТГУ, группа 752, 1965-1970)

«Главное — постановка задачи» — это девиз научной деятельности Геннадия Петровича. Если задача чётко и корректно поставлена, то с большой вероятностью она будет рано или поздно решена. В противном случае трудно ожидать, что решение будет получено. Этот девиз, высказанный им на банкете по случаю защиты дипломов студентами нашей группы, запомнился мне на всю жизнь.

Геннадий Петрович был куратором нашей 752-й группы радиофизического факультета. Похоже, что это был его первый опыт в роли куратора после того, как он защитил кандидатскую диссертацию по криптографии. Помню, как на первом курсе одногруппники послали меня на кафедру ЭВТиА (электронно-вычислительной техники и автоматики) узнать, кто же все-таки является куратором нашей 752-й группы. Все мы, тогда ещё первокурсники, представляли, что куратор — это как классный руководитель в школе.

На старших курсах Геннадий Петрович вёл почти все занятия по специальности в нашей подгруппе «дискретчиков» из девяти студентов. Это были спецкурсы по важнейшим разделам дискретной математики:

— теории множеств и булевой алгебре;
— теории алгоритмов и конечных автоматов;
— теории групп, крайне актуальной и в настоящее время;
— теории кодирования информации (коды, обнаруживающие и исправляющие ошибки).

Занятия проходили в тёплой, дружеской, практически домашней обстановке.

Геннадий Петрович также руководил курсовыми и дипломными работами, побуждая нас к творческой самостоятельности и научной точности. Его дипломниками были Виктор Беляев, Дмитрий Черемисинов и Валерий Томашев. Каждый работал над своим аспектом задачи, связанной с оптимизацией размещения аппаратуры. Геннадий Петрович настоял на том, чтобы по итогам наших дипломных работ были представлены тезисы на семинар по Комбинаторной математике в МГУ, а затем статья в журнал «Известия Сибирского физико-технического института». Геннадий Петрович руководил, но на соавторство не соглашался, если сам не принимал участия в написании статьи. Мы благодарны ему за первые уроки в сочинении научно-технических текстов.

Из реликвий у меня сохранился автограф с его ответом на мою попытку доказательства одной теоремы из теории графов.

**Фомичев** В. М. (профессор Финансового института при Правительстве РФ, Москва)

Стал вспоминать интересные эпизоды и понял, что, скорее всего, получится повторение того, что многие напишут. Разве если только вспомнить, как ГП в свои 65-70 лет по-мальчишески выкладывался на спортплощадках (футбол, волейбол), потому что, видимо, не позволял себе делать что-то вполсилы.

Потом вдруг вспомнил, что я ему посвятил стихи. Высылаю эти стихи теперь Вам в надежде, что они будут интересны всем, кто любил нашего Геннадия Петровича.

### Г. П. Агибалову

Это божий крест — иметь характер И болеть душою за людей.
От отца досталось да от матери —
Пронести его теперь сумей.
С мощной деревенскою закваской, Не привыкший врать или ловчить, Ход нечестный ты готов с остраткой,
Приостановив, изобличить.

Ты льстецу упрешь колено в горло, Чтобы он не смог уже лизать.
Словом, зашифрованную подлость Ты сумеешь голой показать.
Бьёшься ты с начальством не за деньги, Совесть не даёт тебе молчать.
«Отвечай» — зовёт она в смятеньи.
Как тут промолчать, не отвечать?
Мы с тобой встречаемся на CRYPTax, Чувствуем души твоей «fairplay».
Ты соврать не дашь, не так воспитан, Шанс даря нам быть чуть-чуть честней.
Видим и любовь к тебе студентов,
Слышим строк неповторимый звук, Разве что не слышим комплиментов, Ты не переносишь их на дух.
Стих твой льётся вольно и широко, Заполняя души до краёв.
А в стихах любви и боли столько, Что стремишься слушать вновь и вновь.
Брось, Петрович, подводить итоги, Ты ещё не все нам рассказал.
И Сибири тайные дороги
Ты пока не все нам показал.
Ты ещё не раз нас всех научишь, Что поставить во главу угла.
И докажешь — честность все же лучше, Чем бесчестье в окруженьи благ.

09.12.2011

**Харин Ю. С.** (профессор БГУ, Минск)

Профессор Геннадий Петрович Агибалов — выдающийся учёный в области дискретной математики, организатор высокорейтингового среди «дискретчиков» журнала «Прикладная дискретная математика», организатор подготовки специалистов-криптографов в Томском государственном университете, человек, безгранично влюблённый в науку и преданный своему делу.

С Геннадием Петровичем меня судьба свела в 1971 г., когда после окончания Томского госуниверситета по кафедре прикладной математики в июне месяце мой научный руководитель Геннадий Алексеевич Медведев направил меня вместе с Юрием Ивановичем Параевым на Всесоюзную школу-семинар по стохастическим системам (село Жукин под Киевом). Так получилось, что в это же время в командировку в Киев в Институт кибернетики АН Украины собирался Геннадий Петрович Агибалов. Лететь в Киев надо было с пересадкой в Москве. Самолеты в Москву летали два раза в неделю, и у нас троих билеты оказались на один и тот же рейс. Для меня, только что со студенческой скамьи, стремящегося в науку, такая неожиданная поездка с ведущими профессорами была большой гордостью; я впитывал все их привычки, шутки, советы. В московский аэропорт Внуково мы прилетели поздно вечером, а улетать в Киев надо было рано утром. В аэропорту мы увидели объявление о частной квартире в посёлке рядом с Внуково и поехали туда переночевать. Геннадий Петрович имел аскетический

характер, не проявлял нисколько усталости. Проснулись рано утром. Я навсегда запомнил фразу Геннадия Петровича: «Понежиться можно, но можно и не нежиться», после которой он резко вскочил и моментально активизировался. Мне кажется, в этой фразе проявился его сильный характер и бесстрашие перед нагрузками и трудностями.

Геннадий Петрович несколько раз участвовал в работе нашей Минской конференции «Компьютерный анализ данных и моделирование» и всегда вызывал симпатии у участников конференции. Память о дорогом Геннадии Петровиче Агибалове навсегда сохранится у всех знавших его сотрудников НИИ прикладных проблем математики и информатики БГУ.

Черемушкин А. В. (профессор, член-корр. Академии криптографии РФ, Москва)

Двадцать лет назад на одном из пленумов УМО вузов по образованию в области информационной безопасности ко мне подошёл незнакомый профессор из ТГУ и предложил выступить у них в университете по тематике компьютерной безопасности. Это был Геннадий Петрович, который тогда с удивлением узнал, что есть такая специальность КБ, образовательный стандарт по которой предусматривает чтение криптографических дисциплин. Как потом рассказывал сам Геннадий Петрович, ему в молодости в рамках одной из НИР пришлось исследовать ряд практических криптографических задач, после чего он решил писать диссертацию в этой области. Но столкнувшись с известными трудностями, ему пришлось сменить тему. В результате он всё-таки выбрал близкую открытую тему по изучению свойств конечных автоматов и успешно защитил кандидатскую, а затем и докторскую диссертацию. Поскольку я тогда выразил сомнение в возможности осуществления такой командировки, Геннадий Петрович сразу же высказал идею о создании регулярной школы-семинара, которая через несколько лет получила название SIBECRYPT.

Об этой школе-семинаре, о её географии, охватившей большую часть городов Сибири, участниках из многих городов России от Калининграда до Восточной Сибири, из Белоруссии и Украины, об удивительных и незабываемых экскурсиях, о многочисленных удачных находках и оригинальных задумках по её проведению, конкурсах-соревнованиях и творческих вечерах, пришедших на смену стандартным товарищеским ужинам, можно написать отдельную книгу. В её организации, во многом, раскрылся многогранный талант и сибирский характер Геннадия Петровича. Он везде старался брать с собой студентов, находил докладчиков и вставлял в программу большое число лекций-обзоров по разным областям, организовывал рейтинги докладов в номинациях «студент» и «аспирант», сам готовил выступления на вечере самодеятельности. Меня всегда поражала открытость и душевность атмосферы этих поездок. Видя такое отношение организаторов, выступавших против всякой официальности и формализма, во всех городах и вузах нас принимали очень тепло и по-домашнему. И для меня было самым удивительным, что всё это происходило, как правило, далеко не всегда благодаря, а подчас и вопреки решениям администрации, а в основном при поддержке единичных энтузиастов из профессорско-преподавательского состава.

Поскольку в рамках существующих серий журнала Вестник ТГУ издание тезисов докладов и законченных статей было затруднительно, то Геннадий Петрович успешно реализовал идею создания собственного научного журнала и его приложения под придуманным им удачным названием «Прикладная дискретная математика» (ПДМ). Хотя в то время многие научные журналы испытывали большие трудности, журнал ПДМ был успешно зарегистрирован, вошёл в перечень ВАК и базу данных Scopus. Он занял очень востребованную нишу среди немногочисленных российских журналов, в которых

специалисты по дискретной математике и её приложениям могут публиковать свои работы. Как главный редактор, Геннадий Петрович внимательно прочитывал и редактировал все прошедшие независимое рецензирование публикации, поправляя как молодых, так и уже известных авторов.

Мне часто приходилось бывать на кафедре, организованной Геннадием Петровичем, участвуя в работе ГЭК и защитах диссертаций. В небольшой комнате, которая одновременно выполняла роль кабинета заведующего кафедрой, преподавательской и учебной аудитории для приёма курсовых и дипломных работ, висели фотографии со всех выпусков и два больших портрета А. Д. Закревского и К. Э. Шеннона, а в шкафу стояло оригинальное издание книги Д. Кана. О Шенноне можно не говорить, а Закревского Геннадий Петрович почитал как своего учителя, под руководством которого он участвовал в разработке одного из первых отечественных языков моделирования работы электронных схем. Кафедра никогда не была многочисленной, и меня поразило, что Геннадий Петрович сам читал до восьми различных дисциплин в одном семестре. При этом у него хватало энергии на «семейное» проведение дня начала учебы, дня образования кафедры и многих других ярких, не входящих в учебный план мероприятий, о которых потом многие студенты вспоминали как о чём-то главном, повлиявшем на их дальнейшее отношение к специальности. Созданная при его непосредственном участии команда SiBears из ТГУ трижды завоевала первое место в общероссийском соревновании CTF по компьютерной безопасности. Многие из его учеников впоследствии защитили диссертации в области дискретной математики. При его энергичном участии в университете был образован диссертационный совет по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность», один из трёх в стране, проводивший защиты по физико-математическим наукам, в котором прошло несколько успешных защит кандидатских и докторских диссертаций.

Вкладывая всю душу в организацию учебной и научной работы, Геннадий Петрович был непреклонен в своём нетерпимом отношении ко всякому формальному и бюрократическому отношению к главному делу его жизни. Будучи патриотом, глубоко переживая за будущее страны, чувствуя несправедливость навязываемых реформ в области образования и науки, он пытался в своей работе сохранить главное, подхватить и развить полезное новое и противостоять всему наносному и конъюнктурному. Понятно, что такой «неуживчивый» характер создавал много трудностей прежде всего для самого Геннадия Петровича, но несмотря ни на что он продолжал поступать так, как считал единственно возможным и как поступал всю свою жизнь.

Г. П. Агибалов вписал славную страницу в историю Томского государственного университета, и память о нём сохранится у всех коллег и учеников, а также многочисленных участников Всероссийской школы-семинара в области криптографии и компьютерной безопасности.

Чернушенко Ю. (выпускник кафедры ЗИК)

Для меня Геннадий Петрович стал маяком в учёбе. Он бескомпромиссно смотрел в суть вещей и учил этому других. Его увлечённость и лихость заражали студентов, а амбициозность задач и достижений вызывали уважение. Он был многогранный — но простой, острый — но добрый, умный — но весёлый. Я горжусь тем, что был его учеником, и он остаётся в моём сердце.

Шурупов А. Н. (к.ф.м.н., Москва)

В моей памяти остался жизнерадостный и добрый наставник молодежи, душа компании и глубокий собеседник.

Юфит Я. Г. (ученик, затем коллега Геннадия Петровича, Лондон)

Мне посчастливилось познакомиться с Геннадием Петровичем будучи студентом первого курса, в старом спортивном зале университета по ул. Никитина, 4, когда я начал заниматься спортивной гимнастикой. В зале моё внимание привлёк серьезный и сосредоточенный, крепкого сложения молодой человек, явно старше студенческого возраста. Он аккуратно и красиво работал на снарядах и практически ни с кем не общался. Позже мне сказали, что это молодой кандидат физико-математических наук Агибалов Гена (Геннадий Петрович).

Вторая знаковая встреча состоялась на лекции «Введение в специальность» для студентов второго курса общего потока радиофизического факультета, где ведущие преподаватели рассказывали о различных направлениях научных исследований, осуществляемых на факультете и в Сибирском физико-техническом институте. Мне очень понравилась манера чтения лекции Г. П. Агибалова: неторопливая, приглашающая к совместному рассуждению. Он рассказывал о дискретной математике и о конечных автоматах, совершенно незнакомых мне разделах математической науки и кибернетики. Заинтригованный, я выбрал одну из курсовых работ, предложенных Г. П. Агибаловым, и в дальнейшем не разочаровался в выборе.

Геннадий Петрович учил меня (и не только) лаконично, точно и грамотно излагать свои мысли не только устно, но и письменно. И если мне удалось чего-то достичь в научной работе, то в этом, несомненно, значительный вклад моего руководителя.

Конечно, можно много говорить, как азартно Геннадий Петрович играл в футбол, о его стихах, о его порядочности и принципиальности, иногда граничащей с жёсткостью, но пусть это осветят другие его ученики, коллеги и друзья.

В моей памяти Геннадий Петрович Агибалов навсегда живой.

Янковская А. Е. (д.т.н., сокурсница Геннадия Петровича)

С Геной Агибаловым я знакома со студенческих лет — мы учились в одной группе радиофизического факультета Томского государственного университета.

У нас был замечательный руководитель курсовых работ — всемирно известный ученый Закревский Аркадий Дмитриевич, Человек с большой буквы. Его мудрость иллюстрирует такая ситуация. Однажды Закревский дал нам с Геной одну и ту же тему курсовой работы, естественно, не сообщив нам об этом. Выполнив работу независимо друг от друга, каждый из нас получил отличную оценку. В результате было получено два решения на основе разных подходов и теорем. Главное, что ни Гена, ни я не знали, что работаем над одной задачей. Мыслимо ли сейчас, чтобы в одной группе студенты, имеющие одну и ту же тему курсовой работы, не общались в научном плане и не обсудили её решение?

С Геной мы одновременно были аспирантами Закревского, успешно завершили и вовремя защитили диссертационные работы уже на совершенно разные темы. При этом мы участвовали в выполнении хоздоговорной работы с ЦКБ «Алмаз», где Аркадий Дмитриевич был научным руководителем, а я — ответственным исполнителем.

Несмотря на научный потенциал, характер у Гены был поистине невыносимый. Не обошло это и меня. Я сформулировала и доказала ряд теорем, которые использовались при создании алгоритма компоновки схем в модули ограниченной вместимости. Агибалов вышел из себя по поводу того, что теоремы не верны и их нельзя использовать. Естественно, на мои ошибки он не указывал. После такого неоднократного и активного обсуждения мы перестали разговаривать. Встречает как-то меня профессор Феликс Петрович Тарасенко: «Аня, не могу понять, ты с Агибаловым не общаешься уже несколько лет. Каким образом у вас вышла совместная статья в журнале «Управляющие системы и машины»?» — Отвечаю: «Я эту статью не писала, и

Гена об этой статье мне не говорил». Гена понял, что он не прав, и включил мои результаты в статью. Будучи честным и порядочным в научном плане, он указал меня соавтором.

После моего ухода из отдела кибернетики СФТИ при ТГУ общение наше возобновилось только лет через 10. Я участвовала в руководимых им научных конференциях, в событиях, посвящённых приезду коллег, работающих совместно в отделе кибернетики, или коллег в научном плане. Например, последний приём был связан с приездом Поттосиных из Минска.

Гену я запомню, прежде всего, как высоко порядочного человека, всемирно известного и талантливого учёного. Он был одним из немногих коллег, с кем хотелось бы обсуждать научные результаты. Обладая глубокими знаниями в области математики, Гена мог дать весьма полезный совет. Я никогда не опасалась, что он мог бы использовать мои идеи в своих интересах.

На нашем курсе было много талантливых во всех отношениях студентов из деревень, таким был и Гена Агибалов. Кроме потенциала в научной области, Гена был известным гимнастом и писал великолепные стихи. Только человек, способный на глубочайшие переживания, может создать строки, после которых хочется плакать.

Гена Агибалов был хорошим человеком и многогранной личностью. Все мы ещё долго будем вспоминать о каждом из его качеств.

Секция 1

# ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.772 DOI 10.17223/2226308X/14/1

## О ПОСТРОЕНИИ МАКСИМАЛЬНЫХ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ РОДА 3

Ю. Ф. Болтнев, С. А. Новоселов, В. А. Осипов

Описываются два метода построения максимальных гиперэллиптических кривых рода три над конечным полем, т. е. кривых, число точек на которых достигает верхнюю границу Хассе — Вейля — Серра. Рассматриваются кривые с уравнением $y^2 = x^7+ax^4 +bx$, допускающие декомпозицию на эллиптические кривые. В основе первого метода — построение пары суперсингулярных эллиптических кривых над простым полем, $j$-инвариант одной из которых равен 1728 или 0, а j-инвариант другой кривой также известен. По построенным эллиптическим кривым строится искомая максимальная гиперэллиптическая кривая над подходящим расширением простого поля. Этот метод не исчерпывает всех максимальных кривых, но даёт весьма эффективный алгоритм построения некоторых их семейств. Второй метод основан на факторизации многочленов Лежандра, которые представляют собой инварианты Хассе соответствующих эллиптических кривых в декомпозиции якобиана. Метод позволяет построить все возможные максимальные кривые для случая b = 1 и поля $F_{p^2}$, и мы применяем его для построения всех максимальных кривых для p 6 7151 и a 6= 0.

**Ключевые слова:** максимальная гиперэллиптическая кривая, суперсингулярная эллиптическая кривая, характеристический многочлен.

Максимальные кривые, т. е. кривые с максимально возможным числом точек, достигающим верхнюю границу Хассе — Вейля — Серра, находят широкое применение как в криптографии, так и в теории алгебраических кодов. Пусть $C : y^2 = = x^7 + ax^4 + bx$ – гиперэллиптическая кривая рода 3 над конечным полем $F_q$, $q = p^n$, $p > 3$. В случае, когда b – кубический вычет, якобиан $J_C$ этой кривой допускает декомпозицию на эллиптические кривые, что описывается следующей теоремой, ранее доказанной авторами в [1].

**Теорема 1** [1]. Пусть $C : y^2 = x^7 + ax^4 + bx$ – гиперэллиптическая кривая рода 3, определённая над конечным полем $F_q$, $q = p^n$, $p > 3$, и b – кубический вычет. Тогда:

1) Если $q = 1 \pmod 6$, то $J_C \sim E_1 \times E_2$ над $F_q$ и $x_{C,q}(T) = (T^2 - t_1T + q)(T^2 - t_2T + q)^2$, где $E_1 : y^2 = x^3 + ax^2 + bx$, $E_2 : y^2 = x^3 - 33/bx + a$ – эллиптические кривые; $t_1, t_2$ – их следы Фробениуса.
2) Если $q = 5 \pmod 6$, то $J_C \sim E_1 \times E_2 \times E_2$ над $F_q$ и $x_{C,q}(T) = (T^2 - t_1T + q)(T^2 - t_2T + q)(T^2 + t_2T + q)$, где $E_2$ – скручивание кривой $E_2$.

Для установления соотношения между $j$-инвариантами эллиптических кривых $E_1$ и $E_2$ нами доказана следующая теорема.

**Теорема 2.** Пусть заданы две эллиптические кривые над полем $K$:

$$E_1 : y^2 = x^3 + ax^2 + bx,\ E_2 : y^2 = x^3 - 3\beta bx + a.$$

Тогда справедливы следующие соотношения для их $j$-инвариантов:

$$j(E_1) = \frac{2^8 \cdot 256(a^2 - 3b)^3}{b^2(a^2 - 4b)}; \qquad j(E_2) = \frac{4 \cdot 1728b}{a^2 - 4b};$$

$$j(E_1) = \frac{4}{27}\left(28 - \frac{4}{j(E_2)}\right)^3$$

**1. Максимальные кривые в случае $j(E_1) = 0$ или $j(E_1) = 1728$**

**Следствие 1.** Справедливы следующие утверждения:

1) $j(E_1) = 0 \Leftrightarrow j(E_2) = 4 \cdot 1728$;
2) $j(E_1) = 1728 \Leftrightarrow j(E_2) = 1728$ или $j(E_2) = -8 \cdot 1728$.

**Замечание 1.** Случай $j(E_1) = j(E_2) = 0$ невозможен, так как тогда дискриминант многочлена $x^7 + ax^4 + bx$ обращается в нуль и кривая $C$ будет не гладкой.

Кривая $C$, заданная над $F_q$, называется максимальной кривой, если число точек на кривой $N = 1 + q + g\lfloor 2\sqrt{q} \rfloor$, то есть достигается верхняя граница Хассе – Вейля – Серра:

$$1 + q - g\lfloor 2\sqrt{q} \rfloor \le N \le 1 + q + g\lfloor 2\sqrt{q} \rfloor.$$

Аналогичная граница известна также для якобианов [2, Theorem 14.15]:

$$(\sqrt{q} - 1)^{2g} \le |J_C(F_q)| \le (\sqrt{q} + 1)^{2g}.$$

Если $C$ – максимальная кривая, то $|J_C| = (1 + \lfloor 2\sqrt{q} \rfloor + q)^g$. Таким образом, порядок якобиана максимальной гиперэллиптической кривой рода $3$ равен

$$|J_C(F_q)| = (1 + \lfloor 2\sqrt{q} \rfloor + q)^3.$$

Это, в свою очередь, означает, что характеристический многочлен кривой имеет вид

$$\chi_{C,q}(T) = (T^2 + \lfloor 2\sqrt{q} \rfloor T + q)^3.$$

Тогда для гиперэллиптической кривой $C : y^2 = x^7 + ax^4 + bx$ рода 3, определённой над конечным полем $F_q$, $q = p^n$, $p > 3$, выполняется

$$J_C \sim E_1 \times E_2,$$

где $E_1 : y^2 = x^3 + ax^2 + bx$, $E_2 : y^2 = x^3 - 3\alpha x + a$ – эллиптические кривые, заданные над $F_q$. Их характеристические многочлены:

$$\chi_{E_1,q}(T) = \chi_{E_2,q}(T) = T^2 + \lfloor 2\sqrt{q} \rfloor T + q.$$

Заметим, что в случае рассмотрения суперсингулярных эллиптических кривых над простым полем имеем

$$X_{E1,P}(T) = X_{E2,P}(T) = T^2 + \mathrm{P}.$$

Согласно методу Вейля [3] для вычисления числа точек эллиптической кривой, число точек кривой $E$ над произвольным расширением $F_q$, $q = p^r$, равно

$$N_r = p_r + 1 - a_r - e_r.$$

Здесь $a$ и $в$ — корни характеристического многочлена, который в случае суперсингулярных над полем $F_p$ кривых $E_1$ и $E_2$ равен $XE/_{F_p}(T) = T_2 + p$. Нетрудно видеть, что

$$a_r + в^r = (i^{py} + (-i^{py} = \begin{cases} -2p^{r/2}, & r = \pm 1 \pmod 4, \\ I\,2p^{r/2}, & r = 2 \pmod 4, \\ 0, & r = 0 \pmod 4. \end{cases}$$

Таким образом, имеем

$$p^r + 1, \quad r = \pm 1 \pmod 4,$$
$$p^r + 1 + 2p^{r/2}, \quad r = 2 \pmod 4,$$
$$p^r + 1 - 2p^{r/2}, \quad r = 0 \pmod 4.$$

Видно, что число точек будет максимально при $r = 2 \pmod 4$, и кривая является максимальной, так как достигается верхняя граница Хассе — Вейля — Серра. Можно заметить, что

$$N_r = p_r + 1 + 2p^{r/2} = 1 + 2_v'q + q = X_E(1) \wedge X_E(T) = T_2 + b2^{qR} + q.$$

Таким образом, для построения максимальной гиперэллиптической кривой нужно построить суперсингулярные эллиптические кривые $E_1$ и $E_2$ над простым полем $F_p$ и рассмотреть их в расширении степени $r = 2 \pmod 4$.

С л у ч а й 1 . Будем искать кривую $E_2$ в виде $y^2 = x^3 + Ax$. Заметим, что $j$-инвариант такой кривой $j(E_2) = 1728$. Согласно следствию 1, получаем $j(E_1) = 1728$.

Из [3] известно, что эллиптическая кривая данного вида суперсингулярна над простым полем в случае, когда $p = 3 \pmod 4$. Это равносильно $p = 7, 11 \pmod{12}$ при $p > 3$.

Напомним, что $E_2 : y^2 = x^3 - 3\text{-}3^{/}bx + a$, тогда из сравнения коэффициентов получим $a = 0$, $b = -A^3/27$. Имеем искомое уравнение максимальной гиперэллиптической кривой:

$$C : y^2 = x^7 + ax^4 + bx = x^7 - \frac{A^3}{\sim^x}.$$

Таким образом, перебрав все коэффициенты $A\,G\,F_p$, построим семейство максимальных гиперэллиптических кривых над расширением $F_q$, соответствующих эллиптической кривой $E_2$ вида $y^2 = x^3 + Ax$, где $q = p^r$; $p > 3$; $p = 7, 11 \pmod{12}$; $r = 2 \pmod 4$.

С л у ч а й 2 . Будем искать кривую $E_1$, такую, что $j(E_1) = 1728$. По следствию из теоремы 2, $j(E_2) = 1728$ или $j(E_2) = -8 \cdot 1728$. Но случай $j(E_1) = j(E_2) = 1728$ мы уже рассмотрели, поэтому теперь рассмотрим случай $j(E_1) = 1728$ и $j(E_2) = -8 \cdot 1728$.

По известному методу (например, [4]) находим уравнение кривой $E_2$ по заданному $j$-инварианту:

$$E_2 : y^2 = x^3 - \frac{x}{3} + \frac{}{9}.$$

Отсюда $a = 16/9$, $b = (8/9)^3$, и получаем уравнение максимальной гиперэллиптической кривой:

$$C : y^2 = x^7 + ax^4 + bx = x^7 + \frac{}{}x^4 + \text{—}xx.$$

$$9 \qquad 9_3$$

Перебором классов изоморфизма кривых $E_2$ мы получили, что кривая $E_2$ суперсингулярна при $p = 31, 131, 251, 383, 439, 1459, 1999, 2203, 2999, 3299, 4523, 4759, 5399, 5471, 8719, 9323, \ldots$ При этом все кривые, изоморфные суперсингулярной кривой $E_2$, будут тоже суперсингулярны. Их можно получить следующим образом:

$$E_2 : y_2 = x_3 - -u_4x + \frac{}{39}u_6,\ u \in F_p.$$

Сравнивая с уравнением $y^2 = x^3 - 3/bx + a$, получаем коэффициенты

$$a=196\ u^6,\ b=9_3\ u_{12}-$$

Имеем следующее уравнение для семейства максимальных гиперэллиптических кривых:

$$C : y^2 = x^7 + \frac{}{9}u^6x^4 + \wedge -u^{12}x_{9_3}$$

Кривая $E_2$, являющаяся скручиванием кривой $E_2$, будет суперсингулярной в случае, когда $E_2$ суперсингулярна. Кроме того, весь класс кривых, изоморфных кривой $E_2$, состоит из суперсингулярных кривых. Уравнение кривых, полученных скручиванием кривой $E_2$, выглядит следующим образом:

$$E_2 : y = x - u_2xx + \frac{8}{}\sim\wedge u\ .$$

Сравнивая с уравнением $y^2 = x^3 - 3/bx + a$, получаем коэффициенты

$$a=196\ u^3\ b=9_3\ u^6.$$

Тогда имеем следующее уравнение для семейства максимальных гиперэллиптических кривых:

$$C : y^2 = x^7 + \frac{}{9}u^3x^4 + \wedge -u^6x.$$

С л у ч а й 3 . Будем искать кривую $E_1$, такую, что $j(E_1) = 0$. По следствию из теоремы 2 имеем $j(E_2) = 4 \cdot 1728$. Так как $j(E_1) = 0$, кривая $E_1$ суперсингулярна в случае, когда $p = 2 \pmod 3$, что равносильно $p = 5 \pmod 6$, когда $p > 3$. Аналогично случаю 2, по заданному $j$-инварианту $j(E_2)$ находим уравнение кривой $E_2$:

$$E_2 : y^2 = x_3 - 4x + \frac{8}{3}.$$

Отсюда $a = 8/3$, $b = (4/3)^3$, и уравнение максимальной гиперэллиптической кривой принимает следующий вид:

$$_3C : y^2 = x^7 + |x^4 + \wedge r\text{-}x_{3_3}$$

Перебор классов изоморфизма кривых $E_2$ показал, что кривая $E_2$ суперсингулярна при $p = 359\ 647\ 719\ 971\ 4391\ 6263\ 6983\ \ldots$ При этом все кривые, изоморфные суперсингулярной кривой $E_2$, будут тоже суперсингулярны. Их можно получить следующим образом:

$$E_2 : y^2 = x_3 - 4u_4x + \frac{}{3}u^6,\ u \in F_p.$$

Имеем следующее уравнение для семейства максимальных гиперэллиптических кривых:

$$C \blacksquare 'll^2 — T^{3\,4\,8}?6m4\ \text{-I-} — ?/1^2\text{T}$$
$$\text{C} : y — \text{x} + \text{u x} + \text{^3 u x}.$$

Кривая $E_2$, являющаяся скручиванием кривой $E_2$, будет суперсингулярной в случае, когда $E_2$ суперсингулярна. Кроме того, весь класс кривых, изоморфных кривой $E_2$, состоит из суперсингулярных кривых.

Уравнение кривых, полученных скручиванием кривой $E_2$, выглядит следующим образом:

$$Ee_2 : y^2 — x^5 — 4u^2x + -u^3.$$
$$3$$

Тогда получаем уравнение для семейства максимальных гиперэллиптических кривых:

$$C \blacksquare Ц^2 — 8\ 3\ 8\text{-}11^3\text{'}?^{6\ 7}\ \text{-I-}\ ^4\ 7/^6\text{T>}$$
$$\text{C} : y — \text{x} + — \text{u x} + \text{^|3 u x}.$$

**Пример 1.** Построим семейство максимальных гиперэллиптических кривых рода 3, заданных над полем $F_{31}$. Они являются максимальными над его расширением степени 2, то есть над полем $F_{961}$. Для данного поля якобиан максимальной гиперэллиптической кривой должен иметь порядок

$$(\text{Vq} + 1)^{2g} — (\text{V961} + 1)^6 — (32)^6 — 2^{30} — 1073741824.$$

При этом характеристические многочлены всех кривых над полем $F_{961}$ имеют вид $Xc,_{961}(x) — (x + 31)^6$, а для этих же кривых, рассматриваемых над полем $F_{31}$,— $\text{Xc}_{,31}(\text{x}) — (x^2 + 31)^3$. Далее приведены 20 максимальных гиперэллиптических кривых; кривые в левом столбце построены как в случае 1, в правом — как в случае 2:

| | |
|---|---|
| $y^2 — x^8 + 4x$ | $y^2 — x^7 + 14x^4 + 16x$ |
| $y^2 \quad 7 + 2x$ | $y^2 \quad 7 + 3x^4 + 2x$ |
| $y^2 \quad 7 + 30x$ | $y^2 \quad 7 + 19x^4 + x$ |
| $y^2 \quad 7 + 27x$ | $y^2 \quad 7 + 17x^4 + 16x$ |
| $y^2 \quad 7 + 15x$ | $y^2 \quad 7 + 24x^4 + 4x$ |
| $y^2 \quad 7 + 29x$ | $y^2 \quad 7 + 6x^4 + 8x$ |
| $y^2 \quad 7 + 8x$ | $y^2 \quad 7 + 12x^4 + x$ |
| $y^2 \quad 7 + 23x$ | $y^2 \quad 7 + 25x^4 + 8x$ |
| $y^2 \quad 7 + x$ | $y^2 \quad 7 + 28x^4 + 2x$ |
| $y^2 \quad 7 + 16x$ | $y^2 \quad 7 + 7x^4 + 4x$ |

---

**2 Максимальные кривые вида $y^2 — x^7 + ax^4 + x$ над $F_{p^2}$**

за время $O(\log^4 q)$ битовых операций с помощью теоремы 1 с использованием алгоритма Схоофа— Элкиса — Аткина для вычисления следов Фробениуса. Для заданной характеристики $p$ все кривые p-ранга 0 вида $y^2 — x^7 + ax^4 + x$ могут быть найдены построить максимальные кривые — найти сначала все кривые p-ранга 0, а затем вы

Для группы точек p-кручения якобиана кривой выполняется $Jc\,[p_s]\,' Z/p^{ts}Z$, где число t, 0 6 t 6 3, не зависит от s и называется p-рангом кривой [2, с. 61]. Известно, что

все максимальные кривые имеют p-ранг 0 [5, Corollary 5]. Поэтому один из способов

брать среди них максимальные. Проверка на максимальность может быть выполнена

с помощью матрицы Картье — Манина кривой, так как её ранг равен p-рангу. Структура матриц Картье — Манина нашей кривой описана в [6]. Для кривой над полем $F_{p^2}$ матрица Картье — Манина имеет вид

$$\begin{matrix} P_{(p-6)/2}(-a/6)^{p+1} & 0 & 0 \\ 0 & P_{(p-1)/2}(-a/2)^{p+1} & 0 \\ 0 & 0 & P_{(p-1)/6}(-a/6)^{p+1} \end{matrix}$$

для случая, когда $p = 1 \pmod 3$, и

$$\begin{matrix} M_{-5)/2}(-a/6)^{p+1} & 0 & 0 \\ 0 & P_{(p-1)/2}(-a/2)^{p+1} & 0 \\ 0 & 0 & P_{(p-5)/6}(-a/6)^{p+1} \end{matrix} \quad \backslash$$

для случая, когда $p = 2 \pmod 3$. Здесь $P_m(x)$ — многочлен Лежандра степени $m$. Поэтому p-ранг кривой $y^2 = x^7 + ax^4 + x$ равен $0$ тогда и только тогда, когда $-a/2$ является корнем многочлена $L_1(-a/2) = \gcd P_{(p-1)/2}, P_{(p-1)/6}$ для $p = 1 \pmod 3$ или $L_2(-a/2) = \gcd P_{(p-1)/2}, P_{(p-5)/6}$ для $p = 2 \pmod 3$. Таким образом, для фиксированного $p$ мы можем найти все кривые p-ранга $0$ с помощью факторизации многочленов $L_1, L_2$ либо доказать, что таких кривых не существует ($L_1$ или $L_2$ в этом случае — константы).

Сложность метода. Построить многочлен Лежандра $P_m(x)$ можно по известным $(m \backslash i = O(m(m+1))$ операций в поле. Нахожде- $i=1$ ние наибольшего общего делителя для многочленов степени не больше $(p-1)/2$ занимает время $O((p-1)/2)$ операций в поле [7, с. 325]. Факторизация многочленов $L_1$ и $L_2$ может быть выполнена [7, с. 390] за время $O(bp/6c^2 \log p)$ операций в поле, учитывая, что $\deg L_1 6 (p-1)/6$ и $\deg L_2 6 (p-5)/6$. Проверка на максимальность занимает время $O(\log^4 q)$. Предполагая, что количество проверяемых кривых небольшое, получаем в итоге эвристическую сложность в $O(p^2 \log^2 p)$ битовых операций. При этом нахождение всех максимальных кривых простым перебором коэффициентов занимает время $Oe(p^2 \log^4 p)$.

Используя полученный метод, мы построили все максимальные кривые над полем $F_{p^2}$ с параметром $a\,6 = 0$ (случай $a = 0$ изучен в [8, § 4]) для $p\,6\,7151$ и определили поля, над которыми таких кривых не существует. Данные по количеству максимальных кривых для $p < 200$ представлены в таблице. Полные данные с явными уравнениями максимальных кривых можно найти на домашней странице второго автора[1].

Число максимальных кривых вида $y^2 = x^7 + ax^4 + x$ над $F_{p^2}$, $3 < p < 200$, $a\,6 = 0$

| p | Кол-во |
|---|---|
| 5-29, 37-43, 53, 61, 67, 73, 89-101, 107-127, 137-163, 173-181, 193, 197 | 0 |
| 31,47, 59, 79, 83 | 2 |
| 71,103,131,167 | 4 |
| 191,199 | 6 |

[1] http://crypto-kantiana.com/semyon.novoselov/genus3/maximal_curves

ЛИТЕРАТУРА


1. Novoselov S. A. and Boltnev Y. F. Characteristic polynomials of the curve $y^2 = x^{2g+1} + ax^{g+1} + + bx$ over finite fields // Прикладная дискретная математика. Приложение. 2019. № 12. С.44-46.
2. Cohen H. and Frey G. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall/CRC, 2006.
3. Blake I. F., Seroussi G., and Smart N. P. Elliptic Curves in Cryptography. Cambridge University Press, 1999.
4. Menezes A. Elliptic curve public key cryptosystem. Kluwer Academic Publ., 1993.
5. Tafazolian S. A family of maximal hyperelliptic curves // J. Pure Appl. Algebra. 2012. V. 216. No. 7.

P. 1528-1532.
6. Novoselov S. A. Hyperelliptic curves, Cartier — Manin matrices and Legendre polynomials // Прикладная дискретная математика. 2017. № 37. С. 20-31.
7. Von zur Gathen J. and Gerhard J. Modern Computer Algebra. Cambridge University Press, 2013.
8. Kodama T., Top J., and Washio T. Maximal hyperelliptic curves of genus three // Finite Fields Their Appl. 2009. V. 15. No. 3. P. 392-403.

УДК 519.214 DOI 10.17223/2226308X/14/2

# ЦЕНТРАЛЬНАЯ ПРЕДЕЛЬНАЯ ТЕОРЕМА ДЛЯ U -СТАТИСТИК ОТ ЦЕПОЧЕК МЕТОК ВЕРШИН НА ПОЛНОМ ГРАФЕ

2. М. Меженная, В. Г. Михайлов

В полном графе с вершинами 1, 2, . . . , n вершины 2, 3, . . . , n снабжены независимыми случайными метками, принимающими значения из конечного множества $A_N$ . Рассматривается совокупность всех цепей по s смежных рёбер, каждая из которых выходит из вершины 1 и не проходит через одну и ту же вершину дважды. Каждой цепи соответствует s-цепочка из случайных меток пройденных вершин. Рассматривается U-статистика $U_k(s)$ с ядром, зависящим от $\kappa$ таких s-цепочек. Число $k > 2$ считается фиксированным, а $s > 1$ может меняться. Установлено, что достаточным условием асимптотической нормальности $U_k(s)$ (при обычной стандартизации) является условие вида $DU_k(s) > C\, n^{2(ks-1)+\kappa}$, где $C, \kappa > 0$.

**Ключевые слова:** U -статистика, центральная предельная теорема, полный граф, цепочка, случайные метки.

Исследование свойств выборочных характеристик и статистических критериев привело к необходимости изучения распределений функционалов от последовательностей случайных величин $X_1, \ldots, X_n$ вида

$$U_n = U_n(X_1,\ldots,X_n) = \sum_{1 \le j_1 < \ldots < j_r \le n} f(X_{j_1},\ldots,X_{j_r}), \qquad (1)$$

называемых U -статистиками [1]. Число r называется порядком U -статистики. Функционалы вида (1) широко используются для проверки свойств случайных последовательностей, качества датчиков псевдослучайных чисел, наличия или отсутствия зависимости между членами последовательности, наличия образцов или повторений специального вида и в задачах, связанных с защитой информации.

Основные результаты об асимптотическом поведении распределений U -статистик с непрерывными ядрами можно найти в [2]. Результаты для U -статистик от дискрет

ных последовательностей, например для числа пар одинаковых знаков, пар одинаковых цепочек и пар эквивалентных цепочек, получены в [3] и [4] соответственно.

В работе [5] установлено, что для последовательности случайных величин, удовлетворяющей условию абсолютной регулярности [6] с коэффициентом $\beta(t) \le t^{-h(t)}$, где $h(t) > 0$ и $h(t) \to \infty$ $(t \to \infty)$ (например, для цепи Маркова), достаточным условием асимптотической нормальности является условие на дисперсию $\mathbf{D}U_n > Cn^{2(r-1)+\kappa}$, где $\kappa > 0$. Разумеется, это относится и к последовательности независимых случайных величин. Как известно [3], в последовательности независимых одинаково распределённых случайных величин на конечном алфавите при их неравновероятном распределении число $k$-кратных повторений $s$-цепочек имеет дисперсию порядка $n^{2k-1}$ и сходится (при подходящей стандартизации) по распределению к нормальному распределению при $n \to \infty$.

В настоящей работе приведён аналогичный результат для $U$-статистики от цепочек меток вершин на полном графе.

Введём несколько определений. Пусть $K_n$ — полный граф с $n$ вершинами из множества $V = \{1,\dots, n\}$ и с $\Pi$ рёбрами; $a_2,\dots,a_n$ — независимые в совокупности случайные величины, принимающие значения из множества $A_N = \{0, 1, \dots, N-1\}$, причём

$$P[a_j = k] = p_k \in (0; 1), k \in A_N, \qquad \sum_{k=0}^{N-1} p_k = 1.$$

Далее будем считать, что $a_j$ — метка вершины с номером $j$, $j \in V \setminus \{1\}$.

Обозначим через $\{w(s)\}$ цепь (связный путь без повторения рёбер) из $s > 1$ рёбер в графе $K_n$, начинающийся из вершины с номером 1, не имеющей метки, и не проходящий через одну и ту же вершину дважды. Обозначим через $a(\{w(s)\})$ соответствующую цепи $\{w(s)\}$ последовательность из $s$ меток вершин, через которые проходит цепь (с учётом их порядка). Число таких путей равно числу способов выбрать оставшиеся $s$ вершин из $n-1$ вершин графа (кроме вершины с номером 1) с учётом порядка, $\frac{(n-1)!}{(n-s-1)}$ поэтому в $K_n$ всего $T = A_{n-1}^{s}$ цепей длины $s$ с требуемыми свойствами. Занумеруем их и будем писать $\{w_u(s)\}$, $u = 1, \dots, T$.

Пусть $f$ — ограниченная по абсолютной величине константой $F$ функция от $k > 2$ $s$-мерных векторных аргументов, симметричная относительно их перестановки. Рассмотрим $U$-статистику вида

$$U_k(s) = \sum_{1 \le u_1 < \dots < u_k \le T} f(a(\{w_{u_1}(s)\}),\dots, a(\{w_{u_k}(s)\})). \qquad (2)$$

Здесь аргументами функции $f$ выступают последовательности из $s$ меток вершин, образованных цепями рассматриваемого вида в $K_n$.

Обозначим $N(0; 1)$ стандартный нормальный закон распределения; $\xrightarrow{d}$ — сходимость по распределению.

**Теорема 1.** Пусть число $k > 2$ фиксировано, $s > 1$. Если $\mathbf{D}U_k(s) > Cn^{2(s-1)+\kappa}$, где $C, \kappa > 0$, то

$$\frac{U_k(s) - \mathbf{E}U_k(s)}{\sqrt{\mathbf{D}U_k(s)}} \xrightarrow{d} N(0;1), \text{ то}$$

Теорема 1 сводит доказательство асимптотической нормальности для таких U-статистик, как число повторений цепочек в последовательности дискретных случайных величин, к проверке скорости роста их дисперсий. В ряде случаев это упрощает обоснование их использования в практических задачах (примеры см. в [7]).

Для доказательства теоремы 1 использовался топологический вариант метода моментов, предложенный в [8].

ЛИТЕРАТУРА


1. Hoeffding W. A class of statistics with asymptotically normal distribution // Ann. Math. Statist. 1948. Vol. 19. No.3. P. 293-325.
2. Королюк В. С., Боровских Ю. В. Теория U -статистик. Киев: Наук. думка, 1989.
3. Михайлов В. Г. Центральная предельная теорема для числа неполных данных повторений // Теория вероятн. и ее примен. 1975. Т. 20. Вып. 4. С. 880-884.
4. Шойтов А. М. Нормальное приближение в задаче об эквивалентных цепочках // Тр. по дискр. матем. 2007. Т. 10. С. 326-349.
5. Mikhailov V. G. and Mezhennaya N. M. Normal approximation for U- and V -statistics of a stationary absolutely regular sequence // Sib. Elektron. Mat. Izv. 2020. V. 17. P. 672-682.
6. Doukhan P. Mixing: Properties and Examples. Lecture Notes in Statistics 85. N.Y.: Springer Verlag, 1994.
7. Rukhin A., Soto J., Nechvatal J., et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22r1a. Natl. Inst. Stand. Technol. Spec. Publ., 2010.
8. Janson S. Normal convergence by higher semiinvariants with applications to sums of dependent random variables and random graphs // Ann. Probab. 1988. V. 16. No. 1. P. 293-325.


УДК 519.1 DOI 10.17223/2226308X/14/3

# О НАИБОЛЬШЕМ ПОРЯДКЕ ПОДСТАНОВОК ЗАДАННОЙ СТЕПЕНИ

В. М. Фомичёв

Необходимым требованием к системе шифрования является достаточно большой порядок группы, которая ассоциируется с шифром (то есть порождается подстановками шифра). В связи с этим представляет интерес величина ^(n), оценивающая порядки циклических групп подстановок степени n, в том числе циклических групп, порождённых шифрующими подстановками. Известно, что порядок подстановки равен наименьшему общему кратному длин её циклов. Однако мало изучена функция ^(n), принимающая значения, равные наибольшему порядку подстановки степени n. Показана монотонность функции ^(n), получена двухсторонняя оценка её значений: $Q_{w(n)}$ 6 ^(n) 6 [*y/n*- - 1) p, где $П_{w(n)}$ произведение всех первых (в порядке возрастания) простых чисел, сумма которых не больше n. Получена асимптотическая оценка нижней границы при больших n:

$$Xn) > 224k!(1,665)k(\ln k)^{(k-15)/2}$$

при любом $n > 1000$ и $k = \lfloor p2n/\ln n \rfloor$ .

**Ключевые слова:** порядок подстановки, цикловая структура подстановки, простое число.

Каждая подстановка есть произведение независимых циклов. Если длины циклов подстановки g равны $l_1, \ldots, l_m$, то её порядок равен

$$\text{ord } g = \text{НОК}(l_i,\ldots,l_m).$$

Если в записи подстановки имеется $k_i$ циклов длины $l_i$, $i = 1, \ldots, m$, то это свойство записывается с помощью цикловой структуры $C(g)$ подстановки $g$:

$$C(g) = l_1^{[k_1]}, \ldots, l_m^{[k_m]}; \qquad (1)$$

эти числа связаны со степенью $n$ подстановки равенством

$$k_1 l_1 + \ldots + k_m l_m = n.$$

Далее считаем, что длины циклов упорядочены: $l_1 < \ldots < l_m$.

Обозначим:

– $S_n$ – группа всех подстановок степени $n$;

– $S_n^{(m)}$ – множество всех подстановок степени $n$, состоящих из $m$ циклов, $1 \leq m \leq n$;

– $ORD_n = \{\text{ord}\, g : g \in S_n\}$;

– $\lambda(n) = \max\limits_{g \in S_n} \text{ord}\, g$;

– $g_{max}$ – подстановка $g \in S_n$, такая, что $\text{ord}\, g = \lambda(n)$.

Необходимым требованием к системе шифрования является достаточно большой порядок группы, которая ассоциируется с шифром (то есть порождается подстановками шифра). В связи с этим представляет интерес величина $\lambda(n)$, оценивающая порядки циклических групп подстановок степени $n$, в том числе циклических групп, порождённых шифрующими подстановками.

Тривиальные оценки для порядка подстановок из $S_n$ имеют вид

$$1 \leq \text{ord}\, g \leq n!,$$

где нижняя оценка достижима при любом $n$ для тождественной подстановки и верхняя оценка достижима лишь при $n \leq 2$.

Задача нахождения $\lambda(n)$ сводится к определению наибольшего значения НОК$(l_1, \ldots, l_m)$, где максимум берётся по всем разбиениям $n$-множества на $m$ непустых блоков порядков $l_1, \ldots, l_m$.

**Утверждение 1.** Функция $\lambda(n)$ монотонно неубывающая с ростом $n$.

Доказательство. Пусть $g = g_n^{max}$ и цикловая структура подстановки $g$ определена равенством (1). Возьмём подстановку $h \in S_{n+1}$ со свойством

$$C(h) = \begin{cases} l_1, \ldots, l_m, & l_1 = 1, \\ j_i, 1, l_1, \ldots, l_m, & l_1 > 1. \end{cases}$$

Отсюда $\lambda(n) = \text{ord}\, g = \text{ord}\, h \leq \lambda(n+1)$. ■

**Замечание 1.** Функция $\lambda(n)$ не является строго возрастающей. Например, $\lambda(5) = \lambda(6)$, так как

$$C(g_{max}) = \{2^{[1]}, 3^{[1]}\}, \quad \lambda(5) = 6,$$

$$C(g_{max}) = \{1^{[1]}, 2^{[1]}, 3^{[1]}\} \text{ или } C(g_{max}) = \{6^{[1]}\}, \quad \lambda(6) = 6.$$

**Утверждение 2.** Для любого $n > 1$

$$ORD_n \not\subseteq \{1, \ldots, n\}.$$

**Доказательство.** Следует из существования в $S_n$ подстановки $g_l$ с цикловой структурой $C(g_i) = \{1^{n-l}, l_{[1]}\}$, $l = 1,\ldots,n$. ■

Множество натуральных чисел $L = \{l_1, l_2, \ldots, l_m\}$, где $m > 1$ и $l_1 < \ldots < l_m$, назовём r-разреженным, $r > 0$, если $l_m - l_1 = m - 1 + r$; при $r = 0$ множество $L$ назовём сплошным. Множество натуральных чисел $L_0 = \{A_1, A_2, \ldots, A_m\}$ назовём 2-сжатием множества L, если положительны обе разности $A_1 - l_1$ и $l_m - A_m$, и 1-сжатием множества $L$, если одна из разностей $A_1 - l_1$ и $l_m - A_m$ положительна, а другая равна 0.

Обозначим: $\wedge(L) = l_1 + l_2 + \ldots + l_m$; $Z(L) = l_1 l_2 \ldots l_m$.

**Утверждение 3.** Для любого r-разреженного множества $L = \{l_1, l_2, \ldots, l_m\}$ имеется сплошное множество $L^0$, являющееся:

1) 2-сжатием множества $L$ при $r > 1$, таким, что $\wedge(L) \leq E(L_0)$ и $Z(L) < Z(L_0)$;

2) 1-сжатием множества $L$ при $r = 1$, таким, что $E(L) \leq E(L_0)$ и $Z(L) < Z(L^1)$.

Занумеруем простые числа в порядке возрастания: $p_1 = 2$, $p_2 = 3$, . . .

При $n > 1$ обозначим: $Q(n) = \{(p_{i_1}, \ldots, p_{i_r})\}$ – семейство всех множеств простых чисел, для которых $p_{i_1} + \ldots + p_{i_r} \leq n$, $r \leq n/2$, числа $i_1, \ldots, i_r$ натуральные; $\Pi(n) = \max p_{i_1} \ldots p_{i_r}$ – наибольшее (по всем наборам из $Q(n)$) значение произведения чисел $Q(n)$ набора.

**Теорема 1.** Для любого $n > 3$ верны оценки:

$$\Pi(n) \leq \wedge(n) \leq \wedge p2(n - 1)\ "|!.$$

**Доказательство.**

Для любого $n > 3$ и любого набора простых чисел $(p_{i_1}, \ldots, p_{i_r}) \in Q_n$ существует подстановка степени $n$, содержащая циклы длины $p_{i_1}, \ldots, p_{i_r}$. Порядок такой подстановки равен $p_{i_1} \ldots p_{i_r}$ в силу попарной взаимной простоты чисел набора. Нижняя оценка доказана.

Пусть подстановка $g$ степени $n$ порядка $\wedge(n)$ содержит циклы, множество длин которых есть $L = \{l_1, \ldots, l_m\}$. Если $E(L) = d < n$, то подстановка $g$ имеет два или более циклов одинаковой длины $l_r$, $r \in \{1, \ldots, m\}$, где $1 \leq l_r \leq n - d$. Тогда существует подстановка $h$ степени $n$ с множеством длин циклов $L_1 = \{l_1, \ldots, l_{m-1}, l_m + l_r\}$, при этом $Z(L) < Z(L_1)$. Отсюда получаем

$$\operatorname{ord} g = НОК(L) \leq Z(L) < Z(L_1).$$

Рассуждая аналогично, за конечное число шагов перейдём от подстановки $g$ к подстановке $g^0$ степени $n$, у которой длины всех циклов различные и $\operatorname{ord} g < n(L_0)$, где $L_0$ – множество длин всех циклов подстановки $g^0$. Значит, $\wedge(n)$ не превышает наибольшее значение $Z(L)$, где максимум берется по наборам $L$ для множества всех подстановок степени $n$ с различными длинами всех циклов.

В соответствии с утверждением 3, верхняя оценка $Z(L)$ достигается на одной из подстановок степени $n$, у которой множество длин циклов $L$ есть сплошное множество.

Оценим произведение $n(l,m) = (l + 1)\ldots(l + m)$ при условии, что числа $l$ и $m$ таковы, что $£(l,m) = (l + 1) + \ldots + (l + m)$ есть величина порядка $n + o(n)$, что не нарушает справедливость оценки $\operatorname{ord} g$ с помощью числа $n(l,m)$.

Суммируя арифметическую прогрессию, получаем

$$£(l, m) = (l + (m + 1)/2)m = n + o(n). \quad (2)$$

Если при фиксированном $l > 0$ взять $m =$ УЖ-) то

$$) > ^l,\ p2(n - l)) = n + p2(n - l)(l + 1/2) - l.$$

Тогда значение Я $1, ^2(n — 1)$ удовлетворяет (2) при $l = o(pn)$. Взяв $l = 1$, $m = p2(- — 1)$, получим

$$п\ (1, p2(п -1\ ]\ ) 6\ p2(п - 1)$$

Следовательно, $\operatorname{ord} g < ^2(n — 1)$

**Следствие 1.** При любом $n > 1000$ и $k =$ $^2n/\ln n$ верна нижняя оценка

$$^(n) > 224\ k!(1,665)_k(In\ k)^{(k-15)/2}.$$

Доказательство. Для получения ограничения снизу для $\operatorname{ord} g$ оценим произведение первых простых чисел, сумма которых не превышает $n$.

В соответствии с верхней оценкой Россера [2]

$$p_k < k \ln k + k \ln \ln k + 8k.$$

Заметим, что $p_1 + p_2 + p_{15} = 328$, $p_{16} = 53$. Следовательно, при любом $n > 381$ выполнено условие

$$S^{(\{P_1,P_2,...,P_k\})}\ 6^{n,} \qquad (3)$$

если $k > 16$, и условие

$$P\ r^(r)\ 6\ n — 328,$$

где $^(r) = \ln r + \ln\ln r + 8$. Так как при $r > 1$ функция $^(r)$ монотонно возрастает, то

$$\text{£ } r^{(H} < ^{(k)} \text{£ } r = ^{(k)} \frac{!к\text{-}^{к} — 15)(k + 16)}{2} - \text{--------}$$

Значит, условие (3) удовлетворено, если

$$»(k)< k_{-15} X k_{+16)}\ 6\ n - 328.$$

В частности, при $n > 1000$ и $16\ 6\ k\ 6$ $^2n/\ln n$ имеем

$$^(k) = ^\ln 2n - \frac{(k - 15)(k + 16)}{2} 6\ n\sim + \backslash - 120, \qquad (5)$$
$$\ln n\ 2 \ln n$$
$$- \ln \ln n + \ln(- \ln 2n - - In\ In\ n) + 8.$$

Заметим, что при $n > 1000$

$$- \ln 2n - - \ln\ln n \backslash +8 < 6{,}145 \bullet \ln\ln n,$$

тогда

$$\hat{}(k) < 2 \ln 2n + 5{,}645 \cdot \ln\ln n. \qquad (6)$$

Следовательно, при $n > 1000$ и $16 \le k \le \hat{}2n/\ln n$ из (4)-(6) получаем

$$\frac{n \ln 2n}{2 \ln n} + \ln 2nd \frac{\sqrt{n}}{60 \ln 2n + 5{,}645 \cdot \ln \ln n} \left( \frac{n}{\ln n} + A/ \frac{n}{2 \ln n} - 120 \right) \ge n - 328.$$

Так как при $n > 1000$ это неравенство выполнено, то условие (3) удовлетворено при
$16 \le k \le \hat{}2n/\ln n$ . Отсюда $Ш(П) > \hat{}2n/\ln n$ при $n > 1000$ и по теореме 1

$$\hat{}(n) > P_1 P_2 \ldots p_k$$

при указанных $k$. Оценим произведение простых чисел.

Обозначим константу $c_{15} = p_1 p_2 \ldots p_{15} = 614889782588491410$.

В соответствии с оценкой Россера $p_r > r \ln r$, где $r > 1$ [2], по теореме 1 при $n > 1000$
и $k = \hat{}2n/\ln n$ получаем

$$\hat{}(n) > C_{15} \prod_{r=16} r \ln r = \frac{C_{15Д}}{15!} \prod_{r=16} \ln r > 4{,}7 \cdot 10^5 k! \prod_{r=16} \ln r \qquad (7)$$

Функция $\ln r$ выпуклая вверх, тогда

$$(\ln r)^2 > \ln(r - h) \ln(r + h)$$

при любых $r > 1$ и $h < r$. Следовательно, при $k > 16$

$$\prod_{r=16} \ln r > (\ln 16)^{(k-15)/2} (\ln k)^{(k-15)/2}.$$

Заметим, что $д/\ln 16 > 1{,}665$ и $4{,}7\hat{} 10^5 (\ln 16)^{-15/2} > 224$. Отсюда и из (7) следует нужная оценка для $\hat{}(n)$. ■

В таблице приведены оценки и точные значения функции $\hat{}(n)$ для $n \le 12$.

| $n$ | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|
| Верхняя оценка | 6 | 6 | 24 | 24 | 24 | 24 | 120 | 120 | 120 |
| Точное значение, длины циклов $g_{max}$ | 4, 4 | 6, 2+3 | 6, 6 | 12, 3+4 | 15, 3+5 | 15, 1+3+5 | 30, 2+3+5 | 30, 1+2+3+5 | 60, 3+4+5 |
| Нижняя оценка по наборам простых чисел | 3, {3} | 6, {2,3} | 6, {2,3} | 10, {2,5} | 15, {3,5} | 15, {3,5} | 30, {2,3,5} | 30, {2,3,5} | 42, {2,3,7} |

ЛИТЕРАТУРА

1. Rosser B. The n-th prime is greater than n logn // Proc. London Math. Soc. 1939. V. 45. P. 21-44.

Секция 2

# ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 519.7 DOI 10.17223/2226308X/14/4

## ГИБРИДНЫЙ ПОДХОД К ПОИСКУ БУЛЕВЫХ ФУНКЦИЙ С ВЫСОКОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ НА ОСНОВЕ ЭВРИСТИЧЕСКИХ МЕТОДОВ[8]

Н. Д. Атутова

Предложен комбинированный подход к поиску булевых функций с высокой алгебраической иммунностью на основе эвристических методов, в частности генетического алгоритма и алгоритма Hill Climbing. Для булевых функций от n 6 8 переменных проведены вычислительные эксперименты, продемонстрировавшие эффективность предлагаемого подхода.

**Ключевые слова:** генетический алгоритм, алгоритм Hill Climbing, алгебраическая иммунность, нелинейность, эвристики.

Развивающийся интерес к криптоанализу повышает потребность в улучшении стойкости шифров. Для защиты от статистических и аналитических методов криптоанализа для построения компонент шифра необходимо использовать булевы функции, обладающие хорошими криптографическими характеристиками. В 2003 г. N. Courtois и W. Meier в [1] предложили новый метод криптоанализа шифров, названный алгебраическим криптоанализом. Высокая алгебраическая иммунность помогает противостоять такому криптоанализу.

Целью работы является построение булевых функций с максимальной алгебраической иммунностью — характеристикой, повышающей стойкость шифра к алгебраическим атакам.

Алгебраическая иммунность булевой функции $f$ ($\mathrm{AI}(f)$) — минимальное число $d$, такое, что существует булева функция $g$ степени $d$, не тождественно равная нулю, для которой выполняется равенство $fg = 0$ или $(f \oplus 1)g = 0$, где $f$ и $g$ — функции от равного числа переменных. Известно, что для любой функции $f$ от $n$ переменных справедливо $AI(f) \leqslant \lceil n/2 \rceil$.

Задача полного описания класса булевых функций, обладающих максимальной алгебраической иммунностью, а также получения новых конструкций таких функций является открытой проблемой.

Существует три способа нахождения функций с высокой алгебраической иммунностью: полный перебор, алгебраическое конструирование и эвристики. При росте числа переменных множество булевых функций растёт дважды экспоненциально, что ухудшает эффективность полного перебора. Алгебраическое построение заведомо сужает множество решений. Перспективным является подход, использующий эвристические

[8] Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования РФ № 075-15-2019-1613, и лаборатории криптографии JetBrains Research.

методы, в основе которых лежит структурированный перебор с параметрами для достижения желаемого результата.

Предлагается рассмотреть применение эвристических методов, в частности генетического алгоритма и алгоритма Hill Climbing. Специфика применения данных алгоритмов для поиска булевых функций с высокими значениями нелинейности впервые описана в [2]. Получены также теоретические результаты применения этих алгоритмов для функций от 16 переменных. Эффективность эвристических методов продемонстрирована в ряде работ: в [3] исследована возможность применения алгоритма имитации отжига для поиска функций с высокой нелинейностью и низкой автокорреляцией; в [4] реализован генетический алгоритм для поиска бент-функций и сбалансированных функций; в [5] приведены результаты применения гибридного генетического алгоритма для построения сбалансированной булевой функции с оптимальными криптографическими характеристиками.

Для достижения максимального значения алгебраической иммунности реализованы два алгоритма.

**Генетический алгоритм** (ГА) — это метод поиска, аналогичный естественному отбору в природе. Для получения более жизнеспособных потомков к особям из начальной популяции итерационно применяются скрещивание и мутация. Последовательно происходит полное обновление популяции потомками, обладающими наибольшими значениями целевой функцией. В терминах нашей задачи:

- особь — вектор значений булевой функции;
- начальная популяция — случайное множество особей, без ограничений;
- мутация — перестановка двух случайных различных битов вектора значений входной функции;
- целевая функция — алгебраическая иммунность;
- скрещивание — однородный кроссинговер. На вход поступают булевы функции $f$ и $g$, представленные векторами значений $(f_0, f_1, \ldots, f_{2^n-1})$ и $(g_0, g_1, \ldots, g_{2^n-1})$. На выходе — булева функция $h$, вектор значений $(h_0, h_1, \ldots, h_{2^n-1})$ которой определяется следующим образом: если $f_i = g_i$, то $h_i = f_i$; если $f_i \neq g_i$, то $h_i$ принимается равным $f_i$ или $g_i$ с одинаковой вероятностью, $i = 0, 1, \ldots, 2^{n-1}$.

Введём некоторые ограничения на скрещивание. Для этого нам потребуется расстояние Хэмминга.

Расстоянием Хэмминга $\mathrm{dist}(f, g)$ между булевыми функциями $f$ и $g$ называется число координат, в которых различаются их векторы значений.

Если $\mathrm{dist}(f, g) > 2^{n-1}$, то вместо вектора значений функции $g$ рассматривается вектор, полученный инверсией всех битов вектора значений функции $g$. В рамках работы вероятность выполнения операции скрещивания принималась равной $0{,}8$.

Далее в таблице представлены экспериментальные результаты применения генетического алгоритма для булевых функций при $n = 4, 6, 8$. Алгоритм повышает значения алгебраической иммунности до максимальной теоретической оценки для всех особей популяции. Подсчитано количество функций с максимальным значением целевой функции, получаемых на каждой итерации при каждом обновлении популяции.

**Hill Climbing** – итерационный алгоритм, который начинается с произвольного решения задачи, а затем пытается найти лучшее путём пошагового изменения одного из элементов решения. В рамках рассматриваемой задачи используется понятие нелинейности — характеристики, повышающей стойкость к линейному криптоанализу

[6]. Пре*образованием Уолша — Адамара* булевой функции $f$ называется функция $W_f$: $F_n \wedge Z$, где

$$W_f(y) = P(-1)^{f(x) \oplus h^{x,y}},\ y \in F_n\ hx,yi = X_1У_1 \Phi \ldots \Phi X_nY_n.$$

С помощью преобразования Уолша — Адамара можно вычислить нелинейность функ-

$$N_f = 2^{n-1} - \frac{1}{2} \max_{y \in n} |W_f(.<$$

При чётном числе переменных $n$ максимально возможное значение нелинейности равно $2^{n-1} - 2^{n/2-1}$. В случае нечётного $n$ точное значение максимальной нелинейности неизвестно.

Алгоритм для повышения нелинейности описан в [2]. На вход поступает вектор значений булевой функции. Алгоритм итеративно пытается улучшить нелинейность, изменяя одну из координат. На каждой итерации коэффициенты Уолша — Адамара разбиваются на множества и последовательно происходит проверка условий повышения значения целевой функции. В настоящей работе Hill Climbing применяется для поддержания высокой нелинейности после мутации потомков на каждой итерации генетического алгоритма.

Известно следующее соотношение, связывающее нелинейность и алгебраическую иммунность булевой функции [7]:

$$N_f > 2 \sum_{i=0}^{Al(f)-2}$$

Соотношение определяет верхнюю границу алгебраической иммунности: если нелинейность булевой функции достаточно высока, то эта граница увеличивается. В данной работе при поиске булевых функций с максимальной алгебраической иммунностью на каждой итерации поддерживается высокое значение нелинейности для получаемых потомков с помощью алгоритма Hill Climbing. Проведённые эксперименты показали эффективность такого подхода. Результаты экспериментов для $n = 4, 6, 8$ представлены в таблице, где $n$ — число переменных; $P$ — размер популяции; $T$ — число итераций.

Результаты применения ГА и Hill Climbing

| n | P | T | min, среднее, max значения Al(f) в исходной популяции | min, среднее, max значения Al(f) после применения ГА | Количество функций с max Al(f) при применении ГА | Количество функций с max Al(f) при применении ГА + Hill Climbing |
|---|---|---|---|---|---|---|
| 4 | 10 | 20 | (0; 1,1; 2) | (2; 2; 2) | 609 | 715 |
| 6 | 10 | 20 | (0; 1,6; 3) | (3; 3; 3) | 649 | 718 |
| 8 | 10 | 20 | (1; 2,5; 4) | (4; 4; 4) | 683 | 703 |
| 8 | 20 | 20 | (1; 2,75; 4) | (4; 4; 4) | 2864 | 2989 |

Полученные булевы функции могут быть использованы при поиске векторных булевых функций с высокой компонентной алгебраической иммунностью. Наличие высокой компонентной алгебраической иммунности S-блоков способствует противостоянию алгебраическому криптоанализу поточных и блочных шифров.

ЛИТЕРАТУРА

1. Courtois N. and Meier W. Algebraic attacks on stream ciphers with linear feedback // LNCS. 2003. V. 2656. P. 345-359.

2. Millan W., Clark A., and Dawson E. An effective genetic algorithm for finding highly nonlinear Boolean

functions // LNCS. 1997. V. 1334. P. 149-158.

3. Clark J., Jacob J., Stepney S., et al. Evolving Boolean functions satisfying multiple criteria // LNCS. 2002. V. 2551. P. 246-259.
4. Picek S., Jakobovic D., Miller J., et al. Cryptographic Boolean functions: one output, many design criteria // Appl. Soft Computing. 2016. No. 40. P. 635-653.
5. Behera P. and Gangopadhyay S. An improved hybrid genetic algorithm to construct balanced Boolean function with optimal cryptographic properties // Evolutionary Intelligence. 2021. No. 1. P. 1-15.
6. Matsui M. Linear cryptanalysis method for DES cipher // LNCS. 1994. V. 765. P. 386-397.
7. Лобанов М. С. Точные соотношения между нелинейностью и алгебраической иммунностью // Дискретный анализ и исследование операций. 2008. Т. 15. № 6. С. 34-47.

УДК 519.7 DOI 10.17223/2226308X/14/5

# S-БЛОКИ С МАКСИМАЛЬНОЙ КОМПОНЕНТНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ ОТ МАЛОГО ЧИСЛА ПЕРЕМЕННЫХ[9]

Д. А. Зюбина, Н. Н. Токарева

Пусть π — перестановка $n$ элементов, $f$ — булева функция от n переменных. Рассмотрим векторную булеву функцию $F_n: F_n \to F_n^n$ вида $F_n(x) = (f(x), f(\pi(x)), \bullet\bullet\bullet, f(\pi^{n-1}(x)))$. Изучается компонентная алгебраическая иммунность функции $F_n$ в зависимости от булевой функции f и перестановки $n$ при n = 3, 4, 5. Получены полные множества булевых и частичные векторных булевых функций с максимальной алгебраической иммунностью от малого числа переменных.

**Ключевые слова:** булева функция, векторная булева функция, алгебраическая иммунность, компонентная алгебраическая иммунность.

S-блоки играют решающую роль в обеспечении стойкости блочных шифров к различным типам атак. Основная причина этого в том, что в классических и современных блочных шифрах нелинейный слой представлен именно данными блоками. S-блок является отображением множества двоичных векторов длины $n$ в множество двоичных векторов длины $m$. В 2003 г. в [1] был представлен новый вид криптоанализа — алгебраический, основанный на понижении степени системы уравнений, описывающей шифр. Для противостояния такому роду атак необходимо, чтобы S-блок имел максимально возможное значение компонентной алгебраической иммунности.

Будем рассматривать S-блоки определённого вида, а именно $F_n(x) = (f(x), f(\pi(x)), \ldots, f(\pi^{n-1}(x)))$, где $F_n: F_n \to F_{2n}$; $f$ — булева функция от $n$ переменных; $\pi$ — циклический сдвиг влево на один. Эта конструкция предложена А. Удовенко в решении олимпиадной задачи на NSUCRYPTO-2016 [2]. Он показал, что при таком построении векторной функции можно получить функцию с максимальной алгебраической иммунностью от 3, 4, ... , 10 переменных. В настоящее время остаётся открытым вопрос о существовании векторной булевой функции с максимальной компонентной иммунностью $\lceil n/2 \rceil$ от произвольного числа переменных $n$.

Алгебраической иммунностью $AI(f)$ булевой функции $f$ называется минимальное число $d$,

[9]Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF-2022-0018) при поддержке лаборатории криптографии JetBrains Research.

такое, что существует булева функция $g$ степени $d$, не тождественно равная нулю, для которой выполняется равенство $fg = 0$ или $(f \oplus 1)g = 0$ [3]. Известно, что для произвольной булевой функции $f$ от $n$ переменных выполнено $AI(f) \le \lceil n/2 \rceil$. Компонентной алгебраической иммунностью $AI_{comp}(F)$ векторной булевой функции $F$ называется минимальная алгебраическая иммунность её компонентных функций, т. е. функций $f_b(x) = \langle b, F(x) \rangle$, где $b \in F_n$, $b \ne 0$ и $\langle a, b \rangle = a_1 b_1 \oplus \ldots \oplus a_n b_n$ – скалярное произведение векторов по модулю 2.

В данной работе для построения S-блока с максимальной компонентной алгебраической иммунностью реализован метод нахождения линейного подпространства размерности $n$ в множестве, содержащем векторы значений нулевой функции и всех булевых функций от $n$ переменных с максимальной алгебраической иммунностью $\lceil n/2 \rceil$. В первую очередь путём полного перебора формируется множество булевых функций с максимальной алгебраической иммунностью. К этому множеству добавляется нулевой вектор. Далее из этого множества выбирается функция и на её основе строятся оставшиеся $n - 1$ функций (применением перестановки $\pi$ к аргументам); все такие функции также лежат в этом множестве. Затем проверяется, порождают ли все $n$ функций линейное подпространство размерности $n$. Если да, то данное подпространство позволяет построить S-блок с максимальной компонентной иммунностью, выбрав в качестве координатных функций S-блока базис подпространства. Для однозначности пусть функция строится в виде $F_\pi(x) = (f(x), f(\pi(x)), \ldots, f(\pi^{n-1}(x)))$.

Для $n = 3$ путём полного перебора получено, что существует 56 булевых функций с максимальной алгебраической иммунностью 2. Из них на основе 12 функций (им отвечают четыре подпространства) можно построить векторную булеву функцию с максимальным значением иммунности. Все эти функции можно представить в виде АНФ общего вида.

**Утверждение 1.** Булевы функции $f$ от трёх переменных с максимальной алгебраической иммунностью 2, такие, что векторные функции вида $F_\pi(x) = (f(x), f(\pi(x)), f(\pi^2(x)))$, где $\pi$ – циклический сдвиг, также имеют максимальную компонентную алгебраическую иммунность 2, можно описать следующей конструкцией:

$$f(x_1, x_2, x_3) = x_i + x_j + x_i x_k + a, \quad \text{где } \{i, j, k\} = \{1, 2, 3\},\ a \in F_2.$$

Для $n = 4$ путём полного перебора получено, что существует 54 952 булевых функций с максимальной алгебраической иммунностью 2. При рассмотрении всевозможных перестановок $n$ (а не только циклического сдвига влево, как это происходило ранее) оказалось, что только при шести перестановках существуют векторные булевы функции, которые сохраняют максимальную иммунность. Эти перестановки можно представить в векторном виде: (2, 3, 4, 1), (2, 4, 1, 3), (3, 1, 4, 2), (3, 4, 2, 1), (4, 1, 2, 3), (4, 3, 1, 2) или циклическом (1234), (1243), (1342), (1324), (1432), (1423). Для каждой перестановки существует 6144 булевых функций (или 1536 линейных подпространств), построенные на основе которых векторные булевы функции также имеют максимально возможную компонентную алгебраическую иммунность.

**Утверждение 2.** Пусть $f$ – булева функция от $n$ переменных с максимальной алгебраической иммунностью $\lceil n/2 \rceil$. Если векторная булева функция $F_n(x) = = (f(x), f$

$(n(x)),\dots,f(n^{n-1}(x)))$ имеет максимальную компонентную алгебраическую иммунность, то $n$ является полноцикловой перестановкой.

Для $n = 5$ путём полного перебора получено, что всего существует 197 765 122 булевых функций с максимальной алгебраической иммунностью 3. Существует как минимум четыре булевых функции (им отвечает одно подпространство), на основе которых строится векторная булева функция с максимальным значением иммунности.

С учётом экспериментальных результатов сформулированы следующие гипотезы:

**Гипотеза 1.** Для любого $n > 2$ в множестве, состоящем из булевых функций от $n$ переменных с максимальной алгебраической иммунностью и нулевой функции, существует линейное подпространство размерности $n$.

Данная гипотеза доказана для $n = 2, 3, 4, 5, 6, 8, 10$ благодаря собственным результатам и результатам А. Удовенко. Для $n = 7, 9$ пока не найдено таких подпространств.

**Гипотеза 2.** Пусть $f$ – булева функция от $n$ переменных с максимальной алгебраической иммунностью $\mathrm{d}n/2\mathrm{e}$. Тогда в её АНФ присутствует по меньшей мере по одному моному каждой степени $i$, где $i = 1, 2, \dots, \mathrm{d}n/2\mathrm{e}$.

Данная гипотеза проверена для $n = 2, 3, 4, 5, 6, 8, 10$ благодаря собственным результатам и результатам А. Удовенко.

Таким образом, возможно построение S-блока от малого числа переменных, который устойчив к алгебраическим атакам. В дальнейшем планируется анализ булевых и векторных булевых функций от большего числа переменных.

ЛИТЕРАТУРА

1. Courtois N. and Meier W. Algebraic attack on stream ciphers with linear feedback // LNCS. 2003. V. 2656. P. 345-359.
2. Tokareva N., Gorodilova A., Agievich S., et al. Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography // Прикладная дискретная математика. 2018. № 40. С. 34-58.
3. Meier W., Pasalic E., and Carlet C. Algebraic attacks and decomposition of Boolean functions // LNCS. 2004. V. 3027. P. 474-491.

УДК 519.7 DOI 10.17223/2226308X/14/6

## О НЕКОТОРЫХ СВОЙСТВАХ САМОДУАЛЬНЫХ ОБОБЩЁННЫХ БЕНТ-ФУНКЦИЙ[10]

А. В. Куценко

Бент-функции вида $F_n \to Z_q$, где $q > 2$ — натуральное число, называются обобщёнными бент-функциями. Обобщённые бент-функции, для которых можно определить дуальную бент-функцию, называются регулярными. Регулярная обобщённая бент-функция называется самодуальной, если она совпадает со своей дуальной. Получены необходимые и достаточные условия самодуальности обобщённых бент-функций из класса Елисеева — Мэйорана — МакФарланда. Представлен полный спектр расстояний Ли между данными функциями. Доказано несуществование аффинных самодуальных обобщённых бент-функций. Приведён класс изомет- ричных отображений, сохраняющих самодуальность обобщённой бент-функции. С помощью данных отображений получена уточнённая классификация самоду-

[10]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке РФФИ (проект № 20-31-70043) и лаборатории криптографии JetBrains Research.

альных бент-функций вида $F_4 \wedge Z_4$.

**Ключевые слова:** самодуальная бент-функция, обобщённая бент-функция, класс Елисеева — Мэйорана — МакФарланда, расстояние Ли.

Через $F_{2^n}$ обозначим линейное пространство всех двоичных векторов длины $n$ над полем $F_2$. Пусть $q$ — натуральное число; обобщённой булевой функцией от $n$ переменных называется отображение вида $F_n \wedge Z_q$. Множество всех обобщённых булевых функций от $n$ переменных обозначим $GF_n$ Для каждой пары $x,y \in F_n$ через $\langle x, y \rangle$ обо- $n$ значается значение $x_i y_i$. Весом Хэмминга $\mathrm{wt}(x)$ вектора $x \in F_{2^n}$ называется число $i=1$ его ненулевых координат. Расстояние Хэмминга между булевыми функциями $f, g$ от $n$ переменных — число двоичных векторов длины $n$, на которых эти функции принимают различные значения; обозначается $\mathrm{dist}(f, g)$. Согласно [1], назовём ортогональной группой порядка $n$ над полем $F_2$ группу

$$O_n = \{L \in GL(n, F_2) : LL^T = I_n\},$$

где $L^T$ — транспонирование $L$; $I_n$ — единичная матрица порядка $n$ над полем $F_2$.

Обобщённым преобразованием Уолша — Адамара функции $f \in GF_{q^n}$ называется функция $H_f : F_n \wedge C$, заданная равенством

$$H_f(y) = \sum_{x \in F_n} w^{f(x)} (-1)^{\langle x, y \rangle}, \; y \in F_n, \; x \in F_n$$

где $w = \exp(2\pi i/q)$. Функция $f \in GF_n$ называется *обобщённой бент-функцией*, если $|H_f(y)| = 2^{n/2}$ для каждого $y \in F_{2^n}$ [2]. Обзор различных обобщений бент-функций представлен в работе [3]. Множество обобщённых бент-функций обозначается через $GB_{q^n}$. *Весом Ли* вектора $x \in Z_q$ называется число $\mathrm{wt}_L(x) = \min\{x, q - x\}$. *Расстояние Ли* $\mathrm{dist}_L(f, g)$ между функциями $f, g \in GF_{q^n}$ определяется как

$$\mathrm{dist}_L(f, g) = \sum_{x \in F_n} \mathrm{wt}_L(\sigma(x)),$$

где $\sigma \in GF_n$ и $\sigma(x) = f(x) + (q - 1)g(x)$ для любого $x \in F_n$.

Пусть $f \in GB_{q^n}$, тогда если существует функция $f \in GF_{q^n}$, такая, что $H_f(y) = = w^{f(y)} 2^{n/2}$, то бент-функция $f$ называется *регулярной*, а функция $f$ — дуальной к $f$. Дуальная функция также является регулярной обобщённой бент-функцией. Если $f = = f$, то $f$ называется *самодуальной* обобщённой бент-функцией. Если $f = f + q/2$, то $f$ называется *антисамодуальной* обобщённой бент-функцией. Всюду далее считается, что $q$ — чётное натуральное число.

Открытой проблемой является полная характеризация и описание класса булевых самодуальных бент-функций ($q = 2$). Этому и другим вопросам, связанным с самодуальными бент-функциями, посвящёно большое количество работ (C. Carlet, L. E. Danielson, M. G. Parker, P. Sole, X. Hou, T. Feulner, L. Sok, A. Wassermann и др.). Подробную информацию о бент-функциях и их приложениях можно найти в книге [4]. В ряде работ исследованы свойства самодуальных бент-функций в рамках различных обобщений бент-функций: так, в [5, 6] рассматривается обобщение вида $F_n \wedge F_p$, где $p$ простое. Получен ряд результатов, в частности представлена полная классификация квадратичных самодуальных бент-функций. Связь самодуальных обобщённых бент-функций вида $F_n \wedge Z_4$ и самодуальных булевых бент-функций исследована в работе [7]. На основе обнаруженной взаимосвязи сделан вывод о несуществовании самодуальных обобщённых бент-функций указанного вида в случае

нечётного числа переменных.

В настоящей работе исследуются свойства самодуальных обобщённых бент-функций $F_n \wedge Z_q$, где $q$ — чётное натуральное число.

Булевы бент-функции от чётного числа переменных $n$, представимые в виде

$$f(x,y) = h(x, \pi(y)) \oplus g(y), \quad x,y \in F_{n/2},$$

где $\pi$ — перестановка на множестве $F_{n/2}$ и $g$ — булева функция от $n/2$ переменных, формируют хорошо известный класс Елисеева — Мэйорана — МакФарланда. Обобщённые бент-функции вида

$$f(x,y) = 2h(x, \pi(y)) + g(y), \quad x,y \in F_{n/2},$$

образуют класс обобщённых бент-функций Елисеева — Мэйорана — МакФарланда.

**Утверждение 1.** Обобщённая бент-функция Елисеева — Мэйорана — МакФарланда

$$f(x,y) = 2h(x,y) + g(y), \quad x,y \in F_{n/2},$$ является (анти)самодуальной

тогда и только тогда, когда

$$\pi(y) = L(y \oplus b), \quad g(y) = 2h(b,y) + d, \quad y \in F_{n/2},$$

где $L \in O_{n/2}$; $b \in F_2^{n/2}$; $wt(b)$ — чётное (нечётное) число; $d \in Z_q$.

Спектр расстояний Хэмминга между самодуальными бент-функциями из класса Елисеева — Мэйорана — МакФарланда получен в работе [8]. Далее представлен спектр расстояний Ли между (анти)самодуальными обобщёнными бент-функциями из класса Елисеева — Мэйорана — МакФарланда. Для данного спектра используется обозначение $Sp_L$.

**Теорема 1.** Справедливо

$$Sp_L = \{q \cdot 2^{n-2}\} \cup \{2q \cdot 2^{n-2}\} \cup \{(2r+1) \cdot 2^{n-r} : 1 \le r \le n/2-1\}.$$

Более того, все приведённые расстояния достижимы.

На основе данного результата можно сделать вывод о минимальном расстоянии Ли между рассматриваемыми функциями.

**Утверждение 2.** Минимальное расстояние Ли между (анти)самодуальными обобщёнными бент-функциями из класса Елисеева — Мэйорана — МакФарланда от $n$ переменных равно $q \cdot 2^{n-3}$.

Хорошо известно, что булева бент-функция и, как следствие, самодуальная булева бент-функция не может быть аффинной. Тем не менее в работе [9] показано, что для обобщённых бент-функций данный вопрос нетривиален, в частности, для случая, когда $q$ кратно 4, существуют аффинные обобщённые бент-функции. Следующий результат показывает отсутствие аффинных самодуальных обобщённых бент-функций для произвольного чётного $q$.

**Теорема 2.** Для любого положительного чётного $q$ и произвольного натурального

n не существует самодуальных обобщённых бент-функций вида

$$f(x) = \mathrm{PP}_{i=1} A_i X_i + A_0,$$

где $A_0, A_1, \ldots, A_n \in Z_q$

Далее представлен класс отображений, сохраняющих (анти)самодуальность обобщенной бент-функции.

**Теорема 3.** Отображения множества всех обобщённых булевых функций от n переменных в себя, имеющие вид

$$f(x) \to f(L(x + c)) + 2h(c, x) + d, \quad x \in F_n,$$

где $L \in O_n$, $c \in F_n$, wt(c) — чётное число, $d \in Z_q$, сохраняют (анти)самодуальность обобщённой бент-функции.

Заметим, что каждое такое отображение сохраняет расстояние Хэмминга и расстояние Ли между обобщёнными бент-функциями, то есть является изометричным. С помощью отображений данного вида получена уточнённая классификация кватернарных самодуальных бент-функций от четырёх переменных (таблица).

Классификация самодуальных обобщённых бент-функций от четырёх переменных для q = 4

| Вектор значений представителя класса эквивалентности | Размер класса |
|---|---|
| 0220202022000000 | 24 |
| 2022220222020200 | 64 |
| 0330313133110110 | 48 |
| 0330302132010110 | 120 |
| 1321213122010100 | 96 |
| 0220213023100000 | 48 |
| Число функций | 400 |

ЛИТЕРАТУРА


1. Janusz G. J. Parametrization of self-dual codes by orthogonal matrices // Finite Fields Appl. 2007. V. 13. No.3. P. 450-491.
2. Schmidt K.-U. Quaternary constant-amplitude codes for multicode CDMA // IEEE Trans. Inform. Theory. 2009. V. 55. No. 4. P. 1824-1832.
3. Токарева Н. Н. Обобщения бент-функций. Обзор работ // Дискрет. анализ исслед. опер. 2010. Т. 17. №1. С. 33-62.
4. Tokareva N. Bent Functions: Results and Applications to Cryptography. Acad. Press, Elsevier, 2015. 230 p.
5. *Cesmelioglu A., Meidl W., and Pott A.* On the dual of (non)-weakly regular bent functions and self-dual bent functions // Adv. Math. Commun. 2013. V. 7. No. 4. P. 425-440.
6. *Hou X.-D.* Classification of p-ary self dual quadratic bent functions, p odd // J. Algebra. 2013. V. 391. P. 62-81.
7. *Sok L., Shi M., and Sole P.* Classification and construction of quaternary self-dual bent functions // Cryptogr. Commun. 2018. V. 10. No. 2. P. 277-289.
8. *Kutsenko A. V.* The Hamming distance spectrum between self-dual Maiorana — McFarland bent functions // J. Appl. Industr. Math. 2018. V. 12. No. 1. P. 112-125.
9. *Singh B. K.* On cross-correlation spectrum of generalized bent functions in generalized Maiorana — McFarland class // Inform. Sci. Lett. 2013. V. 2. No. 3. P. 139-145.

УДК 519.7 DOI 10.17223/2226308X/14/7

# О СВОЙСТВАХ РАЗНОСТНЫХ ХАРАКТЕРИСТИК XOR ПО МОДУЛЮ $2^n$ [11]

Н. Муха, Н. А. Коломеец, Д. А. Ахтямов, И. А. Сутормин, М. А. Панферов, К. М. Титова, Т. А. Бонич, Е. А. Ищукова, Н. Н. Токарева, Б. Ф. Жантуликов

Рассматривается вероятность $adp_{\oplus}(a, в, Y)$ преобразования разностей в функции XOR по модулю $2^n$, где $a,e,Y$ е $Z_n$- Эта величина используется при анализе примитивов с симметричным ключом, сочетающих XOR и сложение по модулю, например ARX-конструкций. Основное внимание уделяется характеристикам с максимальной вероятностью при одном фиксированном аргументе. Установлено, что $\max_{a,в} adp_{\oplus}(a, в, Y) = adp_{\oplus}(0,Y, Y)$, и доказано, что существуют либо две, либо восемь различных пар (a,в), для которых достигается вероятность $adp_{\oplus}(0, Y,Y)$- Получены упрощенное представление величины $adp_{\oplus}(0, 7, Y)$ и формула для $\min_{Y} adp_{\oplus}(0, Y, Y)$.

**Ключевые слова:** ARX, XOR, сложение по модулю, разностный криптоанализ.

ARX — одна из современных архитектур в симметричной криптографии. В компонентах таких шифров используются только три операции: сложение по модулю $2^n$, циклический сдвиг и покомпонентное сложение по модулю 2 (XOR). Архитектуру ARX имеют блочные шифры FEAL [1], Threefish [2], один из победителей eSTREAM поточный шифр Salsa20 [3] и его модификация ChaCha [4], входящая в TLS, а также финалисты SHA-3 хэш-функции BLAKE [5] и Skein [2]. Разностный криптоанализ [6] основан на изучении преобразования разностей открытых текстов в разности шифртекстов, сложность такого изучения является недостатком ARX-шифров. Выбирая в качестве разности разность по модулю $2^n$, вероятности разностных характеристик операции XOR определяются функцией $adp_{\oplus}$:

$$adp_{\oplus}(a, в \to Y) = \frac{\#\{x, y \in Z_n : (x + a) \oplus (y + в) = (x \oplus y) + Y\}}{4^n}$$

С вектором $x \in Z_{2^n}$ мы ассоциируем целое число $x_0 + x_1 2^1 + \ldots + x_{n-1} 2^{n-1}$, $x + a$ означает сложение по модулю $2^n$ ассоциированных с $x$ и $a$ чисел, $-x$ является обратным к ассоциированному с $x$ числу относительно сложения по модулю $2^n$. Известно [7], что $adp_{\oplus}(a, в \to Y)$ при $a, в, Y \in Z_n$ представимо в виде произведения матриц размера $8x8$, что позволяет эффективно вычислять $adp_{\oplus}$ за линейное по $n$ время.

Отметим, что данная работа началась в рамках Первого воркшопа Математического центра в Академгородке (см. http://mca.nsu.ru/workshop/).

Приведём преобразования аргументов, не меняющие значение $adp_{\oplus}$.

**Утверждение 1.** Пусть $a, в, Y \in Z_n$. Тогда справедливо следующее:

1) $adp_{\oplus}$ является симметрической, т. е. не меняет значение при перестановке $a, в, Y$;

2) значение $adp_{\oplus}$ не изменится, если к любым двум аргументам прибавить $2^{n-1}$ по модулю $2^n$: $adp_{\oplus}(a, в \to Y) = adp_{\oplus}(a + 2^{n-1}, в + 2^{n-1} \to Y)$;

[11] Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования РФ № 075-15-2019-1613, и лаборатории криптографии JetBrains Research.

3) $adp_{\oplus}(a,e \wedge Y) = adp_{\oplus}(a,e \wedge -Y)$; в силу п. 1 можно поставить « —» перед любым аргументом.

В [7, теорема3] сформулирована теорема о максимальном значении $adp_{\oplus}(a,e^Y)$ при фиксированном $Y$. Однако доказательство не было приведено («The proof is omitted from the conference version») и впоследствии нигде не было опубликовано. Мы доказали, что это утверждение действительно является верным.

**Теорема 1.** Для любого $Y \in Z_n$ выполняется

$$\max_{a,e \in Z_n} adp_{\oplus}(a,e \wedge Y) = adp_{\oplus}(0, Y \wedge Y)\bullet$$

Метод доказательства позволяет также найти количество пар $(a, в)$, на которых достигается значение $adp_{\oplus}(0, Y \wedge Y)$.

**Следствие 1.** Количество пар $(a, в) \in Z_n \times Z^{\wedge}$, таких, что $adp_{\oplus}(a, в \wedge Y) = = adp_{\oplus}(0, Y \wedge Y)$, где $Y \in Z_n$, равно:

1) $2$, если $Y = 0$ или $Y = 2^{n-1}$, а именно это пары

$$(0, 0), (2^{n-1},2^{n-1}) \text{ при } Y = 0 \text{ и } (0, 2^{n-1}), (2^{n-1},0) \text{ при } Y = 2^{n-1};$$

2) $8$ для всех других $Y$, а именно это пары

$$(0,Y), (Y,0), (2^{n-1},-Y+2^{n-1}), (-Y + 2^{n-1}, 2^{n-1}),$$
$$(0,-Y), (-Y,0), (2^{n-1}, Y + 2^{n-1}), (Y + 2^{n-1}, 2^{n-1}).$$

Заметим, что все приведённые пары являются симметриями, описанными в утверждении 1. Кроме того, если $Y$ равна $0$ или $2^{n-1}$, то $adp_{\oplus}(0,Y \wedge Y) = 1$.

Используя S-функции [8], величину $adp_{\oplus}(0, Y \wedge Y)$ можно представить в виде произведения матриц размера $3 \times 3$. Однако если исключить старший бит, достаточно матриц размера $2 \times 2$.

**Теорема 2.** Для любого $Y \in Z_n^n$ выполнено

$$adp_{\oplus}^{(0,}(Y \wedge Y) = (1,^{1)}B_{Y_{n-2}} B_{Y_{n-3}} \text{---} B_0^{(1,\,0)T},$$

где $B_0 = \begin{matrix} 4 & 41 \\ & 01 \end{matrix}$ ; $B_1 = \begin{matrix} & 10 \\ & 14 \end{matrix}$.

Более прозрачную формулу для $adp_{\oplus}(0,Y \wedge Y)$ получить не удалось. Косвенным подтверждением сложности этой задачи является непростое выражение для минимального из значений $adp_{\oplus}(0, Y \wedge Y)$ при фиксированном $n$.

**Теорема 3.** Пусть $m_n = \min_{Y \in Z_n} adp_{\oplus}(0, Y \wedge Y)$. Тогда для любого $n$ выполнено

$$m_{n+2} = 4\,{}^{11}m_{n+1} + 4\,m_n.$$

**Следствие 2.** Числа $m_n$, $n = 1, 2, \ldots,$ образуют последовательность Хорадама [9] и для них верно

$$m_n = \frac{}{34 \bullet 8_n} \backslash ((17 + \vee 17)(1 + \text{УЙ})^n + (17 - 7\wedge 17)(1 - \text{УЙ})^n).$$

Тем не менее сумму всех элементов $adp_{\oplus}(0, Y \wedge Y)$ вычислить несложно.

**Утверждение 2.** Для любого $n$ выполнено

$$\mathrm{P}\, adp_{\oplus}(0,Y \wedge Y) = 2\,(3/2)^{n-1}.$$
$$Y \in Z_n$$

Подробно с результатами работы можно ознакомиться в [10].

ЛИТЕРАТУРА

1. Shimizu A. and Miyaguchi S. Fast data encipherment algorithm (FEAL) // 1988. LNCS. 1988. V.304.

P. 267-278.
2. Ferguson N., Lucks S., Schneier B., et al. The Skein Hash Function Family. http://www. skein-hash.info. 2009.
3. Bernstein D. J. Salsa20 Specification. https://cr.yp.to/snuffle/spec.pdf. 2005.
4. Bernstein D. J. ChaCha, a Variant of Salsa20. https://cr.yp.to/chacha/ chacha-20080128.pdf. 2008.
5. Aumasson J.-P., Meier W., Phan R. C.-W., and Henzen L. The Hash Function BLAKE. https://www.researchgate.net/publication/316806226_The_Hash_Function_BLAKE. 2014.
6. Biham E. and Shamir A. Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4. No. 1. P. 3-72.
7. Lipmaa H., Wallen J., and Dumas P. On the additive differential probability of exclusive-or // LNCS. 2004. V. 3017. P. 317-331.
8. Mouha N., Velichkov V., De Canniere C., and Preneel B. The differential analysis of S-func- tions // LNCS. 2011. V. 6544. P. 36-56.
9. Horadam A. F. Basic properties of a certain generalised sequence of numbers // The Fibonacci Quarterly. 1965. V. 3. No. 3. P. 161-176.
10. Mouha N., Kolomeec N., Akhtiamov D., et al. Maximums of the additive differential probability of Exclusive-Or // IACR Trans. Symmetric Cryptology. 2021. V. 2021. No. 2. P. 292-313.

УДК 519.7 DOI 10.17223/2226308X/14/8

# УЛУЧШЕННЫЕ ОЦЕНКИ ДЛЯ ЧИСЛА k-ЭЛАСТИЧНЫХ И КОРРЕЛЯЦИОННО-ИММУННЫХ ДВОИЧНЫХ ОТОБРАЖЕНИЙ

К. Н. Панков

Получены улучшенные нижние и верхние оценки для числа корреляционно-иммунных порядка *к* и k-эластичных *((n, m, k)-устойчивых)* двоичных отображений.

**Ключевые слова:** распределённый реестр, блокчейн, информационная безопасность, устойчивые вектор-функции, эластичные вектор-функции, корреляционно-иммунные функции.

В настоящее время использование систем распределённого реестра, основанных на технологии цепной записи данных (блокчейн) [1], становится всё более распространённым в самых различных отраслях современной цифровой экономики [2]. Пандемия COVID-19, продолжавшаяся весь 2020 год и не оконченная до сих пор, дала, согласно мнению ряда экспертов [3], дополнительный импульс развитию дистанционных доверенных сервисов, основой функционирования которых являются системы распределённых реестров, признанные в Российской Федерации, согласно [4], средством криптографической защиты информации. Как уже отмечалось в [5], в связи с расширением применения технологии блокчейн жизненно важным становится исследование информационной безопасности систем распределённого реестра, на этой технологии основанных. Одним из способов обеспечения безопасности данных в подобных системах является использование шифрования, например поточного, в связи с чем возникает задача оценки числа корреляционно-иммунных и $(n, m, к)$-устойчи-

вых двоичных отображений, которые могут быть использованы в системах поточного шифрования в качестве комбинирующих отображений.

Понятия корреляционной иммунности и $(n, m, k)$-устойчивости будем понимать в соответствии с [6], где подробно рассмотрены их свойства. Задаче оценки числа отображений и булевых функций, обладающих соответствующими свойствами, посвящён целый ряд работ, среди которых можно отметить [7- 10]. Ряд результатов был доложен автором на конференциях SIBECRYPT [11-13].

Обозначим через $V_n$ множество двоичных векторов размерности $n$. Корреляционная иммунность и k-эластичность (или $(n, m, k)$-устойчивость) двоичного отображения $f(a) = (f_1(a), f_2(a),..., f_m(a)) : V_n \to V_m$, согласно [6], сводится к обладанию этими свойствами всеми ненулевыми линейными комбинациями координатных функций (компонентами [14]). В [15, 16] получены асимптотические оценки числа корреляционно-иммунных и $(n, m, \ldots)$-устойчивых двоичных отображений с точностью до оценок мощности множества специального вида $<^{**}(m, N)$:

$$<^{**}(m, N) = \{T = (r_J, 0 = J \subset \{1,..., m\}, I \subset \{1,..., n\}, |I| \le k) : (Z_2)^N : \forall I \; \forall s \in \{1,...,m\} \; \forall J \subset \{1,...,m\}, s \in J \; (V_m(P(-1)^{x_I + x_J}) r_J = 0\}$$

где $Z_{2^{m-1}}$ — кольцо вычетов по модулю $2^{m-1}$; $\chi_m(J)$ — индикаторный вектор множества $J \subset \{1, \ldots, m\}$ [17].

Если использовать обозначение [8] то легко показать, что

$$M(n, k) = \sum_{s=0}^{k} \binom{n}{s}$$

$$<^{**}(m,N) = (<(m))^{M(n,k)},$$

где

$$<(m) = n \sim r = (r_J, 0 = J \subset \{1,..., m\}) : (Z_{2^{m-1}})^{2^1} : \forall s \in \{1,...,m\} \; \forall J \subset \{1,...,m\}, s \in J \; (V_m \; P' \; (-1)^{x_J}) r_j = 0\}.$$

В [15] найдены точные значения мощности множества $<(m)$ при $m \in \{1, 2, 3, 4\}$ и верхние и нижние оценки при $m > 5$:

$$m - 1 \le \log_2 |<(m)| \le (m - 2) 2^m - m + 3.$$

Последний результат удалось улучшить:

**Теорема 1.** Во введённых обозначениях при $m > 5$ выполняется

$$\frac{m^2 - m}{2} + 17 \le \log_2 |<(m)| \le (m - 2) 2^m - m + 3 - \frac{1}{16}.$$

Обозначим через $R(n, m, k)$ множество всех $(n, m, \ldots)$-устойчивых (k-эластичных) двоичных отображений из $B_m$ всех $m$-мерных двоичных функций от $n$ переменных,

а через $K(n, m, k)$ – множество всех корреляционно-иммунных порядка $k$ двоичных отображений из $B_n^m$.

Для упрощения записи удобно ввести следующее обозначение:

$$T(n, m, k) = (2^m —$$

Используя теорему 1, легко доказать

**Следствие 1.** Пусть при всех достаточно больших $n$ для произвольного $0 < Y < < 1/3$ выполняется неравенство $\kappa (5 + 2\log_2 n) + 6m \; 6 \; n (1/3 — Y)$. Тогда существует $n_0$, такое, что для любых $£_1, £_2 > 0$, $n > n_0$ верны неравенства

$$/m^2 - m - \frac{12}{} + 17\text{^ M } (n, k) - £_1 \; 6 \; \text{iog}_2 |R [n, m, k]| - m2^n + T (n_m, k) \; 6$$
$$6 (16m - 47) \; 2^{m-4} — m + 3) \; M (n, k) + £_2.$$

**Следствие 2.** Пусть при всех достаточно больших $n$ для произвольного $0 < y < < 5/18$ выполняется неравенство $k (5 + 2\log_2 n) + 6m \; 6 \; n (5/18 — y)$. Тогда существует $n_0$, такое, что для любых $£_1, £_2 > 0$, $n > n_0$ верны неравенства

$$( \text{-------} \; 2 \frac{m^2 — m — 12}{\text{--------}} + 17 \; j \; M (n, k) — £_1 \; 6$$

$$6 \log_2 |K (n, m, k)| — m2^n — n^{\pm} + \text{^g}^{2} \; \text{Д} — k\text{^} (2^m — 1) + m2^{m-1} + T (n, m, k) \; 6$$

$$6 ((16m — 47) \; 2^{m-4} — m + 3) \; M (n, k) + £_2$$

Полученные в следствиях 1 и 2 результаты улучшают оценки, полученные ранее в работах [11, 12, 16, 18].

ЛИТЕРАТУРА


1. МР 26.4.001-2018 «Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров» М.: Технический комитет по стандартизации «Криптографическая защита информации», 2018. 10 с.
2. Блокчейн-революция в банках и финансовых институтах. Отчет. М.: MINDSMITH, 2020. https://mindsmith.io/blockchain-finance/
3. Колонка MINDSMITH: Блокчейн в зените лета. 6 августа 2020 года. https://ict.moscow/news/blockchain-trends-mindsmith/
4. Елистратов А., Маршалко Г. Б., Светушкин В. Подводные камни сертификации блок- чейн-решений // Открытые системы. СУБД. 2019. № 1. С. 19.
5. Pankov K. Enumeration of Boolean mapping with given cryptographic properties for personal data protection in Blockchain Data Storage // Proc. 24th Conf. Open Innovations Assoc. FRUCT, Moscow, Russia, 2019. P. 300-306.
6. Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.
7. Денисов О. В. Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций // Дискретная математика. 1991. № 2. С. 25-46.
8. Денисов О. В. Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. № 1. С. 82-95.
9. Canfield E. R., Gao Z., Greenhill C., et al. Asymptotic enumeration of correlation-immune Boolean functions // Cryptogr. Commun. 2010. No. 1. P. 111-126.
10. Potapov V. N. A lower bound on the number of boolean functions with median correlation immunity // 16th Int. Symp. “Problems of redundancy in information and control systems”, Moscow, Russia, 2019. P. 45-46.
11. *Панков К. Н.* Уточнённые асимптотические оценки для числа (n, m, к)-устойчивых двоичных

отображений // Прикладная дискретная математика. Приложение. 2017. № 10. С. 46-49.
12. *Панков К. Н.* Уточнённые асимптотические оценки для числа корреляционно-иммунных двоичных функций и отображений // Прикладная дискретная математика. Приложение. 2018. №11. С. 49-52.
13. *Панков К. Н.* Рекуррентные формулы для числа k-эластичных и корреляционно-иммунных двоичных отображений // Прикладная дискретная математика. Приложение. 2019. № 12. С. 62-66.
14. *Carlet C.* Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications. V. 134. N.Y.: Cambridge University Press, 2010. P. 398-472.
15. *Панков К. Н.* Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Математические вопросы криптографии. 2014. №4. С. 73-97.
16. *Pankov K. N.* Improved asymptotic estimates for the numbers of correlation-immune and k- resilient vectorial Boolean functions // Discr. Math. Appl. 2019. No. 3. P. 195-213.
17. *Сачков В. Н.* Курс комбинаторного анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013. 336 с.
18. *Панков К. Н.* Улучшенные асимптотические оценки для числа корреляционно-иммунных и k-эластичных двоичных вектор-функций // Дискретная математика. 2018. №2. С. 73-98.

УДК 519.719.2 DOI 10.17223/2226308X/14/9

# О СПОСОБЕ ПОСТРОЕНИЯ ДИФФЕРЕНЦИАЛЬНО 25-РАВНОМЕРНЫХ ПОДСТАНОВОК НА $F_{2^{2m}}$

Д. Б. Фомин

Рассмотрены способы построения дифференциально 25-равномерных подстановок на $F_{2^{2m}}$ для случая $m > 3$. Предложенный подход излагается с использованием так называемого T U -представления функций и обобщает известный способ построения дифференциально 4-равномерных подстановок поля $F_{2^{2m}}$ с применением подстановки обращения ненулевых элементов поля.

**Ключевые слова:** *S-Box, подстановка, дифференциальная равномерность,* T U - *представление.*

Исследование способов построение нелинейных биективных преобразований с заданными криптографическими характеристиками является актуальной и сложной задачей. Одним из известных подходов, позволяющих строить нелинейные преобразования с достаточно высокими криптографическими характеристиками и допускающие эффективную программную и аппаратную реализацию, является использование подстановок, имеющих декомпозицию.

Пусть $F_2 = \{0, 1\}$ – поле из двух элементов с операциями сложения «+» и умножения «•»; $(F_n, +) = \{(a_0, a_1, \ldots, a_{n-1}) : a_i \in F_2, i = 0, \ldots, n-1\}$ — арифметическое векторное пространство размерности $n$. Задав специальным образом операцию умножения на множестве $F_{2^n}$, можно определить поле $F_{2^n}$, состоящее из $2^n$ элементов. Везде

далее считаем, что фиксирована биекция между $F_{2^n}$ и $F_{2^n}$. Произвольную функцию $F$: $F_n \to F_m$ будем называть $(n, m)$-функцией. Тогда $(n, 1)$-функция есть булева функция, биективная $(n, n)$-функция – подстановка.

**Определение 1** [1]. Пусть $F$ – $(n, m)$-функция, $1 \le t \le \min(n,m)$, $x_1, y_1 \in F_2$, $x_2 \in F_{n-t}$, $y_2 \in F_{m-t}$, $x = x_1 \| x_2 \in F_n$, $y = y_1 \| y_2 \in F_m$. Тогда если существуют такие функции $T: F_2 \times F_{n-t} \to F_2$, $U: F_{n-t} \times F_2 \to F_{m-t}$, что при фиксации $x_2$ произвольным значением $T(x_1, x_2)$ есть биекция по переменной $x_1$ и функция $F$ представима в виде

$$F(x) = F(x_1 \| x_2) = T(x_1, x_2) \| U(x_2, T(x_1, x_2)), \quad (1)$$

то такое представление функции $F$ в виде (1) будем называть $TU$-представлением.

**Замечание 1.** Известно [2], что в случае $m = n$ функция $F$ является подстановкой, если функция $U(x_2, x_1)$ является подстановкой по $x_2$ при фиксации $x_1$.

**Определение 2.** Для $F: F_n \to F_m$ и произвольных $a \in F_n \setminus \{0\}$, $b \in F_m$ положим $d_{F,b} = |\{x \in F_n: F(x + a) + F(x) = b\}|$.

Будем говорить, что $F$ является дифференциально $\delta_F$-равномерной функцией, если

$$\delta_F = \max_{a \in F_n \setminus \{0\}, b \in F_m} \delta_{a,b},$$

значение $\delta_F$ будем называть показателем дифференциальной равномерности функции $F$.

Использование нелинейных преобразований с меньшим показателем дифференциальной д-равномерности при синтезе криптографических примитивов позволяет гарантировать стойкость последнего к разностному методу криптографического анализа.

Известно достаточно много примеров подстановок, обладающих высокими криптографическими характеристиками и имеющих $TU$-представление:

- подстановка, $CCZ$-эквивалентная подстановке Диллона, – единственная известная в настоящий момент 2-равномерная подстановка на $F_{2^m}$ [3];
- подстановка, линейно эквивалентная подстановке алгоритмов ГОСТ Р 34.11-2012 и «Кузнечик» (ГОСТ Р 34.12-2018) [2];
- подстановки из работ [4-7].

Для $a \in F_{2^{n-t}}$ обозначим:

- $\delta_{m,a}$ – показатель дифференциальной д-равномерности подстановки, которую задаёт функция $T(x_1, x_2)$ при фиксации $x_2 = a$;
- $\Delta_{T,U}(a, \alpha)$ – количество решений уравнения

$$T(x_1, a) + T(x_1 + a_1, a + a_2) = b_1, \; a_1, b_1 \in F_{n-t}, \; a_2 \in F_2 \setminus \{0\}.$$

Получен следующий критерий дифференциальной д-равномерности функции $F$, имеющей $TU$-представление.

**Теорема 1.** Пусть у функции $F$ имеется $TU$-представление (1). Тогда показатель дифференциальной д-равномерности функции $F$ меньше либо равен значению

$$2^t \cdot \max < d_{T,a}, \qquad \max \qquad \text{Д}^{a1,a2,B1}_{T,a}$$

[ $a2_{\in}F^{n}\backslash\{0\}$ Доказательство теоремы следует из того факта, что при каждой из $2^t$ фиксаций $x_2$ значением $a_2$ уравнения вида

$$T(x_i, 0_2) + T(x_i + a_i, a_2 + «_2) = B_1$$

являются следствием уравнений

$$F(x_i, a_2) + F(x_i + a_i, a_2 + «_2) = B_1 \text{ КВ} 2.$$

Теорема 1 позволяет строить дифференциально 25-равномерные преобразования, а замечание 1 гарантирует биективность этого преобразования.

**Следствие 1.** Пусть в условиях теоремы 1 $t=1$ и $5_{m,a} 6 5$ для всех $a \in F_2$. Тогда функция $F$, имеющая $T\,U$-представление (1), не более чем дифференциально 25-равномерна тогда и только тогда, когда $\max_{a_x,B_x \in Ж^{n-1}} \text{Д}\mathbf{T}O^{1\wedge_1} 6 5$.

Для доказательства следствия необходимо отметить, что $A\mathbf{T}Q^{1\wedge 1} = \text{Д}_{T11^{1,B_1}}$ для всех $a_i, e_i \in F_{n^{-1}}$. Тогда, согласно следствию 1, задача построения дифференциально 25-равномерных подстановок сводится к поиску двух подстановок $П_0, П? \in S(Ж?^{-1})$, таких, что количество решений уравнений

$$n_0(x) + n_i(x + a_i) = B_1 \qquad (2)$$

при всевозможных значениях $a_1, B_1 \in F_{n-1}$ не больше 2. Действительно, если $T(x_1, i) = = n_i(x_i)$, $i \in \{0,1\}$, $U(x_2,x_1)$ — линейная по $x_2$ функция при произвольной фиксации $x_1$, то с использованием формулы (1) получим подстановку с показателем дифференциальной равномерности 25. В качестве $П_0, П_1$ можно взять произвольную дифференциально 2-равномерную подстановку. В этом случае, с учётом следствия 1 и замечания 1, функция $F$ является подстановкой с показателем дифференциальной равномерности большим либо равным 4. При этом если максимальное количество решений (2) равно двум, то подстановка будет дифференциально 4-равномерной, иначе показатель её дифференциальной равномерности будет определяться удвоенным максимальным количеством решений уравнений вида (2).

**Теорема 2.** Пусть $x_i \in F_{2n-1}$, $n$ чётное, $n > 6$, $x_2 \in F_2$, $f$ — произвольная булева функция от $n-1$ переменной, $c \in F_{2n-1}\backslash\{0, 1\}$,

$$T: F_{2n-i} \times F_2 \wedge F_{2n-i},\ T(x_i, x_2) = x_{-1} \cdot c_{x^2},$$
$$U: F_2 \times F_{2n-i} \wedge F_2,\ U(x_2,x_i) = f(x_i) + x_2.$$

Тогда формула (1) задаёт подстановку $F$, при этом

1) если $\text{tr}(c) = \text{tr}(c^{-1}) = 1$, то $5_F = 4$;

2) иначе $5_F = 6$.

**Замечание 2.** Результат п. 1 теоремы 2 доказан в [8], однако следствие 1 позволяет проводить доказательство с более общих позиций.

**Теорема 3.** Пусть $x_i \in F_{2n-i}$, $n$ чётное, $n > 6$, $x_2 \in F_2$, $f$ — произвольная булева функция от $n-1$ переменной, $c \in F_{2n-i}\backslash\{0, 1\}$,

$$T: F_{n^{-1}} \times F_2 \wedge F_{n^{-1}},\ T(x_i,x_2) = x_? \cdot c_{x^2},$$

$$U\colon \mathrm{F}_2 \times \mathrm{F}_{2^{n-i}} \to \mathrm{F}_2,\ U(x_2, x_i) = f(x_i) + x_2.$$

Тогда формула (1) задаёт подстановку $F$, при этом $5_F = 6$.

Напомним, что две $(n, т)$-функции $g$ и $f$ называются расширенно аффинно-эквивалентными, если существуют аффинные подстановки $a$ и $b$ пространств $\mathrm{F}_{2^n}$ и $\mathrm{F}_{2^m}$ соответственно и аффинная $(n, т)$-функция $c$, что $f(x) = (b \circ g \circ a)(x) + c(x)$ [1]. Расширенно аффинно-эквивалентные функции, очевидно, имеют одинаковый показатель дифференциальной равномерности. В доказательстве теоремы 3 используется тот факт, что уравнение третьей степени не может иметь больше трёх решений. Естественно предположить, что если взять в качестве $T(x_1, i) = x^3_1 + a_i x^2_1 + b_i x_1$ – функции, расширенно аффинно-эквивалентные 2-равномерной подстановке $x^3$, то можно построить 4-равномерные подстановки $F$ с использованием формулы (1). Следующее утверждение показывает, что это не так.

**Утверждение 1.** Пусть $x_3 \in \mathrm{F}_{2^{n-i}}$, $n$ чётное, $n > 6$, $x_2 \in \mathrm{F}_2$, $f$ — произвольная булева функция от $n - 1$ переменной, $a, b \in \mathrm{F}_{2^{n-i}}$,

$$T\colon \mathrm{F}_{2^{n-1}} \times \mathrm{F}_2 \to \mathrm{F}_{2^{n-1}},\ T(x_n\ 0) = x^3_1,\ T(x_n\ 1) = x^3_1 + a \cdot x^2_1 + b \cdot x_i,$$
$$U\colon \mathrm{F}_2 \times \mathrm{F}_{2^{n-3}} \to \mathrm{F}_2,\ U(x_2, x_i) = f(x_i) + x_2.$$

Тогда существуют $a_3, в_1 \in \mathrm{F}_{2^{n-i}}$, такие, что количество решений уравнения $T(x_3 + + a_3, 0) + T(x_3, 1) = в_1$ равно $2^{n-3}$, либо $T(x_3, 1)$ не является подстановкой.

Приведём ещё несколько результатов, полученных применением теоремы 1.

**Утверждение 2.** Пусть $x_1 \in \mathrm{F}_{2^{n-1}}$, $n$ чётное, $n > 6$, $x_2 \in \mathrm{F}_2$, $f$ – произвольная булева функция от $n - 1$ переменной,

$$T\colon \mathrm{F}_{2^{n-i}} \times \mathrm{F}_2 \to \mathrm{F}_{2^{n-i}},\ T(x_i, 0) = x_3,\ T(x_i, 1) = x^3,$$
$$U\colon \mathrm{F}_2 \times \mathrm{F}_{2^{n-3}} \to \mathrm{F}_2,\ U(x_2, x_i) = f(x_i) + x_2.$$

Тогда формула (1) задаёт подстановку $F$, при этом $6_F = 8$.

**Утверждение 3.** Пусть $t = 2$, $x_1 \in \mathrm{F}_{2^{n-t}}$, $x_2 \in \mathrm{F}_{2^t}$. Тогда существуют такие $c_{x_2}$, $x_2 \in \mathrm{F}_{2^2}$, $c_{x_0} \neq c_{x_{00}}$ при $x_{0_2} \neq x_{0_2^0}$, что подстановка $F$, задаваемая формулой (1), дифференциально 8-равномерна, где

$T$: $\mathrm{F}_{2^{n-t}} \times \mathrm{F}_{2^t} \to \mathrm{F}_{2^{n-3}}$, $T(x_3, x_2) = x^3 \cdot c_{x_2}$, $2\quad 2\quad 2\quad 1\,2\quad 1\quad x2$

$U$: $\mathrm{F}_2 \times \mathrm{F}_{2^{n-t}} \to \mathrm{F}_2$, при фиксации произвольного $x_3$ функция $U(x_2, x_3)$ является подстановкой по переменной $x_2$.

ЛИТЕРАТУРА


1. Canteaut A. and Perrin L. On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting. Cryptology ePrint Archive: Report 2018/713.
2. Biryukov A., Perrin L., and Udovenko A. Reverse-engineering the S-box of Streebog, Kuznyechik and Stribobrl // LNCS. 2016. V. 9665. P. 372-402.
3. Biryukov A., Perrin L., and Udovenko A. Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem (Full Version). Cryptology ePrint Archive: Report 2016/539.
4. *De la Cruz Jimenez R. A.* Generation of 8-bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-bit S-Boxes and Finite Field Multiplication. 2017. www.cs.haifa.ac.il/orrd/LC17/paper60.pdf.
5. *Fomin D. B.* New classes of 8-bit permutations based on a butterfly structure // Матем. вопр. криптогр. 2019. Т. 10. № 2. С. 169-180.
6. *Фомин Д. Б.* Построение подстановок пространства $\mathrm{V}_{2^m}$ с использованием (2m, m)- функций. //

Матем. вопр. криптогр. 2020. Т. 11. № 3. С. 121-138.
7. Фомин Д. Б. Об алгебраической степени и дифференциальной равномерности подстановок пространства $V_{2m}$, построенных с использованием (2m, т)-функций. // Матем. вопр. криптогр. 2020. Т. 11. №4. С. 133-149.
8. Carlet C., Tang D., Tang X., and Liao Q. New construction of differentially 4-uniform bijections // LNCS. 2013. V. 8567. P. 22-38.

УДК 519.719.325 DOI 10.17223/2226308X/14/10

# УСЛОВИЕ ОДНОЗНАЧНОСТИ РАЗЛОЖЕНИЯ В ПРОИЗВЕДЕНИЕ ФУНКЦИЙ p-ЗНАЧНОЙ ЛОГИКИ ПРИ ЛИНЕЙНОЙ ЗАМЕНЕ ПЕРЕМЕННЫХ

А. В. Черемушкин

Рассматривается множество разложений функции p-значной логики в произведение функций от непересекающихся множеств переменных при различных линейных преобразованиях аргументов. Каждому такому разложению соответствует разложение векторного пространства в прямую сумму подпространств. Приведены условия, при которых разложение определяется однозначно с точностью до перестановки подпространств между собой.

**Ключевые слова:** двоичные функции, разложение в прямую сумму, линейное преобразование.

Пусть $n > 1$, $V_n = Z_p^n$ рассматривается как векторное пространство над полем $Z_p$, $F_n = \{f : V_n \to Z_p\}$ — множество функций от $n$ переменных.

Пусть $1 \leq k \leq n$. Говорят, что переменные $x_{k+1}, \ldots, x_n$ функции $f(x_1, \ldots, x_n)$ являются несущественными, если найдётся функция $h(x_1, \ldots, x_k)$, такая, что $f = h$. Нетрудно видеть, что переменная $x_n$ является несущественной для функции $f$, если и только если $f(x + e^n) = f(x)$ при $e^n = (0, \ldots, 0, 1)$.

Пусть $(\mathbf{H}_n)_f$ — группа инерции функции $f$ в группе сдвигов $\mathbf{H}_n$, т. е. множество $x$ таких сдвигов $I \in \mathbf{H}_n$, что выполнено сравнение $f(x + a) = f(x)$, $x \in V_n$.

Условие тривиальности группы инерции $(\mathbf{H}_n)_f$ равносильно тому, что у всех функций, полученных из $f$ всевозможными линейными заменами переменных, все переменные будут существенными.

Назовём носителем *функции* $f : V_n \to Z_p$ множество векторов, на которых она принимает ненулевые значения:

$$f^{-1}(*) = \{a \in V_n : f(a) = 0\}.$$

Если носитель функции содержится в некотором многообразии размерности $k$, то это позволяет сводить задачу исследования функции от $n$ переменных к задаче исследования функции от $n - k$ переменных.

**Лемма 1.** Пусть функция $f : V_n \to Z_p$ не является константой. Если носитель $f^{-1}(*)$ функции $f$ содержится в многообразии $L + a \subset V_n$, $1 \leq \dim L \leq n - 1$, то существует линейное преобразование $A$ пространства $V_n$, функция $h : Z_p^{n-k} \to Z_p$ и элементы $a_1, \ldots, a_k \in Z_p$, $k = n - \dim L$, такие, что функцию $f(xA)$ можно представить в виде

$$f(xA) = J_{a_1}(x_1) \ldots J_{a_k}(x_k) h(x_{k+1}, \ldots, x_n),$$

где

$$J_a(x_i) = \begin{cases} 1, & x_i = a, \\ , & x_i \neq a. \end{cases}$$

**Лемма 2.** Пусть разложение функции $f$ по первой переменной имеет вид

$$f(x_1,x_2,\ldots,x_n) = \sum^{p-1} J_{a_i}(x_1) f_{a_i}(x_2,\ldots,x_n). \qquad (1)$$

Тогда:

1) если $f(x_1,x_2,\ldots,x_n) = J_{a_1}(x_1) f_{a_1}(x_2,\ldots,x_n)$, то множество $f^{-1}(*)$ содержится в гиперплоскости, задаваемой уравнением $(x, e^1) = a_1$;
2) если в разложении (1) имеется не менее двух ненулевых слагаемых, то множество $f^{-1}(*)$ содержится в гиперплоскости в том и только в том случае, когда все множества $f^{-1}(*)$, $0 \neq a_1 \neq p-1$, одновременно содержатся в одной гиперплоскости.

Будем говорить, что функция $f \in F_n$ *линейно разложима в бесповторное произведение*, если при некотором линейном преобразовании $A$ пространства $V_n$ и $1 \leq k < n$ найдутся функции $f_1$ и $f_2$, для которых выполнено сравнение

$$f(xA) = f_1(x_1,\ldots,x_k) f_2(x_{k+1},\ldots,x_n).$$

С данным разложением связаны разложения вида $f = h_1 h_2$, где $h_i = c_i f_i$; $c_i \in Z_p$, $i = 1, 2$, и выполнено условие $c_1 c_2 = 1$.

**Теорема 1.** Если функция $f = f(x_1,\ldots,x_n)$ имеет тривиальную группу инерции $(H_n)_f$, её носитель не содержится ни в какой гиперплоскости и она линейно разложима в бесповторное произведение, то для этой функции найдётся линейное разложение в бесповторное произведение линейно неразложимых (в бесповторное произведение) сомножителей, однозначно определённое в том смысле, что любое другое такое разложение соответствует тому же самому разложению пространства в прямую сумму подпространств, а соответствующие функции линейно эквивалентны с точностью до константного сомножителя.

Заметим, что для случая $p = 2$ разложение двоичной функции в бесповторное произведение нелинейных неразложимых сомножителей изучено в работе автора [1]. В настоящей работе применяется аналогичный метод доказательства.

В качестве следствия получаем описание группы инерции таких функций в полной аффинной группе.

**Следствие 1.** Если в условиях теоремы функция $f$ представлена в виде произведения линейно неразложимых в бесповторное произведение функций

$$f = f_1 \cdot \ldots \cdot f_m,$$

причём множество функций $\{f_1,\ldots,f_m\}$ разбивается на $t$ классов аффинной эквивалентности с точностью до константного сомножителя:

$$\{f_{M_1},\ldots,\} \in F_{n_1,\ldots,} \quad \{f_{V_1},\ldots,f_{V_q}\} \in F_{n_t,}$$

то для группы инерции бесповторного произведения этих функций справедлив изоморфизм

$$AGL(n,p)_{f_1\ldots f_m} = [AGL(n_1,p)_{f_1}]S_r \times \ldots \times [AGL(n_t,p)_{f_{V_1}}]$$

• Здесь через $G_f$ обозначена группа инерции функции $f$ в группе $G$; $[G]S_r$ – операция экспоненцирования группы $G$ с помощью симметрической группы $S_r$ степени $r$. Аналогичное описание справедливо для полной линейной группы $GL(n, p)$.

ЛИТЕРАТУРА

1. Черемушкин А. В. Однозначность разложения двоичной функции в бесповторное произведение нелинейных неприводимых сомножителей // Вестник Московского государственного университета леса «Лесной вестник». 2004. №4(35). С. 86-90.

УДК 519.7 DOI 10.17223/2226308X/14/11

# О ПРОИЗВОДНЫХ БУЛЕВЫХ БЕНТ-ФУНКЦИЙ[1]

А. С. Шапоренко

Бент-функция может быть определена как булева функция f (x) от n переменных (n чётно), такая, что для любого ненулевого вектора y её производная $D_y f(x) = f(x) \oplus f(x \oplus y)$ сбалансирована принимает значения 0 и 1 одинаково часто. Справедливо ли, что любая сбалансированная функция — производная некоторой бент-функции? Эта задача рассмотрена для частного случая — аффинных функций. Доказано, что любая неконстантная аффинная функция от $n > 4$ (n чётно) переменных является производной для $(2^{n-1} - 1)|B_{n-2}|^2$ бент-функций, где $B_{n-2}$ — класс бент-функций от n - 2 переменных. Получены итерационные нижние границы для числа бент-функций.

**Ключевые слова:** бент-функции, булевы функции, производные бент-функций, нижние границы для числа бент-функций.

Пусть $\langle x, y \rangle$ — скалярное произведение двоичных векторов по модулю 2. Функция $f : Z_n^2 \to Z_2$ называется *булевой функцией* от n переменных. Булева функция от чётного числа переменных называется бент-функцией, если она максимально нелинейна [1]. Обозначим через $B_n$ множество бент-функций от n переменных.

Шифры, в которых применяются бент-функции, более устойчивы к *линейному криптоанализу* [2], потому что бент-функции крайне плохо аппроксимируются аффинными функциями. Бент-функции используются в структуре блочного шифра CAST как координатные функции S-блоков [3], а также для построения регистра сдвига с нелинейной обратной связью в поточном шифре Grain [4]; они связаны также с некоторыми объектами теории кодирования, например с кодами Рида — Маллера [5].

Другое определение бент-функции — булева функция $f(x)$ от n переменных (n чётно), такая, что для любого ненулевого вектора $y$ её производная $D_y f(x) = f(x) \oplus f(x \oplus y)$ сбалансирована — принимает значения 0 и 1 одинаково часто [5]. Справедливо ли, что любая сбалансированная функция — производная некоторой бент-функции? В [6] показано, что любая сбалансированная функция g от $n \geq 6$ переменных степени не выше $n/2 - 1$, такая, что $g(x) = g(x \oplus y)$ для всех x при некотором y, является производной некоторой бент-функции от n переменных. В данной работе эта задача рассмотрена для частного случая сбалансированых функций — аффинных: $\psi_{a,b}(x) = (a,x) \oplus b$, где $a \in Z_n$ — ненулевой вектор и $b \in Z_2$.

**Теорема 1.** Любая неконстантная аффинная функция $\psi_{a,b}(x)$ от $n > 4$ (n чётно) переменных является производной для $(2^{n-1} - 1)|B_{n-2}|^2$ бент-функций.

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке лаборатории криптографии JetBrains Research.

**Лемма 1.** Для любой бент-функции g и любых $y \neq y_0$ справедливо: $D_y g(x) \neq D_{y_0} g(x)$.

**Лемма 2.** Пусть $D_y g(x) = l_{a,b}(x)$ для бент-фукции $g(x)$. Тогда при любом $y_0$ $D_{y_0} g(x) = l_{a,b}(x) \oplus 1$.

Теорема 1 вместе с леммами 1 и 2 даёт итерационные нижние границы для количества бент-функций от $n+2$ переменных (теорема 2).

**Теорема 2.** Для любого чётного $n > 4$ верно

$$|B_{n+2}| > (2^{n+2} - 2)|B_n|^2.$$

Данная граница хуже представленной в [7], но она, вероятно, может быть улучшена, если рассматривать больше одной аффинной функции или учитывать функции, которые не имеют аффинных производных. Однако задача выделения бент-функций, которые имеют производную $'_{a,b}$ и не имеют $'_{c,d}$, является непростой. Бент-функции, которые не имеют аффинных производных, рассмотрены, например, в [8].

ЛИТЕРАТУРА

1. *Rothaus O.S.* On bent functions //J. Combinat. Theory. Ser. A. 1976. V. 20. No. 3. P. 300-305. 2. *Matsui M.* Linear cryptanalysis method for DES cipher // LNCS. 1994. V. 765. P. 386-397.

3. *Adams C.* Constructing symmetric ciphers using the CAST design procedure // Design, Codes, Cryptogr. 1997. V. 12. No. 3. P. 283-316.
4. *Hell M., Johansson T., Maximov A., and Meier W.* A stream cipher proposal: Grain-128 // IEEE Intern. Symp. Inform. Theory. 2006. P. 1614-1618.
5. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press., 2015.
6. *Токарева Н. Н.* О множестве производных булевой бент-функции // Прикладная дискретная математика. Приложение. 2016. № 9. С. 35.
7. *Tokareva N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Adv. Math. Commun. 2011. V. 5. No. 4. P. 609-621.
8. *Canteaut A and Charpin P.* Decomposing bent functions // IEEE Trans. Inform. Theory. 2003. V. 49. No. 8. P. 2004-2019.

Секция 3

# МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7 DOI 10.17223/2226308X/14/12

## XS-СХЕМЫ: СКРЫТИЕ ТАКТОВЫХ ОРАКУЛОВ

С. В. Агиевич

XS-схемы описывают блочные шифры, в которых используются две операции над двоичным словами фиксированной длины: X — поразрядное сложение по модулю 2 и S — подстановка. В работе исследуется модель XS-схем, согласно которой несколько экземпляров простой тактовой схемы, в которой задействована всего одна операция S, объединяются в сложную схему, называемую каскадом. S-операции каскадов интерпретируются как независимые тактовые оракулы. Возможность определения пары «вход — выход» некоторого оракула по паре «вход — выход» всего каскада означает слабость последнего. Мы формализуем свойство каскада скрывать тактовых оракулов, т. е. затруднять определение внутренних пар «вход — выход». Мы показываем, что при использовании регулярной тактовой схемы каскад скрывает оракулов, если число тактов не менее чем в 2 раза больше размерности (числа слов в обрабатываемом блоке данных).

**Ключевые слова:** *блочный шифр, XS-схема, тактовый оракул, линейная рекуррентная последовательность.*

В [1] для описания блочно-итерационных шифров предложено использовать XS-схемы. Элементарная (однотактовая) XS-схема порядка $n$ задаётся тройкой $(a,B,c)$, в которой $a$ и $c$ – двоичные вектор-столбец и вектор-строка размерности $n$, $B$ – двоичная матрица порядка $n$. Схема инстанциируется над полем $F$ из $2^m$ элементов выбором подстановки $S$: $F \to F$, которая называется тактовым *оракулом*. Результатом инстан- циирования является преобразование

$$(a, B, c)[S]: F_n \to F_n,\ x \to y = xB + S(xa)c.$$

Здесь и далее $x$ и $y$ – вектор-строки.

Нас будут интересовать регулярные схемы, только они имеют криптографическое значение. В регулярной схеме матрицы обратимы. Матрица $B$ может быть обратимой или нет, в зависимости от этого схему относят к типу I или II.

$$A = (a\ Ba\ \ldots\ B^{n-1}a), \qquad C = \begin{pmatrix} cB^{n-1} \\ \ldots \\ cB \end{pmatrix}$$

Пусть $(a,B,c)^t$ — $t$-тактовый каскад, полученный соединением $t$ экземпляров элементарной схемы $(a, B, c)$. Инстанциируя экземпляры оракулами $S_1, \ldots, S_t$, получаем преобразование $(a, B, c)^t[S_1, \ldots, S_t]$. Его действие можно описать следующим образом: по входу $x = y(0) \in F_n$ вычисляется последовательность

$$y(m) = y(m-1)B + S_\tau(y(m-1)a)c, \qquad \tau = 1, 2, \ldots, t,$$

и её последний элемент $y = y(t)$ объявляется результатом преобразования.

Оракулы $S_\tau$ моделируют секретные подстановки, действие которых определяется тактовыми ключами, построенными по исходному ключу блочного шифра. Как правило, тактовый ключ достаточно легко определить всего по одной паре «вход – выход»

соответствующего оракула. Поэтому важно, чтобы каскад скрывал своих оракулов в смысле следующего определения.

**Определение 1.** Каскад $(a, B, c)^t$ размерности $n$ над полем $F$ из $2^m$ элементов скрывает тактовых оракулов, если в описываемой ниже игре симулятора с противником последний не может добиться успеха с вероятностью отличной от $1/2^m$. Правила игры:

1) Симулятор выбирает случайные независимые равновероятные подстановки $S_1$, $S_2, \ldots, S_t$ над $F$. Они будут использоваться в качестве тактовых оракулов.
2) Противник выбирает вектор $x \in F_n$ и передает его симулятору.
3) Симулятор вычисляет вектор $y = (a, B, c)^t[S_1, S_2, \ldots, S_t](x)$ и возвращает его противнику.
4) Получив $y$, противник выбирает номер такта $\tau \in \{1, 2,\ldots,t\}$, определяет пару $(u,V) \in F \times F$ и передает её симулятору.
5) Симулятор подводит итог: противник победил, если $v = S_\tau(u)$, и проиграл, если равенство нарушается.

В ходе игры противник демонстрирует умение определять «входы — выходы» тактовых оракулов, а симулятор проверяет это умение. Под противником понимается вероятностный алгоритм. Обратим внимание, что ограничения на его вычислительные ресурсы (время, память) не накладываются. Порог вероятности $1/2^m$ означает, что противник может лишь угадать выход $S_\tau(u)$ на входе $u$ (или вход $S_\tau^{-1}(v)$ на выходе $V$), т. е. каскад действительно скрывает оракулов.

Пусть $u_\tau \in F$ — вход оракула $S_\tau$ во время обработки $x$ и $v_\tau = S_\tau(u_\tau)$ — соответствующий выход, $\tau = 1, 2, \ldots, t$. Векторы $x$ и $y$ связаны следующим образом:

$$y = xB^t + (v_1, v_2, \ldots, v_t)C_t.$$

Здесь $C_t$ — матрица размера $t \times n$, в которой $m$-я строка — это вектор $cB^{t-\tau}$.

В силу регулярности матрица $C_t$ обратима при $t = n$. Поэтому по паре $(x, y)$ можно определить вектор $(v_1, v_2, \ldots, v_t)$ выходов тактовых оракулов, а затем и входы:

$$u_\tau = xB^{\tau-1}a + \sum_{i=1}^{\tau-1} v_i cB^{m-i-1}a, \; m = 1,2,\ldots, t.$$

Таким образом, $n$-тактовый каскад не скрывает оракулов, и число тактов необходимо увеличивать. Следующая теорема показывает, что для скрытия достаточно $2n$ тактов.

**Теорема 1.** Если $(a, B, c)$ — регулярная схема и $t > 2n$, то каскад $(a, B, c)^t$ скрывает тактовых оракулов.

Доказательство. Начнём с рассмотрения схем типа I. Предположим, что существует обратимая матрица $M$ размера $n \times n$ над полем $F$, такая, что $C_t M$ содержит столбец с единственным ненулевым элементом. Пусть, не нарушая общности, это столбец $e_\tau$ с единицей в позиции $m$ и нулями в остальных позициях. Если $e_\tau$ — это $i$-й столбец $C_t M$, то $v_\tau$ можно найти как $i$-ю координату $(xB^t + y)M$, поскольку

$$(v_1, v_2, \ldots, v_t)C_t M = (xB^t + y)M.$$

При запрете на существование $M$ матрица $C_t$, дополненная столбцом $e_\tau$, имеет полный ранг $n + 1$. Данный факт выполняется для любого номера $\tau = 1,2,\ldots,t$. Факт означает, что при любом варианте выбора выхода $v_\tau$ имеется одно и то же число вариантов выбора остальных выходов, при которых $x$ переходит в $y$. Поскольку случайный равновероятный выбор $S_1, S_2, \ldots, S_t$ индуцирует случайный равновероятный

выбор вектора выходов $(v_1, v_2, \ldots, v_t)$ при любом векторе входов $(u_1, u_2, \ldots, u_t)$, все варианты перехода $x \wedge y$ имеют один и тот же вероятностный вес. Поэтому вероятность корректно определить $v_T$ равняется $1/2^m$. С такой же вероятностью окажется корректной любая пара $(u, V)$, выбранная противником.

Остаётся показать, что матрицы $M$ не существует. Предположим противное. Пусть $r$ – некоторый (ненулевой) столбец $M$. Записывая координаты соответствующего столбца $C_t M$ снизу вверх, получаем последовательность

$$cB^0r, cB^1r, \ldots, cB^{t-1}r.$$

Мы имеем дело с линейной рекуррентной последовательностью (л.р.п.) порядка $n$. Л.р.п. ненулевая, поскольку её $n$-префикс ненулевой. Префикс действительно ненулевой, поскольку матрица $C$ из определения регулярности обратима. Более того, из обратимости $C$ следует, что любой $n$-отрезок л.р.п. будет ненулевым. Поэтому отрезок длины $t > 2n$ не может содержать менее двух ненулевых элементов. Другими словами, столбец $C_t M$ не может содержать только один ненулевой элемент. Противоречие.

Рассмотрим теперь регулярные схемы типа II. Для них л.р.п. $(cB^T r)$ снова начинается с ненулевого $n$-префикса. Поскольку $B$ вырождена, после префикса могут идти одни нули. Поэтому можно точно определить выход $S_T$ для $m \in \{t-n+1, t-n+2, \ldots, t\}$. Выходы для остальных $т$ можно определить только с вероятностью $1/2^m$. Аналогичные рассуждения применимы к обратному преобразованию $F^{-1}$. Оно имеет тот же тип II, и в нём в обратном порядке задействованы обратные оракулы $S^{-1}$. Теперь можно определить выход $S^{-1}$, т. е. вход $S_T$, для $m \in \{1, 2, \ldots, n\}$. Другие входы определяются с вероятностью $1/2^m$. Итак, вероятность успешного определения пары $(u_T, v_T)$ целиком не превосходит $1/2^m$. Поэтому любая пара $(u, V)$, выбранная противником, окажется корректной с вероятностью $1/2^m$. ■

Открытым остаётся вопрос о скрытии тактовых оракулов, когда противник может выбрать не один, а несколько входов $x$ и получить соответствующие выходы $y = (a,B,c)^t[S_1, S_2, \ldots, S_t](x)$.

ЛИТЕРАТУРА

1. *Agievich S.* XS-circuits in block ciphers // Матем. вопр. криптогр. 2019. Т. 10. №2. С. 7-30.

УДК 519.7 DOI 10.17223/2226308X/14/13

# РАЗРАБОТКА И АНАЛИЗ ОРАКУЛА ДЛЯ ГИБРИДНОЙ АТАКИ НА КРИПТОГРАФИЧЕСКУЮ СИСТЕМУ NTRU С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА КВАНТОВОГО ПОИСКА[12]

А. О. Бахарев

В силу развития квантовых вычислений возникает необходимость в разработке и анализе криптосистем, устойчивых к атакам с использованием квантового компьютера — алгоритмов постквантовой криптографии. Стойкость многих известных постквантовых криптосистем, основанных на теории решёток, базируется на сложности решения проблемы нахождения кратчайшего вектора в решетке (SVP). Разработана и проанализирована модель квантового оракула, необходимого для реализации гибридного квантово-классического алгоритма решения задачи SVP. На примере постквантовой криптосистемы с открытым ключом NTRU, являющейся финалистом третьего раунда конкурса NIST, получены верхние оценки на число кубит и глубину схемы, требуемые для реализации данного оракула, в зависимости от параметров криптосистемы.

**Ключевые слова:** криптосистема NTRU, квантовый поиск, криптография с открытым ключом, постквантовая криптография.

Квантовые вычисления — это быстроразвивающаяся область компьютерных исследований, которая ставит под угрозу криптографическую стойкость стандартов асимметричного шифрования, используемых в настоящее время. В 2016 г. Национальный Институт Стандартов и Технологий США (NIST) объявил конкурс «Post-Quantum Cryptography Competition», по завершении которого будет принят новый — квантовоустойчивый — стандарт асимметричного шифрования. Претендентами являются подходы на основе решёток, кодов, хэш-функций, изогений и многочленов от многих переменных.

Рассмотрим подход на основе решёток.

**Определение 1.** Пусть $u_1,\dots, u_n \in R_m$ — линейно независимые векторы, $n \leq m$. Решёткой называется множество

$$Zu_i \oplus \dots \oplus Zu_n = \sum_{i=1}^{n} b_i u_i : b_i \in Z$$

Векторы $u_1, \dots, u_n$ называются базисом решётки.

Одной из задач в теории решёток является задача нахождения кратчайшего вектора (SVP), которая заключается в нахождении вектора, имеющего наименьшую длину, в решётке, заданной своим базисом. В общем случае SVP является NP-трудной задачей. Стойкость систем, основанных на решётках, зависит от эффективности решения SVP, так как большинство известных атак сводятся к решению этой проблемы. Перспективными являются разработка и анализ квантовых алгоритмов, которые позволяют ускорить решение данной задачи.

В [1] представлен гибридный квантово-классический подход к поиску кратчайшего вектора решётки на основе GaussSieve [2] — одного из самых эффективных классических алгоритмов (алгоритм 1).

**Алгоритм 1.** Алгоритм GaussSieve (D. Micciancio and P. Voulgaris, 2010)

**Вход:** $B$ — базис решётки.

**Выход:** $v$ — кратчайший вектор решётки.

1: Инициализировать пустой неупорядоченный список $L$ и пустой стек $S$

[12]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке лаборатории криптографии JetBrains Research.

2: **Повторять**
3: получить вектор v из стека (или сгенерировать новый).
4: **Пока** $w$ ^ ПОИСК{w G $L$ : ||v ± wk 6 ||v||}
5: уменьшить v с помощью $w$ (v ^ v ± $w$).
6: **Пока** $w$ ^ ПОИСК{w G $L$ : $kw$ ± v|| 6 ||w||}
7: удалить $w$ из листа $L$;
8: уменьшить $w$ с помощью v ($w$ ^ $w$ ± v);
9: добавить $w$ в стек $S$.
10: **Если** $v$ изменился, **то**
11: добавить $v$ в стек $S$,
12: **иначе**
13: добавить $v$ в лист $L$.
14: **Пока** $v$ не станет кратчайшим вектором.
15: **Вернуть** вектор $v$.

На вход алгоритма поступает базис решётки, на основе которого будут строиться новые векторы при условии пустого стека $S$. Функция «ПОИСК» перебирает векторы $w$ в списке и проверяет одно из условий поиска: k$v$ ± $w$k 6 k$v$k или k$w$ ± $v$k 6 k$w$k; если такой вектор существует, то функция возвращает его, иначе цикл прерывается. В [2] предложено эвристическое условие остановки, которое основывается на количестве коллизий; алгоритм работает до тех пор, пока не получим такое число коллизий, что будем уверены, что нашли кратчайший вектор.

В рамках предложенного в [1] подхода ускорение достигается за счёт использования в функции «ПОИСК» квантового алгоритма Гровера поиска в неупорядоченном списке [3]. Задача, решаемая этим алгоритмом, называется задачей поиска. Предполагается, что есть неупорядоченный список из $K$ элементов, в котором как минимум один элемент удовлетворяет некоторому условию. Требуется найти по крайней мере один такой элемент. Другими словами, определена булева функция $f$, которая по номеру элемента (его двоичному представлению) определяет, является ли элемент подходящим (в этом случае $f = 1$) или нет ($f = 0$). В такой постановке задача поиска сводится к нахождению решениий уравнения $f(x) = 1$.

В классическом варианте при условии, что решение одно, требуется ~K/2 обращений к функции $f$ для нахождения решения. Квантовый алгоритм поиска элемента в неупорядоченном списке решает задачу примерно за *KK* обращений к *оракулу* — квантовому аналогу функции $f$.

Квантовый компьютер, в отличие от обычного, оперирует *кубитами* [4]. Их состояние можно представить как единичный вектор из $C^2$. Произвольный вектор этого пространства может быть представлен в виде

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

где $a, b \in C$ называются *амплитудами;* $|a|^2$ и $|b|^2$ — вероятности обнаружения кубита после измерения в состояниях $|0\rangle$ и $|1\rangle$ соответственно. Говорят, что кубит находится в *суперпозиции* состояний $|0\rangle$ и $|1\rangle$.

В соответствии с постулатами квантовой механики, состояние системы из n кубит описывается вектором состояний из $C^{2^n}$. Эволюция состояния замкнутой квантовой системы во времени описывается унитарным преобразованием.

Известно, что любая булева функция может быть реализована на квантовом

компьютере, а квантовым алгоритмом, решающим задачу поиска, является алгоритм Гровера (рис. 1).

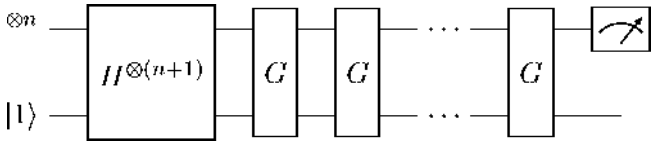



Рис. 1. Алгоритм Гровера [3]: H — вентиль Адамара; G — итерации Гровера (рис. 2)

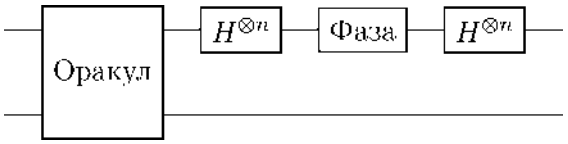



Рис. 2. Итерация Гровера

Преобразования $H^{\otimes n}$ и Фаза являются известными вентилями, в отличие от оракула, который строится под каждую задачу отдельно. В настоящей работе выполнено построение и описание оракула для квантового подхода к решению задачи поиска подходящего вектора из списка в алгоритме GaussSieve.

Оракул, представленный на рис. 3, состоит из двоичного представления номера вектора в списке, $K$ векторов размерности $d$, каждая координата которых кодируется строкой длины $m$, переключателя, проверки условия поиска и ответа. Его работа происходит следующим образом:

1) получение номера вектора на вход и передача его в переключатель;
2) выбор по номеру вектора из списка и копирование его;
3) проверка условия поиска для скопированного вектора;
4) вывод ответа: $1$ – если вектор удовлетворяет условию, $0$ – если нет.

Переключатель представляет собой векторную булеву функцию, которая номеру вектора сопоставляет строку: $i \wedge (0,..., 0,1, 0,..., 0)$, где $1$ стоит на $i$-м месте. Тогда, применяя вентиль CCNOT, можно удобно копировать вектор с номером $i$ из списка. Пример для $i = 2$ и $K = 2$ приведён на рис. 4. Здесь первые два кубита представляют собой строку, полученную из переключателя; $v_1$ и $v_2$ – векторы размерности $d$, каждая координата которых кодируется строкой длины $m$; нижний регистр оставлен для копирования нужного вектора. В итоге работы вектор $v_2$ будет скопирован в нижний регистр.

Проверка условия поиска содержит следующие операции: сложение, вычитание, возведение в квадрат и сравнение целых чисел. Предлагается использовать дополнительный код числа для операции вычитания, таким образом, сложение и вычитание реализуются одной операцией, а сравнение чисел определяется знаком результата вычитания. Сложность реализации операций на квантовом компьютере оценивается количеством кубит и глубиной схемы. В табл. 1 представлены оценки сложности операций. При каждом изменении вектора $v$ или списка $L$ в ходе работы алгоритма GaussSieve оракул строится заново.

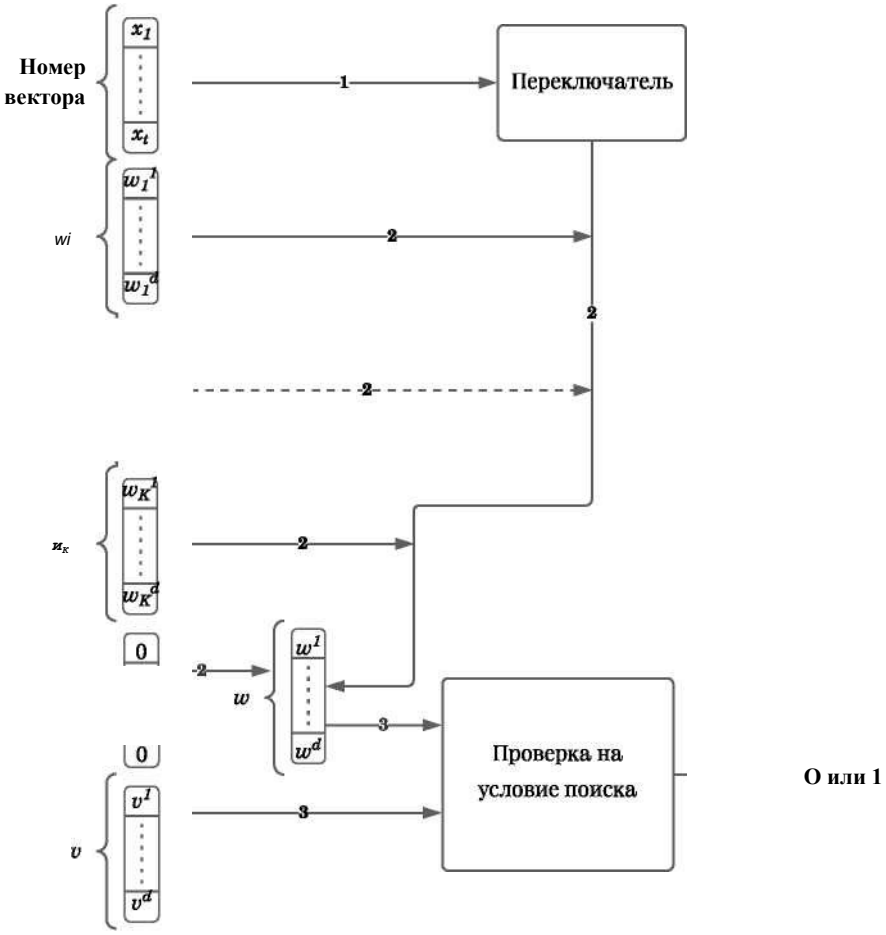



Рис. 3. Предлагаемая схема квантового оракула

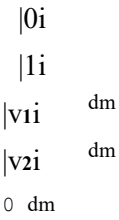



Рис. 4. Пример копирования векторов из списка

Таблица 1

**Количество кубит и глубина схемы, достаточные для реализации операций**

| Операция | Количество кубит | Глубина схемы |
|---|---|---|
| Сложение, вычитание целых m-битных чисел | 4m - 1 | 5m - 2 |
| Возведение целого m-битного числа в квадрат | $6m^2$ - 5m + 2 | $11m^2$ — 15m + 4 |
| Переключатель, где номер вектора представляется целым m-битным числом | $2^m$ + m | $3^m$ |
| Перевод целого m-битного числа в дополнительный код | 4m | 4m + 1 |

**Утверждение 1.** Пусть имеется список длины $K$, состоящий из целочисленных векторов размерности $d$, каждая координата которых кодируется битовой строкой длины $m$. Тогда для реализации квантового оракула, представленного на рис. 3, потребуется не более $\lfloor \log_2 Ke \rfloor + Kdm + K + 18dm^2 - 33dm + 6d^2 + 25d + 2m + 4$ кубит. Глубина схемы не превосходит $3^{\lfloor \log_2 Ke \rfloor} + Kdm + 33dm^2 - 67dm + 15d^2 + 35d - 2m + 19$.

Для анализа была выбрана криптосистема NTRU, так как она прошла в третий раунд конкурса NIST [5] и является одним из четырёх претендентов на новый постквантовый стандарт асимметрического шифрования. NTRU зависит от трёх целочисленных параметров $(N, p, q)$, где $(p, q) = 1$. Работа осуществляется в кольце $R$ полиномов степени не выше $N - 1$ с целочисленными коэффициентами, то есть $R = Z[x]/(x^N - 1)$.

Элемент $F = \sum_{i=0}^{N-1} F_i x \wedge R$ можно представить как вектор

$$F = [F_0, \ldots, F_{N-1}].$$

Операция умножения «*» в $R$ определяется как результат циклической свёртки:

$$F * G = H,$$

$$H_k = \sum_{i=0}^{k} F_i G_{k-i} + \sum_{i=k+1}^{N-1} F_i G_{N+k-i} = \sum_{i+j=k \pmod N} F_i G_j.$$

Если выполняется умножение полиномов по модулю числа, то коэффициенты приводятся по этому модулю.

Секретный ключ: $f$, $g$ – полиномы из $R$ с координатами из множества $\{-1, 0, 1\}$.

Открытый ключ: $N$, $p$, $q$, $h = f_q * g \bmod q$, где $f_q * f = 1 \pmod q$.

Зашифрование: Пусть $m$ – сообщение, представленное в виде полинома из $R$ с коэффициентами из интервала $(-p/2, p/2]$. Тогда зашифрованное сообщение $c$ вычисляется следующим образом: $c = pp * h + m \bmod q$, где ^ – полином из $R$ с некоторыми ограничениями на координаты из множества $\{-1, 0, 1\}$.

Расшифрование: Определим полином $a = f * c \bmod q$. Тогда исходное сообщение восстанавливается следующим образом: $m = f_q * a \bmod p$.

Одна из самых эффективных атак [6] на NTRU сводится к решению SVP в решётке, базис которой образован строками матрицы $M$, построенной на основе открытого ключа:

$$M = \begin{vmatrix} 1 & 0 & \ldots & 0 & h_0 & h_{N-1} & h_1 & \ldots & h_{N-1} \\ 0 & 1 & \ldots & 0 & \cdot & h_0 & & & \cdot \\ \cdot & & & & & & \ddots & & h_{N-2} \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \cdot & \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \cdot & \\ 0 & 0 & \ldots & 0 & q & 0 & \ldots & 0 & \\ 0 & & \ldots & 0 & & q & \ldots & 0 & \\ \cdot & 0 & \cdot & & 0 & \cdot & \cdot & & \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \cdot & \\ \cdot & \cdot & & \cdot & \cdot & \cdot & & \cdot & \end{vmatrix}$$

С большой вероятностью кратчайший вектор решётки, порождённой этим базисом, имеет вид $r = (f, g)$, а параметры оракула можно определить (оценить) следующим образом: $K \geq 2N$, $d = 2N$, $m = \lfloor \log_2 qe \rfloor + 1$.

На основе оценок из табл. 1 посчитана взаимосвязь между параметрами NTRU, количеством кубит и глубиной схемы, достаточных для реализации гибридной квантовоклассической атаки (табл. 2).

Таблица 2

**Верхние оценки числа кубит и глубины схемы**

| Параметры NTRU | Количество кубит | Глубина схемы |
|---|---|---|
| $N$ =1, q = 2 | 105 | 332 |
| $N$ = 2, q = 2 | 266 | 428 |
| $N$ = 8, $q$ = 4 | 3742 | 3498 |
| $N$ = 256, q = 128 | 4138013 | 2945510 |

Таким образом, в работе получены верхние оценки сложности реализации квантового оракула из алгоритма Гровера для реализации гибридного квантово-классического алгоритма на основе GaussSieve, который может быть использован для атак на криптосистемы, стойкость которых зависит от решения задачи SVP. Проанализирована сложность реализации квантового оракула для атаки на постквантовую криптосистему NTRU. На сегодняшний день количество кубит, с которыми оперирует квантовый компьютер, не превосходит 76 [7]. Из полученных оценок следует, что предложенная модель квантового оракула не может быть реализована на квантовом компьютере даже для самых малых параметров NTRU, так как ещё не существует квантового компьютера, оперирующего достаточным количеством кубит. В рамках дальнейшей работы предлагается оптимизировать квантовую схему оракула, получить необходимые оценки для реализации оракула данного класса, а также проанализировать другие известные классические атаки на постквантовые криптосистемы с целью изучения возможности их ускорения с помощью квантовых вычислений.

ЛИТЕРАТУРА

1. Laarhoven T., Mosca M., and van de Pol J. Finding shortest lattice vectors faster using quantum search // Des. Codes Cryptogr. 2015. V. 77. No. 2-3. P. 375-400.
2. Micciancio D. and Voulgaris P. Faster exponential time algorithms for the Shortest Vector roblem // 21st Ann. ACM Symp. Discrete Algorithms (SODA). 2010. P. 1468-1480.
3. Grover L. K. A fast quantum mechanical algorithm for database search // 28th Ann. ACM Symp. Theory Comput. (STOC). 1996. P. 212-219.
4. Nielsen M. A. and Chuang I. L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2010.
5. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.
6. Chen C., Danba O., Hoffstein J., et al. NTRU Algorithm Specifications and Supporting Documentation. https://ntru.org/, 2019.
7. Zhong H.-S., Wang H., Deng Y.-H., et al. Quantum computational advantage using photons. Science. 2020. V. 370. Iss. 6523. P. 1460-1463.

УДК 519.7 DOI 10.17223/2226308X/14/14

# КРИПТОАНАЛИТИЧЕСКАЯ ОБРАТИМОСТЬ ФУНКЦИЙ ДВУХ АРГУМЕНТОВ

Н. Ю. Бердникова, И. А. Панкратова

Предложены тесты криптоаналитической обратимости всех возможных типов для произвольных функций от двух аргументов. Сформулированы алгоритмы построения функции восстановления и генерации обратимых функций; посчитано количество обратимых функций некоторых типов.

**Ключевые слова:** обратимость функции по переменной, криптоаналитическая обратимость, тест обратимости, функция восстановления.

Понятие криптоаналитической обратимости функции введено Г. П. Агибаловым в [1, 2] как обобщение, с одной стороны, понятия «обычной» обратимости функции, с другой — криптоаналитической обратимости конечного автомата [3]. Обобщение понятия обратимости функции сделано в двух направлениях:

- обращение по переменной: по значению функции восстанавливается не весь набор значений аргументов, а только значение некоторой переменной;
- использование кванторов: восстановление значения переменной возможно не обязательно для всех значений остальных переменных.

**Определение 1** [2]. Функция $g(x_1,...,x_n)$ *обратима по переменной* $x_k$, $k \in \{1, ..., n\}$, типа $K_1 ... K_n$, где $K_i \in \{\exists, \forall\}$ и $K_k = \forall$, если существует *функция восстановления* $f$, такая, что верна формула

$$K_1 x_1 \ldots K_n x_n \, f(g(x_1, \ldots, x_n)) = x_k .$$

Понятно, что если функция обратима по всем переменным типа $\forall\forall \ldots \forall$, то она обратима в классическом смысле.

Для каждого типа обратимости возникают следующие задачи:

1) разработка теста обратимости;
2) разработка алгоритма построения функции восстановления;
3) разработка алгоритмов генерации обратимых функций (возможно, с дополнительными условиями — равновероятность генерации любой функции из класса; генерация функций с заданными свойствами и т. п.);
4) подсчёт или оценка количества обратимых функций.

Рассмотрим некоторые из этих задач для случая $n = 2$, т. е. для функций вида

$$\partial : D_1 \times D_2 \to D,$$

где $D_1, D_2, D$ — произвольные множества.

Введём обозначения: $|M|$ — мощность множества $M$ (конечного или бесконечного); $D_g$ — множество значений функции $g$; $G_a$ — множество значений подфункции, полученной из $g$ фиксацией переменной $x_1 = a$, $a \in G_1$:

$$D_g = \{g(x_1, x_2) : x_1 \in D_1, x_2 \in D_2\}, \; G_a = \{g(a, x_2) : x_2 \in D_2\}.$$

Очевидно, что необходимым условием обратимости функции $g(x_1, x_2)$ по переменной $x_k$, $k \in \{1, 2\}$, является $|D_g| > |D_k|$; будем всюду считать, что оно выполнено.

## 1. Обратимость типа $\forall\forall$

Условие обратимости функции $g(x_1, x_2)$ по переменной $x_k$, $k \in \{1, 2\}$, в этом случае записывается так:

$$\exists f \forall x_1 \forall x_2 \, f(g(x_1, x_2)) = x_k .$$

Тест обратимости является частным случаем (при $n = 2$) леммы 1 из [3].

**Утверждение 1** (тест обратимости типа $\forall\forall$). Функция $g(x_1, x_2)$ обратима типа $\forall\forall$ по переменной $x_k$, $k \in \{1, 2\}$, если и только если

$$\forall x_1 \forall x_2 \forall y_i \exists y_2 \, (x_k = y_k \wedge g(x_1, x_2) = \partial(y_1, y_2)).$$

Без ограничения общности (поскольку одноимённые кванторы перестановочны) далее будем считать, что $k = 1$, и переформулируем тест более конструктивным образом.

**Утверждение 2.** Функция $g(x_1, x_2)$ обратима типа W по переменной $x_i$, если и только если

$$\forall a,b \in D_i\,(a = b \wedge G_a \cap G_b = 0). \qquad (1)$$

Функция восстановления $f: D_g \wedge D_1$ строится по формуле

$$\forall x_i \in D_1 \forall X_2 \in D_2\,(f(g(x_i,x_2)) = x_i),$$

функциональность отношения $f$ следует из условия (1).

Можно предложить следующий **алгоритм 1** генерации обратимой функции $g$:

1. Построить произвольное разбиение множества $D$ на классы $D^{(a)}$, $a \in D_i$.
2. Для всех $a \in D_i$:
   2.1) для каждого $x_2 \in D_2$ выбрать в качестве $g(a, x_2)$ случайное значение из множества $D^{(a)}$.

Корректность алгоритма 1 следует из выполнения для построенной функции $g$ условия (1); его полнота — из произвольности выбора разбиения на шаге 1 и значений функции на шаге 2.1.

Если множества $D_i$ и $D$ конечны и $|D| = |D_i| = m$, то количество функций, обратимых типа $\forall\forall$ по переменной $x_i$, равно $m!$.

## 2. Обратимость типа ∀∃

Условие обратимости типа ∀∃ функции $g(x_1,x_2)$ по переменной $x_1$:

$$\exists f \forall x_i \exists x_2\,(f\,(g(x_i, X_2)) = x_i).$$

**Утверждение 3** (тест обратимости типа ∀∃). Функция $g: D_i \times D_2 \wedge D$ обратима типа ∀∃ по переменной $x_i$, если и только если существует такое отображение $\wedge: D_i \wedge D_2$, что выполнено условие

$$\forall_{a,b} \in D_i\,(a = b \wedge g(a, \wedge(a)) = g(b, H^{b)})). \qquad (2)$$

К сожалению, тест не конструктивен, так как требует проверки существования нужного отображения. Если отображение, удовлетворяющее условию (2), удалось найти, то функция восстановления $f: D_g \wedge D_i$ строится так:

1. Для всех $a \in D_i$ положить $f(g(a, \wedge(a))) = a$.
2. Для каждого $y \in D_g$, такого, что значение $f(y)$ не определено на шаге 1, выбрать в качестве $f(y)$ произвольное значение из $D_i$.

Функциональность отношения $f$ следует из того, что, в силу условия (2), все значения $g(a, \wedge(a))$ для $a \in D_i$ попарно различны.

**Алгоритм 2** генерации обратимой типа ∀∃ функции $g: D_i \times D_2 \wedge D$:

**1.** Положить $C = D$.

**2.** Для всех $a \in D_i$:
   2.1) выбрать случайные значения $b \in D_2$ и $c \in C$;
   2.2) положить $g(a, b) = c$;
   2.3) $C := C \setminus \{c\}$;
   2.4) для каждого $x_2 \in D_2 \setminus \{b\}$ выбрать в качестве $g(a, x_2)$ произвольное значение из $D$.

Корректность алгоритма 2: будем параллельно с функцией $g$ строить отображение $\phi : D_1 \to D_2$, полагая в шаге 2.1 $\wedge(a) = b$. Тогда для этих $g$ и $\wedge$ выполнено условие (2), поскольку шаг 2.3 обеспечивает попарную различность значений $g(a, b)$.

Полнота алгоритма 2: пусть для функции $g$ и отображения $\wedge$ выполнено условие (2). Тогда именно эта функция будет построена алгоритмом 2 при выборе значений $b = \wedge(a)$ и $c = g(a,b)$ в шаге 2.1 и значений $g(a,x_2)$ в качестве соответствующих «произвольных» в шаге 2.4.

## 3. Обратимость типа 3V

Условие обратимости типа 3V функции $g(x_1,x_2)$ по переменной $x_2$:

$$\exists f \forall x_i \forall x_2 \, (f(g(x_i,x_2)) = x_2).$$

**Утверждение 4** (тест обратимости типа 3V). Функция $g : D_1 \times D_2 \to D_g$ обратима типа 3V по переменной $x_2$, если и только если существует такое $a \in D_1$, что

$$|G_a| = |D_2|. \qquad (3)$$

Функция восстановления $f : D_g \to D_2$ строится так:

1. Для $a \in D_i$, удовлетворяющего условию (3), и каждого $x_2 \in D_2$ положить $f(g(a, x_2)) = x_2$.
2. Для каждого $y \in D_g$, такого, что значение $f(y)$ не определено на шаге 1, выбрать в качестве $f(y)$ произвольное значение из $D_2$.

Функциональность отношения $f$ следует из того, что, ввиду условия (3), значения $g(a, x_2)$, $x_2 \in D_2$, попарно различны.

**Алгоритм 3** генерации обратимой типа 3V функции $g : D_1 \times D_2 \to D$:

1. Выбрать случайное значение $a \in D_i$.
2. Положить $C = D$.
3. Для всех $b \in D_2$:
   - 3.1) выбрать случайное значение $c \in C$;
   - 3.2) положить $g(a, b) = c$;
   - 3.3) $C := C \setminus \{c\}$.
4. Для всех $x_i \in D_i \setminus \{a\}$:
   - 4.1) для каждого $x_2 \in D_2$ выбрать в качестве $g(x_i, x_2)$ произвольное значение из $D$.

Корректность алгоритма 3: шаг 3 обеспечивают выполнение условия (3) для значения $a$, выбранного на шаге 1. Полнота доказывается так же, как для алгоритма 2.

Пусть все множества $D_1, D_2, D$ конечны и $D_2 = \{b_1, \ldots, b_m\}$. Для подсчёта количества обратимых типа 3V функций вычислим количество необратимых. Условие необратимости (отрицание теста) можно записать так:

$$\forall a \in D_i \, (|G_a| < |D_2|). \qquad (4)$$

Для $a \in D_i$ рассмотрим вектор $g(a, b_i), \ldots, g(a, b_m)$; существует всего $|D|^{|D_2|}$ различных таких векторов, из них $|D|(|D|-1)\ldots(|D|-|D_2|+1)$ состоят из попарно различных значений. Таким образом, количество необратимых функций (удовлетворяющих условию (4)) равно

$$C_{\text{необр}} = |D|^{|D_1|\cdot|D_2|} - |D|(|D|-1)\ldots(|D|-|D_2|+1).$$

Количество обратимых типа 3V функций равно

$$|D|^{|D^1|HD^{z^1}} - C_{\text{необр}};$$

в частности, для $|D| = |D_1| = |D_2| = m$ получаем $m^{m^2} - (m^m - m!)^m$.

ЛИТЕРАТУРА

1. Agibalov G. P. Cryptanalytical finite automaton invertibility with finite delay // Прикладная дискретная математика. 2019. №46. С. 27-37.
2. Agibalov G. P. Problems in theory of cryptanalytical invertibility of finite automata // Прикладная дискретная математика. 2020. № 50. С. 62-71.
3. Agibalov G. P. Cryptanalytic concept of finite automaton invertibility with finite delay // Прикладная дискретная математика. 2019. № 44. С. 34-42.

УДК 004.056 DOI 10.17223/2226308X/14/15

# ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ОДНОГО СПОСОБА КОНТРОЛЯ ЦЕЛОСТНОСТИ ПРИ ХРАНЕНИИ ДАННЫХ БОЛЬШОГО ОБЪЁМА

Д. А. Бобровский, Д. И. Задорожный, А. М. Коренева, Т. Р. Набиев, В. М. Фомичёв

Описан способ встраивания высокопроизводительного алгоритма генерации кода контроля целостности, представленного авторами на РусКрипто’2020, в функцию хэширования, определенную в ГОСТ 34.11-2018 (256 бит). Полученные ранее результаты существенно улучшены. Проведены экспериментальные исследования производительности и криптографических свойств нового алгоритма. Установлено, что предложенный алгоритм производительнее известных криптографических функций хэширования, близок по производительности к CRC32, а по криптографическим свойствам значительно его превосходит.

**Ключевые слова:** аддитивные генераторы, контроль целостности, матрично-графовый подход, перемешивающие свойства, регистры сдвига, AG-S, AG-S- Стрибог, SMHasher.

## Введение

Обеспечение целостности хранимых данных относится к основным задачам защиты информации. В настоящее время применяются различные алгоритмы и подходы: хэш-функции (MD, SHA, ГОСТ 34.11-2018 и др.), хэш-функции с ключом (HMAC), блочные шифры в режиме выработки имитовставки (CMAC). При контроле целостности (КЦ) применяются также некриптографические методы с использованием кодов, обнаруживающих и/или исправляющих ошибки (коды Хэмминга, циклические коды (CRC) и др.).

При динамическом контроле больших объёмов данных, КЦ исполняющей среды функционирования, а также при проведении оперативного аудита целевых систем возникает проблема вычислений с высокой ресурсоёмкостью. Непосредственное использование для решения данной проблемы известных подходов и алгоритмов затруднительно в силу имеющихся у них недостатков: высокой ресурсоёмкости, слабых криптографических характеристик и пр. В работе предложено альтернативное решение на основе комбинации высокопроизводительного алгоритма (например, CRC32) и хэш-функции, соответствующей современным требованиям к криптографической стойкости (например, ГОСТ 34.11-2018). Удачное решение подразумевает компромисс между скоростью

и криптографическими свойствами алгоритмов, исключающими применение вычислительно простых методов построения коллизий (примеры имеющих подобную слабость высокопроизводительных алгоритмов известны [1]).

Исследования при построении нового алгоритма были направлены на решение следующих задач:

- построение высокопроизводительных алгоритмов генерации кодов контроля целостности (ККЦ) и обоснование их свойств;
- обоснование выбора параметров для реализации конкретного алгоритма;
- определение корректной и экономной процедуры дополнения блоков данных до подходящих размеров;
- сложность поиска коллизий, а также оценка вероятности коллизий для случайных входов;
- оценка вычислительной сложности построенных алгоритмов генерации ККЦ;
- разработка способа встраивания высокопроизводительного алгоритма генерации ККЦ в функцию хэширования;
- оценка производительности и криптографических свойств построенного алгоритма.

В работе описан новый алгоритм контроля целостности хранимых данных с использованием хэширования. При реализации алгоритма массив входных данных сначала разбивается на фрагменты, для которых с помощью высокопроизводительного алгоритма генерируются уникальные ККЦ. Конкатенация полученных ККЦ образует вход криптографической хэш-функции, выход хэш-функции есть ККЦ исходных данных. Проведены экспериментальные исследования производительности и криптографических свойств этого алгоритма.

## 1. Описание комбинированного алгоритма

Схема комбинированного алгоритма КЦ дана на рис. 1. Массив входных данных $M$ произвольного размера разбивается на блоки размера 1 кбайт (8192 бита). Если длина массива $M$ не кратна размеру блока, то последний блок дополняется до 1 кбайт. Проанализированы различные алгоритмы дополнения и выбрана схема с учётом характеристик дополняемого блока.

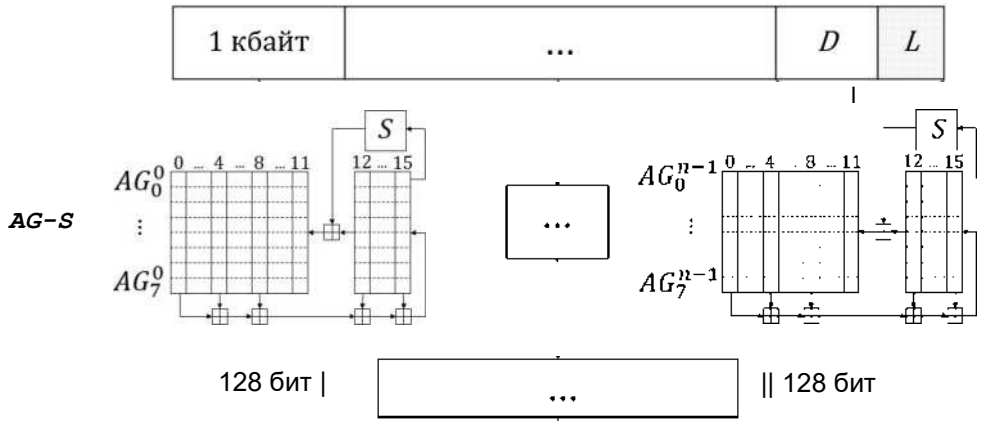



Рис. 1. Схема комбинированного алгоритма AG-S-Стрибог

Для генерации уникального ККЦ каждого блока данных размера 1 кбайт использована схема $AG$-$S$ на основе восьми аддитивных генераторов $AG_0,\ldots,AG_7$ и $S$-бокса из ГОСТ 34.11-2018. Аддитивные генераторы (AG) реализуют преобразования регистра сдвига длины 16 над множеством $V_{64}$ с функцией обратной связи, определённой в [2, 3]. Восемь тактов работы схемы обеспечивают перемешивание данных и формируют 128-битовый код.

Вход хэш-функции по ГОСТ 34.11-2018 есть конкатенация полученных ККЦ для всех блоков данных, а 256-битовое хэш-значение есть ККЦ массива данных M в целом. Алгоритм обозначен AG-S-Стрибог.

## 2. Теоретические исследования класса алгоритмов генерации ККЦ

Для класса преобразований на основе АГ и $S$-бокса (для предложенной схемы это преобразование $V_{8192} \wedge V_{8192}$) доказана биективность преобразования множества состояний $AG_0, \ldots, AG_7$. Это позволило более точно оценить вероятность совпадения ККЦ для двух различных случайных блоков. Оценена сложность поиска блоков с одинаковыми ККЦ ($2^{64}$ опробований входов для схемы из п. 1).

Получены характеристики перемешивающего орграфа, определяющие обоснованный выбор параметров для реализации конкретных преобразований. В частности, с использованием оценки локального экспонента перемешивающего графа преобразования оценена приемлемая для производительности и криптографических свойств глубина итерации преобразования. Оценена теоретическая вычислительная сложность предложенных алгоритмов.

## 3. Экспериментальные исследования

Измерена производительность генерации контрольных кодов разными алгоритмами при входных блоках 1 кбайт (табл. 1). Эксперименты проведены на ПЭВМ с процессором Intel Core i5-8600 3.1 GHz без использования процессорных инструкций SHANI, SSE4.2.

Таблица 1

**Характеристики производительности**

| Алгоритм | CRC32 | SHA2-256 | SHA3-256 | MD5 | CMAC-Magma | Стрибог | AG-S |
|---|---|---|---|---|---|---|---|
| *CpB*, такты/байт | 8,664 | 26,435 | 48,855 | 18,405 | 61,306 | 42,55 | 9,516 |

Проведено сравнение алгоритмов CRC32, MD5, SHA2-256, SHA3-256, Стрибог и AG-S с помощью набора тестов SMHasher [4] для проверки по известной методике [5] реализаций хэш-функций. В табл. 2 приведены результаты следующих тестов: Sanity — на идентичность реализации хэш-функции и её математической модели; Avalanche — на выполнение строгого лавинного критерия; Chi2 — на равномерность распределения хэш-значений с помощью статистики $X^2$; Differential — на поиск коллизий в множестве входов длины 64 и 128 бит, расстояние Хэмминга между которыми не более 5 и 4 соответственно; Collisions — на поиск коллизий и сравнение их количества с ожидаемым. Символами «+» и «-» в табл. 2 обозначено соответственно пройден тест или нет. Для тестов Differential и Collisions указана доля пройденных тестов из их общего числа.

Таблица 2

**Результаты применения набора тестов SMHasher**

| Тест | CRC32 | MD5 | SHA2-256 | SHA3-256 | Стрибог | AG-S -Стрибог |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| Sanity | + | + | + | + | + | + |
| Avalanche | _ | + | + | + | + | + |
| Chi2 | - | + | + | + | + | + |
| Differential | 1/2 | 2/2 | 2/2 | 2/2 | 2/2 | 2/2 |
| Collisions | 6/41 | 36/41 | 41/41 | 41/41 | 41/41 | 25/41 |

## Выводы

1. Алгоритм AG-S от 1,93 до 6,44 раз превышает по производительности известные функции хэширования (бесключевые и ключевые) и близок по производительности к CRC32.

2. По результатам тестов Avalanche, Chi2 и Differential алгоритм *AG-S*-Стрибог не уступает известным функциям хэширования и значительно превосходит алгоритм CRC32. Для усиления свойств алгоритма AG-S следует продолжить исследование коллизий.

ЛИТЕРАТУРА

1. Stigge M., Plotz H., Muller W., and Redlich J.-P. Reversing CRC — Theory and Practice. HU Berlin Public Report, 2006.
2. Фомичев В. М., Коренева А. М., Набиев Т. Р. О новом алгоритме контроля целостности данных // Конференция Рускрипто'20, Московская область, 2020. https://www.ruscrypto.ru/resource/archive/rc2020/files/02_koreneva_fomichev.pdf
3. *Фомичев В. М., Коренева А. М., Набиев Т. Р.* Характеристики алгоритма контроля целостности данных на основе аддитивных генераторов и s-боксов // Прикладная дискретная математика. Приложение. 2020. №13. С. 62-66.
4. https://github.com/rurban/smhasher.
5. Хэш-функция t1ha. ttps://github.com/PositiveTechnologies/t1ha.

УДК 004.056 DOI 10.17223/2226308X/14/16

# ОБ АЛГОРИТМЕ ДОПОЛНЕНИЯ БЛОКОВ БОЛЬШОГО РАЗМЕРА В СИСТЕМАХ КОНТРОЛЯ ЦЕЛОСТНОСТИ

Д. А. Бобровский, Т. Р. Набиев, В. М. Фомичёв

В алгоритмах контроля целостности при расчёте контрольной суммы файла требуется, чтобы его длина была кратна заданной величине (1 бит). При защите файла произвольной длины, как правило, выполняется его дополнение до требуемой длины. Представлена вычислительно простая и эффективная схема дополнения, предназначенная для систем контроля целостности, обрабатывающих большие блоки (порядка 1 кбайт). Схема построена на основе выходов линейного конгруэнтного генератора. Начальное состояние генератора формируется с помощью данных дополняемого блока и исходной длины файла. Результаты анализа криптографических свойств алгоритма контроля целостности и экспериментов по оценке производительности показали преимущества предложенной схемы по сравнению с известными стандартными схемами дополнения.

**Ключевые слова:** *алгоритм дополнения, широкий блок, линейный конгруэнт*

ный генератор, характеристики процедур дополнения, контроль целостности, AG-S, SMHasher.

## Введение

При работе с большими блоками (порядка 1 кбайт), например, как в алгоритме контроля целостности данных на основе аддитивных генераторов и s-боксов [1, 2], определение корректной и экономной процедуры дополнения блоков данных до подходящих размеров является одной из важнейших задач, так как для достижения хорошего перемешивания биты дополнения должны быть реализацией псевдослучайной функции.

Для сравнения проанализированы известные схемы дополнения: дополнение битами (00. . . 0, 00. . . 01), двухступенчатое дополнение (SHA, MD5). Оценена производительность и свойства предложенного алгоритма.

## 1. Описание схемы дополнения

Процедура дополнения файлов произвольной длины (в битах) до длины, кратной $l$, использует линейный конгруэнтный генератор (ЛКГ) над кольцом вычетов $Z_m$, то есть линейное преобразование $g$ кольца $Z_m$ вида

$$g(X) = (aX + c) \bmod m,$$

где $X, a, c \in Z_m$; $a = 0$; числа $a$ и $c$ суть множитель и сдвиг соответственно.

Обозначим $X_0 \in Z_m$ – начальное состояние ЛКГ; $X_{n+1} = g(X_n)$, $n > 0$. ЛКГ порождает периодическую последовательность с начальным состоянием $X_0$ и длиной периода $m$, если сдвиг нечётный и $a = 1 \pmod 4$.

Пусть $D \in V^*$ – исходный файл, представимый как битовая последовательность, где $V^*$ –множество всех двоичных строк конечной длины; $D_0$ – последний неполный блок файла $D$. Если длина $p$ блока $D^0$ меньше $l$, то он дополняется до длины $l$ блоком $L$ длины $l - p$, и дополненный блок имеет вид $D^0 | L$ ($|$ означает присоединение).

Блок $L$ длины $l - p$ вырабатывается следующим образом:

1. Формируется начальное значение ЛКГ $X_0$:
   а) строке $P$ присваивается значение $D^0$, т. е. $P = D^0$;
   б) строка $P$ дополняется нулями до длины, кратной $r = 64$, $P' = (P \| 0^{r-(p \bmod r)})$; т. е. $P'$ =
   в) строка $P'$ разбивается на $\lceil p/r \rceil$ блоков длины $r$: $P' = (P_1 | \ldots | P_{\lceil p/r \rceil})$, где $P_1, \ldots, P_{\lceil p/r \rceil} \in V_r$;
   г) $X_0 = (P_1 \boxplus \ldots \boxplus P_{\lceil p/r \rceil}) \lll ((p/8) \bmod 64)$, где $a \lll b$ – операция циклического сдвига элементов строки $a$ на $b$ позиций; $\boxplus$ – сложение по модулю $2^r$.
2. С помощью ЛКГ [3] с начальным значением $X_0$ и параметрами

$$a = 6364136223846793005,\ c = 1442695040888963407,\ m = 2^{64}$$

порождается последовательность $\lceil (l - p)/r \rceil$ элементов $\{X_1, \ldots, X_{\lceil (l-p)/r \rceil}\}$, из которых формируется строка $L'$:

$$L' = (X_1 \| \ldots \| X_{\lceil (l-p)/r \rceil}).$$

3. Дополнение $L$ образуют старшие $l - p$ бит строки $L'$.

## 2. Экспериментальное сравнение характеристик процедур дополнения

С помощью экспериментов исследованы следующие процедуры дополнения:

1) дополнение нулями;
2) дополнение битовым вектором (100. . . 000);
3) дополнение битовым вектором (100... 000)|| Л, где Л — запись длины дополняемой строки (для записи требуется 2 байта);
4) дополнение в соответствии с процедурой, описанной в п. 1.

Обозначим данные процедуры дополнения как Padding 1, . . . , Padding 4 соответственно.

### 2.1. Продолжительность выполнения операции дополнения

Проведено сравнение производительности процедур дополнения входных векторов. В ходе эксперимента сгенерировано по 20000 случайных входных строк длины L, которые дополнялись до длины 1024 байта, длина L изменялась от 100 до 1000 с шагом 100 байтов.

Программная реализация процедур дополнения выполнена на языке программирования C++. Эксперименты проведены на ПЭВМ с процессором Intel(R) Core(TM) i5-8600 с постоянной тактовой частотой U = 4,1 ГГц, архитектура операционной системы 64-битная (x64). Оптимизация программного кода — /O2.

Время t, затраченное на формирование дополненного блока длины 1024 байт, измерялось с помощью системных часов реального времени стандартной библиотеки std::chrono.

По формуле tU/L рассчитано среднее время, затраченное на дополнение, а также независимая от частоты процессора характеристика производительности процедуры — среднее количество тактов на байт (CpB). Результаты экспериментов приведены в табл. 1 и на рис. 1.

Таблица 1

**Результаты замера скорости процедуры дополнения**

| Характеристика | Padding 1 | Padding 2 | Padding 3 | Padding 4 |
|---|---|---|---|---|
| Среднее время дополнения, нс | 148 | 189 | 204 | 320 |
| Среднее число тактов на байт, *CpB* | 1,475 | 2,266 | 2,399 | 3,452 |

По результатам эксперимента длительность дополнения с помощью ЛКГ больше, чем у других процедур, от 1,5 до 2 раз. Однако важно, что в системах контроля целостности файлов произвольной длины, использующих алгоритмы с большим блоком, например алгоритм AG-S [1], время генерации кода контроля целостности без учёта дополнения составляет 7100 нс. Следовательно, суммарное время с процедурой дополнения нулями составляет 7248 нс, а с предложенной процедурой дополнения — 7420 нс, т. е. общее замедление незначительно и не превышает 2,37 %. Значит, с учётом общей продолжительности генерации кода процедура дополнения на основе ЛКГ другим процедурам существенно не уступает.

### 2.2. Криптографические характеристики процедур дополнения

При анализе алгоритмов генерации кодов контроля целостности важные криптографические характеристики связаны с равномерностью распределения хэш-значений, оценкой лавинного эффекта, поиском коллизий и производительностью хэш-

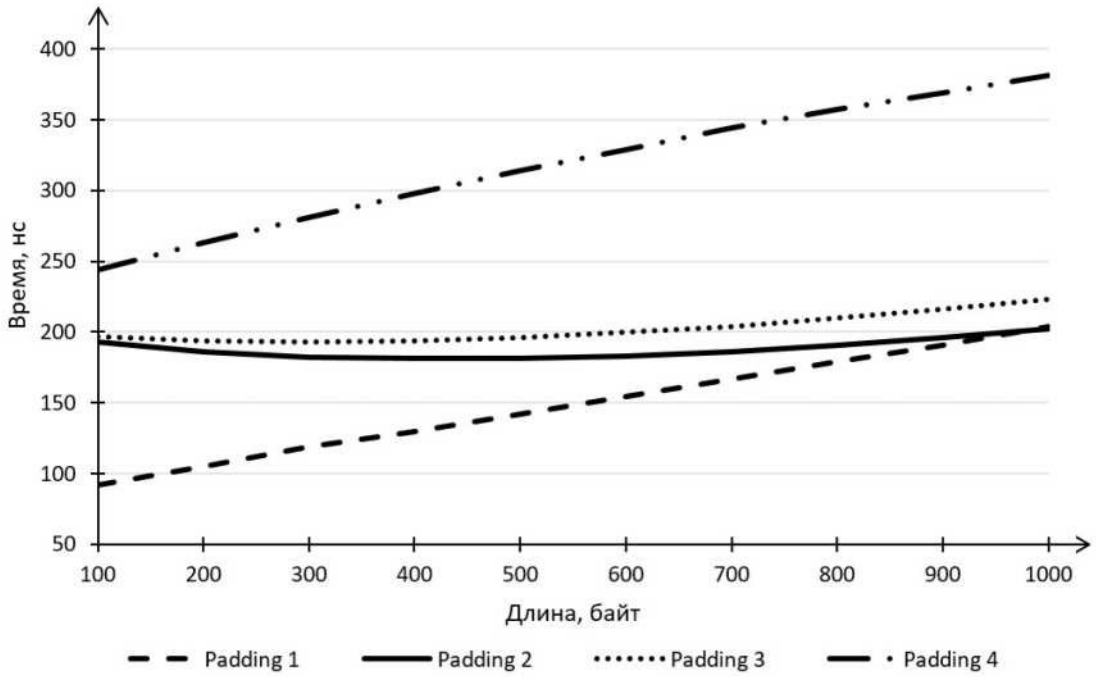



Рис. 1. Зависимость времени дополнения от размера входного блока

функций. Статистические испытания были выполнены с помощью хорошо зарекомендовавшего себя на практике тестового пакета SMHasher [3]. В 2017 г. компания «Positive Technologies» использовала данный пакет тестов для тестирования разработанной функции хэширования [4]. Этот набор тестов (open-source продукт) предназначен для тестирования указанных криптографических характеристик.

При тестировании за основу был взят алгоритм $AG$-$S$-Стрибог [2]. Были подготовлены четыре реализации, где входы дополнялись процедурами дополнения Padding 1- Padding 4. Сравнительные результаты тестирования данных реализаций с помощью тестов SMHasher представлены в табл. 2-4.

Криптографические свойства реализаций в связи с процедурой дополнения были протестированы пакетом SMHasher, а именно группами тестов: «Avalanche» — на выполнение строгого лавинного критерия; «Sparse» — на поиск коллизий среди входов с большим количеством нулевых битов; «Permutation» — на поиск коллизий среди входов, составленных из повторяющихся блоков.

Таблица 2

**Общие результаты тестирования (количество пройденных тестов)**

| Группа тестов | Padding 1 | Padding 2 | Padding 3 | Padding 4 | Всего тестов |
|---|---|---|---|---|---|
| «Avalanche» | 6 | 6 | 12 | 12 | 12 |
| «Sparse» | 7 | 7 | 7 | 9 | 11 |
| «Permutation» | 0 | 2 | 2 | 2 | 15 |
| Общее число пройденных тестов | 13 | 15 | 21 | 23 | 38 |

Суммарное количество пройденных тестов реализации с процедурой дополнения на основе выходов ЛКГ больше, чем при других процедурах дополнения. Группа тестов «Avalanche» полностью пройдена при двухступенчатом дополнении и при дополнении на основе выходов ЛКГ.

Результаты по группам тестов «Sparse» и «Permutation» представлены в табл.

3 и 4.

Таблица 3

**Количество коллизий при различных длинах входа в группе тестов «Sparse»**

| Размер входного вектора, бит | Padding 1 | Padding 2 | Padding 3 | Padding 4 | Всего входных векторов |
|---|---|---|---|---|---|
| 72 | 241644 (0,016 %) | 259209 (0,017%) | 109595 (0,007%) | 0 | 15082603 |
| 96 | 46809 (0,013 %) | 48817 (0,014%) | 28666 (0,008%) | 0 | 3469497 |
| 160 | 719293 (0,026 %) | 724939 (0,024 %) | 468548 (0,017%) | 77968 (0,003 %) | 26977161 |
| 256 | 179226 (0,064 %) | 170800 (0,061 %) | 131358 (0,047%) | 5465 (0,002 %) | 2796417 |
| Всего коллизий | 1186972 | 1203765 | 738167 | 83433 | 48325678 |
| Доля коллизий среди всех входов | 0,024562 | 0,024909 | 0,015275 | 0,001726 | |

Применение процедуры дополнения на основе ЛКГ в группе тестов «Sparse» снижает количество коллизий примерно от 9 до 14 раз, что положительно характеризует её криптографические свойства.

Таблица 4

**Количество коллизий в группе тестов «Permutation»**

| Параметр | Padding 1 | Padding 2 | Padding 3 | Padding 4 | Всего входных векторов |
|---|---|---|---|---|---|
| Общее число коллизий по всем тестам | 8217021 | 6622245 | 6089853 | 4256492 | 20143432 |
| Доля коллизий среди всех входов | 0,407926 | 0,328755 | 0,302324 | 0,211309 | |

Применение процедуры дополнения на основе ЛКГ в группе тестов «Permutation» снижает количество коллизий примерно от 1,5 до 2 раз.

## Выводы

1. Процедура дополнения на основе ЛКГ продолжительнее стандартных процедур дополнения от 1,5 до 2 раз, однако при этом общая продолжительность генерации кода другим процедурам существенно не уступает, замедление составляет не более 2,37 %.

2. На примере алгоритма AG-S-Стрибог экспериментально показано, что процедура дополнения на основе ЛКГ может обеспечить преимущества перед другими известными процедурами по ряду важных криптографических свойств.

ЛИТЕРАТУРА

1. *Фомичев В. М., Коренева А. М., Набиев Т. Р.* Характеристики алгоритма контроля целостности данных на основе аддитивных генераторов и s-боксов // Прикладная дискретная математика. Приложение. 2020. №13. С. 62-66.
2. *Бобровский Д. А., Задорожный Д. И., Коренева А. М. и др.* О контроле целостности данных с использованием хэширования // Рускрипто'21, Московская область, 2021. https://www.ruscrypto.ru/resource/archive/rc2021/files/02_bobrovskiy_ zadorozhniy_koreneva_nabiyev_fomichev.pdf.
3. https://github.com/rurban/smhasher.
4. Хэш-функция t1ha. https://github.com/PositiveTechnologies/t1ha.

УДК 004.056.55 DOI 10.17223/2226308X/14/17

# ПОРОГОВАЯ СХЕМА ПРОТОКОЛА ДИФФИ — ХЕЛЛМАНА

Д. Н. Колегов, Ю. Р. Халниязова

Предлагается пороговая схема протокола Диффи — Хеллмана на эллиптических кривых, которая позволяет создавать и хранить закрытый ключ участника протокола распределённым образом без необходимости восстановления ключа для выполнения криптографических операций на этом ключе.

**Ключевые слова:** пороговая криптография, протокол Диффи — Хеллмана, эллиптические кривые.

Пусть $\mathrm{sk}$ – закрытый ключ участника протокола Диффи – Хеллмана. Будем называть функцией Диффи — Хеллмана функцию $\mathrm{DH}(\mathrm{sk}, \mathrm{Q})$, которая принимает на вход закрытый ключ $\mathrm{sk}$ (скаляр) и точку $\mathrm{Q}$ на эллиптической кривой и возвращает точку $sk \bullet Q$. Под протоколом Диффи – Хеллмана обычно понимают следующую последовательность вычислений ($G$ – образующий элемент подгруппы простого порядка $q$ группы точек эллиптической кривой $E$ над конечным полем):

1) Алиса генерирует случайное число $\mathrm{a} \in \mathrm{Z_q}$, вычисляет значение $\mathrm{A} = DH(a, O')$ и отправляет его Бобу;
2) Боб генерирует случайное число $b \in \mathrm{Z_q}$, вычисляет значение $B = DH\,(b, G)$ и отправляет его Алисе;
3) Алиса вычисляет общий секрет как $K = DH(a, B)$, а Боб– как $K = DH(b, A)$.

Идея пороговой схемы Диффи – Хеллмана заключается в том, чтобы сгенерировать закрытый ключ участника протокола $x$ с помощью распределённого алгоритма некоторыми сущностями, а затем делегировать им вычисление значения функции $DH(x, Q)$, используя методы пороговой криптографии. Будем называть таких сущностей агентами, а участником протокола Диффи – Хеллмана будем называть группу агентов, которая представляет одну из сторон протокола Диффи – Хеллмана и выполняет установленные протоколом шаги.

Если в классическом протоколе Диффи – Хеллмана участником является атомарная сущность (человек, процесс и т. д.), то теперь участник протокола – это группа сущностей – агентов (людей, процессов, . . . ), которые взаимодействуют между собой посредством разработанных протоколов так, что для внешних сущностей (другого участника протокола, сторонних наблюдателей и т. д.) группа агентов неотличима от обычного участника протокола Диффи – Хеллмана. При этом по результатам выполнения этих протоколов любой из агентов знает открытый ключ группы и может представлять группу при взаимодействии с другим участником протокола. Так как группа агентов неотличима для внешних сущностей от обычного участника, то для простоты изложения далее будем считать, что только один из участников протокола Диффи – Хеллмана представлен группой агентов. При этом неважно, какой именно из участников протокола состоит из агентов, так как вычисления, выполняемые участниками, симметричны.

Первым этапом предлагаемой схемы является генерация долей закрытого ключа, а также вычисление открытого ключа соответствующего участника протокола Диффи – Хеллмана. Вычисленный открытый ключ известен каждому агенту из группы, а соответствующий закрытый ключ неизвестен никому и существует только в виде сгенерированных долей. Этот этап описывается протоколом генерации ключей.

Протокол генерации ключей основан на идее распределенной генерации ключей,

которая строится с использованием проверяемой схемы разделения секрета Фельдмана [1]. Каждому агенту $P_j$ ставится в соответствие индекс, который определяет получаемую им долю в схеме Фельдмана. Для простоты будем считать, что индексом агента $P_j$ является значение $j$ (в качестве индексов могут быть использованы любые значения, на которых определены многочлены схемы Фельдмана, если эти значения различны для всех агентов; они устанавливаются на фазе подготовки, не являются секретными и должны быть известны всем агентам). Тогда во всякой схеме Фельдмана агент $P_j$ получает долю $f(j)$, где $f$ — многочлен схемы Фельдмана. При этом генерация итоговых долей на агентах происходит без участия дилера, в результате чего секретная доля закрытого ключа каждого агента известна только ему самому. Это достигается за счёт того, что каждый агент по очереди выступает в роли дилера в схеме Фельдмана, разделяя некоторое случайное значение $u_i$, а затем благодаря свойству схемы Фельдмана (сумма долей $a_i$ и $b_i$ от значений $a$ и $b$ соответственно является долей от значения $a + b$) агенты, складывая полученные значения, получают новые доли от значения $x = \sum_i u_i$, которое не было разделено явным образом.

В ходе протоколов агенты обмениваются открытыми значениями друг с другом, используя схемы обязательств для фиксации передаваемых значений. Обозначения, использованные для описания протоколов, взяты из [2]:

1) Каждый агент $P_i$ выбирает случайное значение $u_i \in_R Z_q$ и вычисляет $[KGC_i, KGD_i] = Com(y_i)$, где $y_i = u_i \cdot G$; $Com$ — алгоритм схемы обязательства; $KGC_i$ — вычисленное с помощью алгоритма обязательство; $KGD_i$ — строка, позволяющая его раскрыть. Затем агент отправляет $KGC_i$ всем агентам.
2) Каждый агент $P_i$ отправляет $KGD_i$ всем агентам, а затем разделяет значение $u_i$ между всеми агентами, используя $(t, n)$-схему Фельдмана. Открытый ключ соответствующего участника протокола Диффи — Хеллмана равен $y = \sum_i y_i = \sum_i u_i \cdot G$.
3) Каждый агент складывает доли, полученные в схемах Фельдмана, для вычисления своей закрытой доли $x_i$. Итоговое значение закрытой доли агента $x_i$ является долей от закрытого ключа $x = \sum_i x_i$ в $(t, n)$-схеме Шамира. При этом закрытый ключ $x$ не восстанавливается ни в какой момент выполнения протокола и существует только в форме долей.

Для вычисления общего секрета предлагается протокол выработки общего секрета. Получая на вход открытый ключ $Y$ другого участника протокола Диффи — Хеллмана, агенты вычисляют общий секрет $S = x * Y$, используя свои доли закрытого ключа, при этом не раскрывая их в ходе протокола:

1) Каждый агент $P_i$ вычисляет коэффициент Лагранжа $\lambda_i$ и значение $w_i = \lambda_i x_i$, которое является долей данного агента в аддитивной $(t — 1, t)$-схеме разделения секрета от значения $x$. Здесь $\lambda_i$ — значение $i$-го базисного многочлена в схеме интерполяции Лагранжа в точке 0.
2) Агент вычисляет значения $S_i = w_i \cdot Y$, $[EXC_i, EXD] = Com(S_i)$, где $Com$ — это алгоритм схемы обязательства, $EXC_i$ — вычисленное с помощью алгоритма

обязательство и $EXD_i$ — строка, позволяющая его раскрыть. Затем агент отправляет $EXC_i$ другим участникам.

3) Агенты отправляют друг другу значения $EXD_i$. Общий секрет равен $S = \sum_i S_i$.

Пороговая схема позволяет расширить число сценариев применения протокола Диффи — Хеллмана, в том числе представляет возможность улучшения свойств безопасности закрытых ключей участников протокола Диффи — Хеллмана: если в классической схеме злоумышленнику достаточно получить доступ к узлу сети, который хранит соответствующий закрытый ключ, то теперь необходимое количество узлов зависит от порога и всегда больше единицы.

Предложенная схема реализована для протоколов Диффи — Хеллмана на кривых Curve25519 и NIST P-256.

Препринт статьи доступен на arxiv.org [3].

ЛИТЕРАТУРА

1. Feldman P. A Practical Scheme for Non-interactive Verifiable Secret Sharing. http://www.cs.umd.edu/~gasarch/TOPICS/secretsharing/feldmanVSS.pdf.
2. Gennaro R. and Goldfeder S. Fast Multiparty Threshold ECDSA with Fast Trustless Setup. https://eprint.iacr.org/2019/114.
3. Kolegov D., Khalniyazova Yu., and Varlakov D. Towards Threshold Key Exchange Protocols. https://arxiv.org/abs/2101.00084.

УДК 003.26 + 004.056 DOI 10.17223/2226308X/14/18

# ИСПОЛЬЗОВАНИЕ РОССИЙСКИХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В ПРОТОКОЛЕ БЕЗОПАСНОСТИ СЕТЕВОГО УРОВНЯ WireGuard[13]

Д. Н. Колегов, Ю. Р. Халниязова

Рассматривается криптографический протокол WireGuard, предназначенный для обеспечения защищённости сетевого уровня TCP/IP и построенный с использованием российских криптографических алгоритмов. Необходимость разработки такого протокола вызвана потребностью в применении WireGuard в отечественных перспективных распределённых и облачных технологиях, построенных с применением средств криптографической защиты информации. Описывается решение данной задачи: выбор примитивов, их внедрение, альтернативные подходы, аспекты программной реализации и тестирования, основные текущие результаты работы, а также актуальные направления исследования. Разработанная спецификация и референсная реализация могут быть использованы в качестве отправной точки для разработки рекомендаций по стандартизации протокола WireGuard с российскими криптографическими алгоритмами.

**Ключевые слова:** WireGuard, GOST, VPN.

В настоящее время в области защищённых сетевых технологий активно исследуются, разрабатываются и применяются протоколы семейства Noise Protocol Framework. Основным протоколом здесь является WireGuard, с недавнего времени также поддерживаемый в ядре Linux.

WireGuard — это свободно распространяемое программное обеспечение с открытым исходным кодом, предназначенное для замены устаревшего протокола IPsec и его

[13]Работа выполнена ООО «Безопасная информационная зона» и НПО «Криптонит» в рамках совместного исследовательского проекта.

реализаций. Несомненными достоинствами WireGuard по сравнению со схожими по назначению программными средствами с открытым исходным кодом, такими, как OpenVPN, Strongswan, Libreswan, Linux XFRM и другими системами с закрытым исходным кодом, реализующими технологии VPN на базе IPsec, являются:

— небольшой размер исходного кода (примерно 3800 LoC на июнь 2020);
— простота дизайна протокола и его конечно-автоматной модели и, как следствие, достижимость простоты программной реализации на практике;
— наличие встроенных в протокол средств защиты от DoS-атак, сетевого сканирования и фаззинга;
— относительная простота верификации как протокола, так и его программной реализации;
— соответствие современным криптографическим требованиям;
— формальная верификация свойств безопасности протокола (считается, что протокол WireGuard в текущей версии, использующей Curve25519, верифицирован);
— высокая производительность.

В настоящее время в зарубежной программной разработке, связанной с сетевыми криптографическими протоколами, повсеместно внедряются реализации и адаптации протоколов семейства Noise в целом и WireGuard в частности. Драйверами этих процессов являются разработка протоколов с постквантовыми криптографическими примитивами, а также развитие технологий SDN/SD-WAN, Service Mesh и MPC.

Кратко перечислим лишь самые основные из них:

— протокол nQUIC, созданный компанией Cloudflare и используемый вместо TLS для протокола QUIC, разрабатываемого в качестве замены TCP;
— постквантовая версия протокола WireGuard, использующая постквантовые криптографические алгоритмы и, несмотря на это, показавшая большую производительность, чем IPsec на базе Curve25519 или OpenVPN;
— VPN Flannel;
— применение WireGuard для защиты транспорта в Kubernetes;
— оверлейная сеть Nebula компании Slack;
— фрэймворк libp2p.

В связи с вышесказанным представляется логичным разработать российскую версию протокола WireGuard, использующую отечественные криптографические алгоритмы.

В 2019 г. в ТК26 было направлено предложение по началу работ для стандартизации Noise/WireGuard. На тот момент этот вопрос никого в Комитете не заинтересовал и поддержки не получил. Несмотря на это, исследовательским подразделением компании BI.ZONE был проведён ряд исследовательских работ по возможности применения криптографических протоколов семейства Noise в облачных и сетевых технологиях: — исследована и обоснована возможность применения постквантовых алгоритмов

в протоколе QUIC;

— разработан прототип протокола управления WireGuard с использованием пороговой криптографии;
— исследована возможность построения пороговой версии WireGuard на произвольных эллиптических кривых.

Поводом к исследованиям по пороговой версии WireGuard стала публикация в 2019 г. множества работ, выявивших уязвимости в технологиях HSM, TPM и Intel SGX (например, plundervault). Это свидетельствует о том, что использование

технологий HSM, TPM, TEE само по себе не говорит о защищённости системы. Данные системы сложны в управлении, а их пользователи не имеют полного контроля над ними. В настоящее время альтернативным методом получения подобных функциональных свойств считается применение технологий Multi-Party Computation и Threshold Cryptography в протоколах распределения ключей (key agreement in a threshold setting). Так как BI.ZONE активно исследует возможность применения протоколов Noise в своих сервисах, нас заинтересовала возможность построения пороговой версии протокола, что позволило бы решать задачу обеспечения главных ключей не стандартными способами с помощью HSM и TPM, а с использованием криптографических алгоритмов. С удивлением было обнаружено, что данным вопросом в мире не интересуются, несмотря на то, что уже разработаны и активно исследуются пороговые схемы алгоритмов криптографической подписи ECDSA, построенные на том же математическом аппарате.

Причина этого в том, что основным источником таких задач выступают технологии криптовалюты и блокчейн, а не сетевые и облачные технологии. Разработка пороговой схемы WireGuard позволяет обеспечить безопасность закрытого статического ключа WireGuard для клиента и/или сервера, но не с помощью аппаратных методов защиты, применяемых в HSM, TPM и TEE, а с помощью пороговой криптографии.

В таблице приведены алгоритмы, определённые в предлагаемой спецификации. Все алгоритмы используют 256-битные значения входных и выходных параметров. Более подробно начальные предложения по замене криптографических алгоритмов представлены в [1, 2]. Референсная реализация протокола Ru-WireGuard доступна в репозитории [3].

| Тип алгоритма | Замена |
|---|---|
| Алгоритм согласования ключа | ГОСТ Р 34.10-2012 VKO или DH |
| Эллиптическая кривая | ГОСТ Р 34.10-2012 GC256A |
| Хэш-функция | ГОСТ Р 34.11-2012 |
| HMAC | ГОСТ Р 34.11-2012 |
| KDF | ГОСТ Р 34.11-2012 KDFTREE или HKDF |
| AEAD | ГОСТ Р 34.12-2015 Кузнечик в режиме MGM |

Для проверки корректности спецификации и программной реализации разработаны три независимых прототипа: два на языке Go и один на языке C. Проведено тестирование возможности работы друг с другом всех прототипов, получены контрольные векторы для основных криптографических значений протокола.

Разработка высокопроизводительной версии протокола не была целью, но, несмотря на это, мы провели базовое тестирование производительности. Ru-WireGuard в настоящее время значительно медленнее wireguard-go. Связано это, во-первых, с тем, что сами по себе криптоалгоритмы оригинального протокола WireGuard быстрее выбранных алгоритмов ГОСТ, а во-вторых, они реализованы на Go Assembler.

Результаты данной работы:

— представлена эталонная реализация протокола Ru-WireGuard;
— исследована производительность полученной референсной реализации в сравнении с оригинальной реализацией wireguard-go;
— проведено тестирование на ошибки спецификации;
— представлены контрольные векторы.

ЛИТЕРАТУРА

1. BI.ZONE. Проект протокола Ru-WireGuard. https://github.com/bi-zone/ruwireguard- spec.

2. Ru-WireGuard: Использование российских криптографических алгоритмов в протоколе безопасности сетевого уровня WireGuard. https://bit.ly/3mChAdq.

3. Reference implementation of the Ru-WireGuard protocol in Go. https://github.com/ bi-zone/ruwireguard-go.

УДК 519.7 DOI 10.17223/2226308X/14/19

# АЛГЕБРАИЧЕСКИЙ КРИПТОАНАЛИЗ НИЗКОРЕСУРСНЫХ ШИФРОВ SIMON И SPECK[14]

А. В. Куценко, Н. Д. Атутова, Д. А. Зюбина, Е. А. Маро, С. Д. Филиппов

Представлены алгебраические атаки на шифры Simon и Speck —два семейства низкоресурсных блочных шифров, имеющих LRX- и ARX-структуры соответственно. Они были представлены Агентством национальной безопасности США в 2013 г., а затем стандартизированы ISO как часть стандарта радиоинтерфейса RFID. Шифры алгебраически кодируются и получаемые системы булевых уравнений решаются с помощью различных SAT-решателей, а также методов, основанных на линеаризации. Впервые к этим шифрам применяются подходы, использующие разреженность систем булевых уравнений. Оценены параметры линеаризации в системах уравнений для обоих шифров. Приведено сравнение эффективности используемых методов.

**Ключевые слова:** алгебраический криптоанализ, блочный шифр, низкоресурсный шифр, Simon, Speck.

Низкоресурсная криптография — направление исследований, представляющее интерес в настоящее время. Это связано с тем, что влияние и использование RFID-меток, ПЛИС, смарт-карт, мобильных телефонов, сенсорных сетей и других криптографических алгоритмов для устройств с ограничениями на используемые ресурсы постоянно растёт и приобретает всё большую важность. Низкоресурсные криптографические примитивы предназначены для обеспечения эффективности и безопасности при ограниченном объёме ресурсов. В этом случае возникает проблема поиска компромисса между безопасностью и эффективностью. В 2013 г. Агентство национальной безопасности США представило семейства Simon и Speck низкоресурсных блочных шифров. Шифр Simon был оптимизирован для производительности на аппаратных устройствах, а Speck — для производительности в программном обеспечении. Но было подчеркнуто, что оба семейства работают исключительно хорошо как в аппаратном, так и в программном обеспечении, обеспечивая гибкость платформы, требуемую будущими приложениями. По состоянию на октябрь 2018 г. шифры Simon и Speck были стандартизированы Международной организацией по стандартизации (ISO) в рамках стандарта радиоинтерфейса RFID (радиочастотной идентификации). Эти шифры являются представителями LRX- и ARX-структур блочных шифров, основой которых является явное использование нелинейных алгебраических операций вместо S-блоков. Это обуславливает интерес к алгебраическому анализу данных шифров. Алгебраический анализ Simon проведён в [1], комбинация алгебраического и

[14]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке лаборатории криптографии JetBrains Research; работа первого автора выполнена при поддержке РФФИ (проект № 20-31-70043).

усечённого дифференциального криптоанализа шифра Simon от малого числа раундов рассмотрена в [2]. Алгебраические атаки представлены SAT-решателем и алгоритмом ElimLin.

Основная идея алгебраического криптоанализа состоит в составлении сложной системы булевых уравнений, описывающих преобразование шифра. Система строится на основе полностью известного алгоритма шифрования. Зашифрование на неизвестном криптоаналитику ключе некоторого количества открытых текстов позволяет провести подстановку в уравнения системы значений векторов открытых текстов и шифртек- стов. На следующем этапе осуществляется решение системы с помощью различных методов относительно битов ключа.

Для анализа шифров было автоматизировано построение системы уравнений, описывающей преобразования раундов шифров.

Simon – семейство низкоресурсных блочных шифров, разработанных для оптимальной производительности аппаратного обеспечения [3]. Имеет структуру классической схемы Фейстеля, на каждом раунде $2n$-битный вход раунда делится на две $n$-битные половины. К левой половине $L$ применяется раундовая нелинейная небиективная функция $F : F_n \wedge F_n$. К выводу функции применяется операция XOR с правой половиной $R$ и ключом $k$, и две половины меняются местами (рис. 1).

Для шифра Simon, вводя новую переменную для каждого выхода побитовой операции ©, для описания $T$ раундов получаем $n(T - 2)$ квадратичных уравнений с $n(T - 2) + k$ неизвестными, где $n$ – размер слова; $T$ – количество раундов; $k$ – длина ключа. При генерации ключа получается $n(T - m)$ уравнений. В результате для шифра Simon с $T$ раундами генерируется $n(T - m) + n(T - 2)$ уравнений. Количество ключей $m$ зависит от размера входного блока $2n$ и количества раундов $T$.

Speck – семейство низкоресурсных блочных шифров, обеспечивающих отличную производительность как в аппаратном, так и в программном обеспечении, но оптимизированных для работы на микроконтроллерах [3]. В каждом раунде $2n$-битных входа делятся на две $n$-битные половины. Каждый раунд Speck применяет операции конъюнкции, циклического сдвига влево и вправо, а также сложения по модулю $2^n$. Параметры имеют следующие значения: $a = 7$ и $в = 2$, если $n = 16$ (размер блока равен 32) и $a = 8$ и $в = 3$ в противном случае. На рис. 2 представлена схема шифрования данного шифра. Ключевое расписание шифра Speck использует раундовую функцию для генерации раундовых ключей.

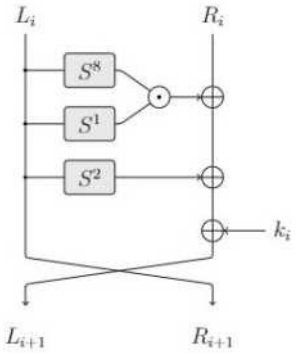



Рис. 1. Схема раундового преобразования шифра Simon [3]

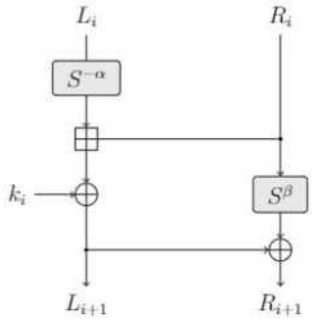



Рис. 2. Схема раундового преобразования шифра Speck [3]

В шифре Speck, вводя на каждом раунде новые переменные, получим следующие

количества уравнений и неизвестных:

$$(7n - 3)(T - 1)+(8n-3)(T - 1)+2n, 2(8n - 3)(T \quad m= 1,$$
$$- 1)+2n, n(5T - 4), m = 1, n(6T - 5), m = 2, \quad m= 2,3,4,$$
$$3, 4.$$

где $e$ — число уравнений; $u$ — число неизвестных.

## 1. Линеаризация

Проведение криптоанализа на небольшом количестве раундов (например, 3 и 4) с выбором стандартных характеристик нецелесообразно, так как ключи не строятся на основе исходных и между ними не будет никакой связи. Поэтому в данной работе рассматриваются шифры с $m=1$ для $T E\{3, 4\}$.

Рассмотрены атаки, основанные на линеаризации. Идея простой линеаризации состоит в том, чтобы присвоить каждому одночлену исходной системы новую переменную. Система после переобозначения становится линейной и решается, например, методом Гаусса. Затем для решений линейной системы проверяется, являются ли они решениями исходной нелинейной системы уравнений.

Количество различных одночленов в исходной системе определяет количество переменных $n'$ в системе линейных уравнений, эффективность линеаризации зависит от ранга $r$ этой системы. Множество решений не пусто, его мощность равна $2^{n'-r} > 0$, поэтому для оценки производительности необходимо проанализировать границы значений $n'$ и $r$.

Рассматривая алгоритм шифрования, можем оценить количество различных мономов для каждого раунда шифра Simon. Для каждой операции вводятся новые переменные и проводится переобозначение при замене $L_{i+1}$ и $R_{i+1}$; в результате получаем следующую оценку количества мономов $M$:

$$M 6 6nT.$$

В шифре Speck основным методом сохранения степени является введение новых переменных для выходных битов нелинейных операций. В этом случае степень не будет превышать $2$. На каждом раунде вводится $28n$ новых переменных. В системе уравнений, описывающей сложение по модулю $2^n$, имеется всего $5(7n - 8)$ мономов. На практике оказалось, что различных мономов в системе уравнений сложения по модулю $2^n$ не больше $25n - 18$. Таким, образом, количество различных мономов на каждом раунде шифра Speck не больше $28n - 18$. Итоговая оценка числа различных мономов, исключая такие, которые образуются при генерации ключей (все уравнения линейны), имеет вид

$$M 6 (28n - 18)T.$$

XL-атака представлена в [4, 5]. На вход поступает система из $m$ полиномиальных уравнений от $n$ неизвестных степени $d$, выбирается степень $D > d$, все уравнения исходной системы умножаются на одночлены степени $D - d$ или меньше, система линеаризуется и на выходе получаем одно или несколько решений.

Для случая $d = 2$ и $D = d + 1$ анализ этой атаки [6] показывает, что единственное решение, вероятно, будет найдено, если $m \sim n^2/6$.

Алгоритм ElimLin описан в [7]. Его суть— поиск скрытых линейных уравнений, существующих в идеале, порождённом данной системой уравнений. Этот алгоритм состоит из двух последовательных шагов:

1) исключение Гаусса: в линейной оболочке исходной системы отыскиваются все линейные уравнения;
2) замена: переменные итеративно выражаются с помощью найденных линейных уравнений, получаемые выражения подставляются в исходную систему.

В табл. 1 и 2 приведены результаты для простой линеаризации, XL-метода и ElimLin. Полученные данные позволяют сравнить эффективность этих методов для Simon и Speck. Для XL-метода $D = 3$. Сложность полного перебора составляет $2_{16}$ (при $n = 16,\ m = 1$). Как видно из табл. 1, метод линеаризации начиная с 4-5 раундов даёт худшие результаты, чем атака полным перебором. Использование метода простой линеаризации для $T > 4$ и XL-метода для пяти раундов (шифра Simon) не улучшает поиск решения по сравнению с полным перебором.

Таблица 1

**Результаты применения атак, основанных на линеаризации**

| Шифр, параметры | Метод | Кол-во уравнений | Кол-во переменных | Кол-во мономов | Кол-во решений |
|---|---|---|---|---|---|
| Simon, $T = 3$, m =1 | Линеаризация | 48 | 32 | 48 | 4, только одно явл-ся ключом |
| | XL-метод | 1584 | 32 | 992 | 1 |
| Simon, $T = 4$, m =1 | Линеаризация | 64 | 48 | 80 | 65536 |
| | XL-метод | 3136 | 48 | 2616 | 256, только одно явл-ся ключом |
| Simon, $T = 5$, m =1 | Линеаризация | 80 | 64 | 112 | $2^{32}$ |
| | XL-метод | 5200 | 64 | 5008 | $2_{336}$ |
| Speck, $T = 3$, m =1 | Линеаризация | 500 | 176 | 1236 | — |
| | XL-метод | 88500 | 176 | 185216 | — |

Таблица 2

**Результаты применения метода ElimLin**

| Шифр, параметры | (Кол-во уравнений, кол-во лин. уравнений) | (Кол-во уравнений, кол-во лин. уравнений) после ElimLin |
|---|---|---|
| Simon, $T = 3$, m =1 | (48, 32) | (48, 32) |
| Simon, $T = 5$, m =1 | (80, 32) | (80, 48) |
| Speck, $T = 3$, m =1 | (500, 132) | (307, 137) |
| Speck, $T = 5$, m = 2 | (1032, 296) | (654, 297) |

## 2. SAT-решатели

Задача булевой выполнимости (SAT) — это задача принятия решения, в которой для произвольной булевой формулы возникает вопрос, существует ли такое значение переменных, что формула имеет значение true. Эта задача является NP-трудной.

Криптоанализ на основе SAT предполагает два этапа: на первом этапе обеспечивается кодирование SAT, например перевод данной системы из алгебраической нормальной формы (АНФ) в конъюнктивную нормальную форму. Мы используем конвертер anf2cnf [8] из библиотеки PolyBoRi, интегрированной в Sage. На втором этапе

полученный экземпляр SAT-задачи решается с помощью SAT-решателя. Для криптографических систем часто применяются SAT-решатели CryptoMiniSat [9] и Lingering (с его параллельными версиями Plingeling и Treengeling) [10]. Мы применяем SAT-решатели CryptoMiniSat (в Sage ver. 6.10) и Lingeling, Plingeling, Treengeling на ПК со следующими параметрами: Core i5-4690 CPU 3,5 ГГц (x4), 12 Гбайт оперативной памяти. Экспериментальные результаты для шифров Simon и Speck представлены в табл. 3 и 4. Рассмотрены два генератора систем уравнений в форме АНФ для шифра Simon: в одном все раундовые ключи являются независимыми переменными, в другом все они представлены алгоритмом ключевого расписания.

Таблица 3

**Результаты SAT-решателя для шифра Simon**

| Параметры | Кол-во ур-ий | Кол-во неизв. | Параметры SAT | SAT | Время, с | RAM, Мбайт |
|---|---|---|---|---|---|---|
| $T = 8$, $m = 2$ (с раунд. ключом) | 224 | 224 | 384 лит., 2528 клоз | CryptoMiniSat<br>Plingeling<br>Treengeling<br>Lingeling | 69811,9<br>4775,5<br>12702,81 | 120,5<br>260,3 182 |
| $T = 8$, $m = 2$ (ключ. расписание) | 128 | 128 | 368 лит., 4448 клоз | CryptoMiniSat<br>Plingeling<br>Treengeling<br>Lingeling | —<br>845,4<br>1188,8<br>4426,12 | —<br>26,6<br>169,2<br>95 |
| $T = 9$, $m = 2$ (ключ. расписание) | 144 | 144 | 480 лит., 6448 клоз | CryptoMiniSat<br>Plingeling<br>Treengeling<br>Lingeling | >260174,3<br>47799,2<br>24547,91 | —<br>>180,7 620,3<br>172 |
| $T = 10$, $m = 2$ (ключ. расписание) | 160 | 160 | 560 лит., 8096 клоз | CryptoMiniSat<br>Plingeling<br>Treengeling<br>Lingeling | —<br><br>17554,9<br>60776,91 | —<br>—<br>458,8 234 |

Таблица 4

**Результаты SAT-решателя для шифра Speck**

| Параметры | Кол-во ур-ий | Кол-во неизв. | Параметры SAT | SAT | Время, с | RAM, Мбайт |
|---|---|---|---|---|---|---|
| $T = 3$, $m = 1$ | 500 | 176 | 1460 лит., 11020 клоз | CryptoMiniSat<br>Plingeling<br>Treengeling<br>Lingeling | 0,56 0,9 0,97<br>0,2 | <br><br><br>9,6 4 1,9 |
| $T = 4$, $m = 2$ | 782 | 320 | 2492 лит., 17380 клоз | CryptoMiniSat<br>Plingeling<br>Treengeling<br>Lingeling | 21,4 3,0 8,25<br>61,4 | <br><br>17,3 15<br>14,8 |
| $T = 5$, $m = 2$ | 1032 | 416 | 3312 лит., 23184 клоз | CryptoMiniSat<br>Plingeling<br>Treengeling<br>Lingeling | 14448,17 | —<br>278 |
| $T = 6$, $m = 2$ | 1282 | 512 | 4132 лит., 28988 клоз | CryptoMiniSat<br>Plingeling<br>Treengeling<br>Lingeling | —<br><br>123353,82 | —<br>— 546 |

Прочерки в таблицах означают, что SAT-решателю не удалось найти решение системы; для шифра Speck CryptoMiniSat при $T = 3, 4$ не выдал размер файла.

### 3. Метод Раддума — Семаева

Данный подход к решению разреженных полиномиальных систем уравнений над полем $F_2$ был представлен Г. Раддумом и И. Семаевым в работе [11]. Анализ и некоторые свойства можно найти в [12].

По исходной системе уравнений строится граф. Вершины соответствуют каждому уравнению (верхний набор вершин), также присутствуют вершины, образуемые пересечением наборов переменных соответствующих уравнений (нижний набор вершин). Каждой вершине приписан список возможных означиваний соответствующих переменных. Обработка и поиск решения осуществляется с помощью так называемой процедуры Agreeing-Gluing (согласования-склейки). Процедура согласования берет две соседние вершины и обновляет их списки, удаляя векторы, которые имеют разные подвекторы для общих переменных. Процедура склеивания заменяет две вершины новой вершиной с обновлённым списком означиваний.

В качестве результатов использования этого алгоритма для атаки на Simon и Speck мы приводим только максимальное количество раундов, для которых алгоритм завершился за допустимое время. Стоит отметить, что временная сложность сильно зависит от эвристики, используемой для запуска процесса согласования, будь то (частичное) разделение или склейка.

Для шифра Simon максимальное число переменных в уравнении зависит от количества раундов и ключей. Для шести переменных количество уравнений равно $n(T - 2) + n(T - m)$.

Благодаря введению новых переменных в каждый раунд шифра Speck количество переменных на каждом раунде не зависит от количества раундов $T$ и ключей $m$. Максимальное количество переменных в одном уравнении равно 6; количество уравнений и переменных представлено в табл. 5 для $m = 1$ и табл. 6 для $m = 2, 3, 4$.

Таблица 5

**Количество переменных каждого уравнения шифра Speck,** $m = 1$

| Кол-во переменных | Кол-во уравнений |
|---|---|
| 6 | $2(T - 1)(2n - 4)$ |
| 5 | $2(T - 1)n$ |
| 4 | $6(T - 1)n + (T - 2)n$ |
| 3 | $2(n + 1)(T - 1)$ |
| 2 | $3n$ |

Таблица 6

**Количество переменных каждого уравнения шифра Speck,** $m = 2, 3, 4$

| Кол-во переменных | Кол-во уравнений |
|---|---|
| 6 | $2(T - 1)(2n - 4)$ |
| 5 | $2(T - 1)n$ |
| 4 | $6(T - 1)n + (T - 2)n$ |
| 3 | $2(n + 1)(T - 1)$ |
| 2 | $(T - 1)n + 3n$ |

Алгоритм Agreeing-Gluing был запущен для Simon до 9 раундов, для Speck — до 6 (табл. 7).

Таблица 7

**Параметры алгоритма Раддума — Семаева для шифров Simon и Speck**

| Параметры | Количество уравнений | Количество неизвестных | Верхний набор | Нижний набор |
|---|---|---|---|---|
| Шифр **Simon** | | | | |
| $T = 7$, m = 2 | 112 | 112 | 112 | 800 |
| $T = 8$, m = 2 | 128 | 128 | 128 | 1072 |
| $T = 9$, m = 2 | 144 | 144 | 144 | 1600 |
| Шифр **Speck** | | | | |
| $T = 3$, m = 1 | 500 | 176 | 500 | 558 |
| $T = 4$, m = 2 | 782 | 320 | 782 | 749 |
| $T = 5$, m = 2 | 1032 | 416 | 1032 | 1005 |
| $T = 6$, m = 2 | 1282 | 512 | 1282 | 1229 |

## 4. Анализ полученных результатов и заключение

В работе предпринята попытка оценить устойчивость шифра Speck к алгебраическому криптоанализу с помощью различных методов. Экспериментальные результаты показывают, что методы алгебраического анализа являются перспективным способом анализа надёжности современных шифров (в частности, низкоресурсных). Применительно к шифрам Simon и Speck показано, что методы, основанные на линеаризации, неэффективны уже при малом количестве раундов. С использованием SAT-решателя для шифра Simon решение найдено до 10 раундов включительно, для шифра Speck — до 6 раундов. Применение алгоритма Раддума — Семаева даёт результат для шифра Simon до 9 раундов, Speck — до 6. Результаты алгебраического анализа показывают, что включение дополнительных нелинейных операций (например, операции сложения по модулю $2^n$) значительно увеличивает время атаки и объём используемой памяти. Поэтому рассмотренные методы более эффективны для криптоанализа шифра Simon, чем для Speck. В то же время разреженность систем уравнений, описывающих шифры Simon и Speck, достаточно высока, что приводит к мысли о целесообразности использования метода Раддума — Семаева, разработанного специально для таких систем.

В дальнейшем планируется провести теоретическую оценку сложности алгебраического анализа для полнораундовых шифров Simon и Speck, а также оценить эффективность использования алгоритма Бухбергера.

ЛИТЕРАТУРА

1. Raddum H. Algebraic analysis of the Simon block cipher family // LNCS. 2015. V. 9230. P. 157-169.
2. Courtois N., Mourouzis T., Song G., et al. Combined algebraic and truncated differential cryptanalysis on reduced-round Simon // 11th Intern. Conf. Security Cryptogr. 2014. P. 399-404
3. Beaulieu R., Shors D., Smith J., et al. The Simon and Speck Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013.
4. Courtois N., Shamir A., Patarin J., and Klimov A. Efficient algorithms for solving overdefined systems of multivariate polynomial equations // LNCS. 2000. V. 1807. P. 293-407.
5. Courtois N. The Security of Cryptographic Primitives based on Multivariate Algebraic Problems. Ph.D. Thesis, Paris, 2001.
6. Bard G. Algebraic Cryptanalysis. Springer, 2009. 356 p.
7. Courtois N. and Bard G. V. Algebraic cryptanalysis of the data encryption standard // LNCS. 2007. V.4887. P.152-169.
8. Albrecht M., Brickenstein M., and Soos M. An ANF to CNF Converter using a Dense/Sparse Strategy. https://doc.sagemath.org/html/en/reference/sat/sage/sat/converters/polybori.html.
9. Soos M. The CryptoMiniSat 5 set of solvers at SAT competition 2016 // Proc. SAT Competition. Helsinki, 2016. P. 28.
10. Biere A. CaDiCaL, Lingeling, Plingeling, Treengeling, YalSAT entering the SAT Competition 2017 //

Proc. SAT Competition. Helsinki, 2017. P. 14-15.
11. Raddum H. and Semaev I. New Technique for Solving Sparse Equation Systems. IACR Cryptology ePrint Archive, 2006/475, 2006.
12. Biere A. New technique for solving sparse equation systems // Des. Codes Cryptogr. 2008. V. 49. No. 1-3. P. 47-60.

УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/14/20

# К ЗАДАЧЕ ОПИСАНИЯ МИНИМАЛЬНЫХ ПО ВКЛЮЧЕНИЮ СОВЕРШЕННЫХ ШИФРОВ

2. В. Медведева, С. С. Титов

Исследуются совершенные по Шеннону (абсолютно стойкие к атаке по шифр- тексту) шифры. На множестве ключей шифра определён граф эквивалентности ключей. Для шифра доказано достаточное условие его минимальности по включению. Построены примеры.

**Ключевые слова:** совершенные шифры, эндоморфные шифры, неэндоморфные шифры.

Рассматривается вероятностная модель $Е_в$ шифра [1]. Пусть $X$, $Y$ — конечные множества соответственно шифрвеличин и шифробозначений, с которыми оперирует некоторый шифр замены, $K$ — множество ключей, причём $|X| = Л$, $|Y| = ц$, $|К| = п$, где $Л > 1$, $ц > Л$. Открытые и шифрованные тексты представляются словами ($'$-граммами, $' > 1$) в алфавитах $X$ и $Y$ соответственно. Согласно [2, 3], под *шифром* $E_в$ будем понимать совокупность множеств правил зашифрования и правил расшифрования с заданными распределениями вероятностей на множествах открытых текстов и ключей. Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются *совершенными*.

Получение строгих доказуемых оценок стойкости для каждого конкретного шифра — это очень сложная, актуальная и до конца не решённая проблема криптоанализа. Различают теоретическую и практическую стойкость шифров (оцениваемую через ресурсы, требуемые на взлом), которую естественно описывать как вероятность успеха в противодействии атакам различного вида. Здесь впечатляющим результатом представляется теорема Шеннона [1] о совершенных (абсолютно стойких к атакам по шифртексту) шифрах, которую можно (нестрого) сформулировать так: атака по шифртексту на совершенный шифр бессмысленна, так как пассивный злоумышленник, перехватив зашифрованный текст, не получает никакой информации (кроме длины сообщения) об исходном открытом тексте. Но совершенный шифр не стоек к атакам активного злоумышленника (который может подменить или модифицировать сообщение).

Перспективным является изучение шифров, близких к совершенным, в том числе «приближённо совершенных» [4, 5]. Для таких шифров теорему Шеннона можно переформулировать — в виде теоремы А. Ю. Зубова — следующим образом: атака по шифртексту на почти совершенный шифр почти бессмысленна. При этом такие шифры приобретают дополнительные полезные свойства. Современные аналоги совершенных шифров пытаются бороться с атаками имитации и подмены, отказываясь от эндоморфности ($Л = ц$), внося информационную избыточность за счёт имитовставок и других приёмов, в том числе повышающих помехоустойчивость. Однако эта проблематика в данный момент не считается центральной — например, потому, что имеется много других более актуальных назревших нерешённых задач. Тем более что она признаётся достаточно сложной, но остающейся в поле зрения исследователей в связи с другими смежными комбинаторными задачами. Кроме этого, данные

исследования могут быть применены для обобщений на почти совершенные шифры.

Описание эндоморфных с минимально возможным числом ключей ($|K| = |Y|$) совершенных шифров даётся теоремой Шеннона, таблица зашифрования таких шифров — это латинский квадрат из равновероятных подстановок зашифрования [1]. Для неэндоморфных ($Л < ц$) минимальных совершенных шифров характерно большое многообразие таблиц зашифрования: они не сводятся только к латинским прямоугольникам размера $ц \times Л$ [6]. Для $Л = 2$, например, таблицы зашифрования могут быть составлены и из неравновероятных инъекций. Однако если все ключи равновероятны, то данный совершенный шифр является выпуклой оболочкой латинских прямоугольников, содержащихся в его таблице зашифрования, согласно аналогу теоремы Биркгофа [7]. Если $Л > 2$, то даже для равновероятных инъекций зашифрования неэндоморфный совершенный шифр может не содержать в своей таблице зашифрования латинских прямоугольников $ц \times Л$ [8].

Описание минимальных по включению (т. е. шифров, содержащих минимально возможное множество ключей зашифрования с ненулевыми вероятностями) неэндоморфных совершенных шифров, не сводящихся к латинским прямоугольникам размера $ц \times Л$, может быть осуществлено с помощью конструкций таблиц зашифрования, не содержащих латинских прямоугольников. Первый этап реализации данного подхода — это построение таких конструкций для шифробозначений, априорные вероятности которых считаются равными.

В работе [9] на основе отношения эквивалентности на множестве ключей получены достаточные условия того, что в таблице зашифрования неэндоморфных (эндоморфных) совершенных шифров отсутствуют латинские прямоугольники (квадраты). В частности, получены достаточные условия того, что таблицы зашифрования эндоморфных совершенных шифров не содержат латинских квадратов.

**Определение 1** [9]. Ключи $k^{0}$ и $k^{00}$ эквивалентны по шифрвеличине $x_i$, если $x_i$ на ключах $k^{0}$ и $k^{00}$ зашифровывается в одно и то же шифробозначение, т. е.

$$k^{0} = k^{00} \circ e_{k_0}(x_i) = e_{k_{00}}(x_i),$$

при этом в обозначении эквивалентности ключей используется биекция: $i \circ x_i$.

**Определение 2** [9]. Попарно различные ключи $k_1, k_2, k_3, \ldots, k_{n-1}, k_n$ образуют цикл длины $n$, если выполняются условия

$$k_i = k_2 = \kappa_3 = \ldots = k_{n-i} = k_n = k_i,$$

где $i_2 6= i_3$, $i_3 6= i_4$, . . . , $i_{n-1} 6= i_n$, $i_n 6= i_1$.

Следующим за минимальными по Шеннону шифрами по количеству ключей идёт класс минимальных по включению шифров, в которых для каждой пары $(x, y)$ шифр- величины $x$ и шифробозначения $y$ имеется не более двух ключей $k$, на которых $x$ зашифровывается в $y$. В каждом столбце таблицы зашифрования каждое шифробо- значение $y$ встречается, следовательно, не более двух раз.

При $u = 4$ такие таблицы построены для семи и восьми ключей [8]. При $u = 5$ такие таблицы тоже могут быть построены.

**Пример 1.** Рассмотрим эндоморфный шифр с множеством из пяти шифр- величин. Пусть $X = \{x_1, x_2, x_3, x_4, x_5\} = \{1, 2, 3, 4, 5\}$ – множество шифрвели- чин; $Y = \{y_1, y_2, y_3, y_4, y_5\} = \{1, 2, 3, 4, 5\}$ – множество шифробозначений; $K = = \{k_1, k_2, \ldots, k_n\}$ – множество ключей.

Таблицы зашифрования (табл. 1 и 2) совершенного эндоморфного шифра с $Л = u = 5$ и вероятностями ключей $P_1 = 0,2$ и $P_2 = \ldots = P_9 = 0,1$ не содержат латинских квадратов.

Таблица 1

| №п/п | K | X1 | X2 | X3 | X4 | X5 | Pk |
|---|---|---|---|---|---|---|---|
| 1 | k1 | 1 | 2 | 3 | 4 | 5 | 0,2 |
| 2 | k2 | 2 | 3 | 4 | 5 | 1 | 0,1 |
| 3 | k3 | 2 | 5 | 1 | 3 | 4 | 0,1 |
| 4 | k4 | 3 | 4 | 5 | 1 | 2 | 0,1 |
| 5 | k5 | 3 | 1 | 2 | 5 | 4 | 0,1 |
| 6 | k6 | 4 | 5 | 2 | 3 | 1 | 0,1 |
| 7 | k7 | 4 | 3 | 5 | 1 | 2 | 0,1 |
| 8 | k8 | 5 | 1 | 4 | 2 | 3 | 0,1 |
| 9 | k9 | 5 | 4 | 1 | 2 | 3 | 0,1 |

Таблица 2

| № п/п | K | xi | X2 | x3 | X4 | X5 | Pk |
|---|---|---|---|---|---|---|---|
| 1 | ki | 1 | 2 | 3 | 4 | 5 | 0,2 |
| 2 | k2 | 2 | 3 | 4 | 5 | 1 | 0,1 |
| 3 | *кэ* | 2 | 5 | 1 | 3 | 4 | 0,1 |
| 4 | *к4* | 3 | 4 | 5 | 1 | 2 | 0,1 |
| 5 | *к5* | 3 | 1 | 2 | 5 | 4 | 0,1 |
| 6 | *кб* | 4 | 5 | 1 | 3 | 2 | 0,1 |
| 7 | *к7* | 4 | 3 | 5 | 2 | 1 | 0,1 |
| 8 | *к8* | 5 | 1 | 4 | 2 | 3 | 0,1 |
| 9 | *к9* | 5 | 4 | 2 | 1 | 3 | 0,1 |

Для шифров, в которых для каждой пары $(x, y)$ шифрвеличины $x$ и шифробозначения $y$ имеется не более двух ключей $k$, на которых $x$ зашифровывается в $y$, естественно определить граф на множестве ключей, а именно: два различных ключа (соответствующих разным инъекциям зашифрования) соединим ребром, если существует такая пара $(x, y)$, что на обоих этих ключах шифрвеличина $x$ зашифровывается в $y$.

**Пример 2.** Рассмотрим графы, соответствующие шифрам с табл. 1 и 2. Ясно, что ключи $k$ с вероятностью $P_k = 0,2$ представляют собой изолированные вершины.

Шифру с табл. 1 соответствует граф эквивалентности ключей, изображённый на рис. 1. Из рис. 1 и табл. 1 видно, что ключи $k_2, k_3, k_5$ образуют цикл длины три:

$$k_2 = к_э = k_5 = k_2;$$

а ключи $k_3, k_4, k_6, k_7, k_9$ образуют цикл длины пять:

$$к_9 = к_э = к_6 = к_7 = к_4 = к_9.$$

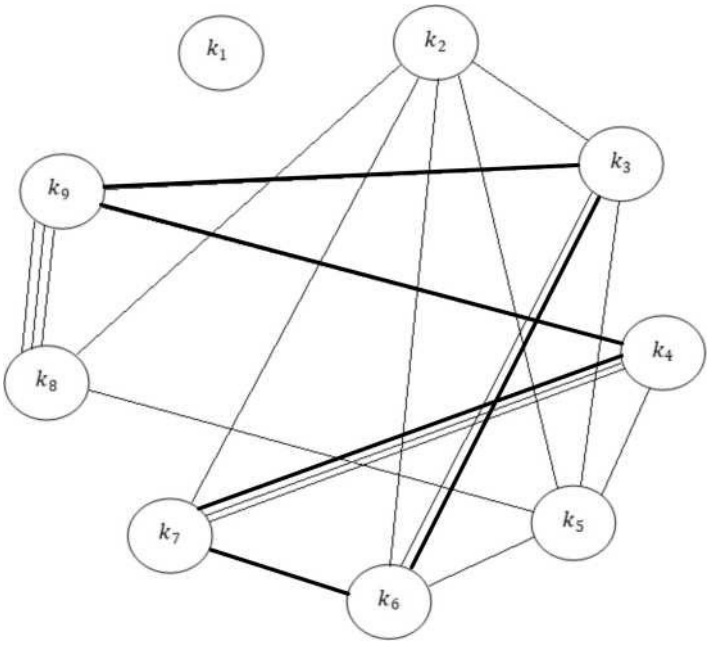



Рис. 1. Граф 1

Шифру с табл. 2 соответствует граф эквивалентности ключей, изображённый на рис. 2. Из рис. 2 и табл. 2 видно, что ключи $k_2, k_3, k_5$ образуют цикл длины три:

$$k_2 \to k_3 \to k_5 \to k_2;$$

а ключи $k_2, k_4, k_5, k_8, k_9$ образуют цикл длины пять:

$$k_2 \to k_5 \to k_4 \to k_9 \to k_8 \to k_2.$$

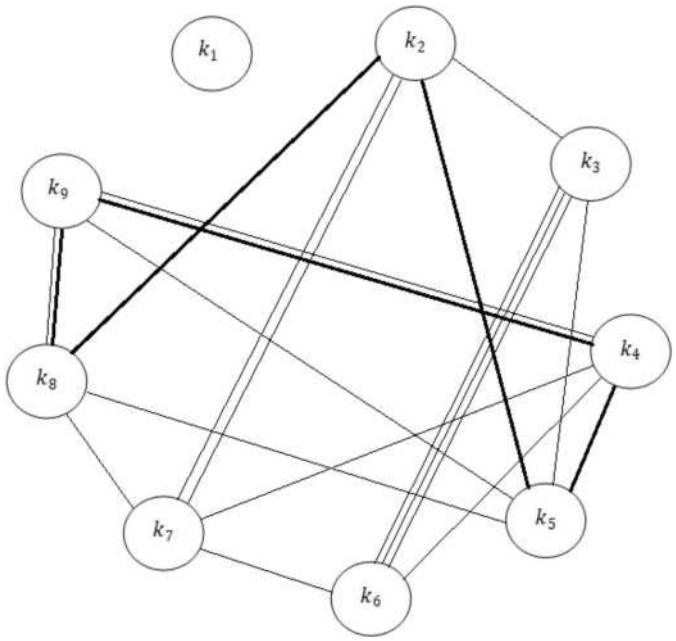



Рис. 2. Граф 2

**Утверждение 1.** Пусть в некоторой неодноэлементной связной компоненте графа

эквивалентности ключей шифра существует цикл нечётной длины. Тогда данный шифр минимален по включению.

Таким образом, в работе предложен графовый подход к исследованию и описанию совершенных шифров, их аналогов и обобщений. В рамках предлагаемого подхода доказано утверждение (достаточное условие минимальности шифра по включению), которое может служить основой для дальнейших обобщений; приведены примеры, иллюстрирующие эффективность подхода. Полученные результаты могут быть применены и для изучения почти совершенных шифров.

ЛИТЕРАТУРА

1. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333-402.
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М.: Гелиос АРВ, 2001.
3. Зубов А. Ю. Совершенные шифры. М.: Гелиос АРВ, 2003.
4. Зубов А. Ю. Почти совершенные шифры и коды аутентификации // Прикладная дискретная математика. 2011. № 4(14). С. 28-33.
5. *Зубов А. Ю.* О понятии ^-совершенного шифра // Прикладная дискретная математика. 2016. № 3(33). С. 45-52.
6. *Медведева Н. В., Титов С. С.* Аналоги теоремы Шеннона для эндоморфных неминимальных шифров // Прикладная дискретная математика. Приложение. 2016. № 9. С. 62-65.
7. *Медведева Н. В., Титов С. С.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. №4 (30). С. 43-55.
8. *Медведева Н. В., Титов С. С.* Геометрическая модель совершенных шифров с тремя шифрвеличинами // Прикладная дискретная математика. Приложение. 2019. № 12. С. 113-116.
9. *Медведева Н. В., Титов С. С.* Конструкции неэндоморфных совершенных шифров // Прикладная дискретная математика. Приложение. 2020. № 13. С. 51-54.

УДК 512.55+003.26 DOI 10.17223/2226308X/14/21

## ПОСТКВАНТОВОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ НА ОСНОВЕ РЕШЁТОК ПРИ УЧАСТИИ НЕСКОЛЬКИХ КАНДИДАТОВ

Д. А. Набоков

В последние годы появляется множество эффективных криптографических схем на основе решёток, среди которых стоит отметить (полностью) гомоморфное шифрование и протокол конфиденциального вычисления. Такие схемы на решётках интересны тем, что являются стойкими к атакам квантового компьютера. В работе реализована схема электронного голосования, эффективно поддерживающая нескольких кандидатов, за которых можно голосовать. Возможны два варианта голосования: голос за единственного кандидата или голоса для любого подмножества кандидатов. В схеме присутствует множество администраций, конфиденциальность голосов сохраняется в случае, когда хотя бы одна администрация остаётся честной. Схема направлена на соблюдение конфиденциальности голосов и про- верямости результатов; для соблюдения других часто рассматриваемых свойств безопасности электронного голосования используются различные предположения, например, что у каждой администрации есть открытые ключи всех допущенных к голосованию лиц. В основе устройства схемы лежат доказательства с нулевым разглашением и схема обязательства с гомоморфными по сложению свойствами. Благодаря доказательствам с нулевым разглашением, проверить результаты голосования может любой участник схемы.

**Ключевые слова:** решётки, электронное голосование, схема обязательства, доказательство с нулевым разглашением, амортизированное доказательство открытия.

## Введение

В работе [1] представлена схема электронного голосования, безопасность которой основана на сложности задач на решётках: M-SIS и M-LWE [2]. Считается, что эти задачи являются сложными как для классического, так и для квантового компьютера, то есть получившаяся схема является постквантовой. Предложенная в [1] схема обеспечивает конфиденциальность голоса и проверяемость результатов, в качестве голоса выступает значение из $\{0, 1\}$, то есть голосование производится за одного кандидата. Авторы предлагают способ расширения схемы при участии в голосовании нескольких кандидатов, однако их способ неэффективен.

Настоящая работа посвящена эффективному расширению постквантовой схемы электронного голосования из [1] для нескольких кандидатов. В связи с этим модель безопасности схемы и доказательство безопасности аналогичны оригинальной. Основные отличия заключаются в следующем:

- В качестве голоса выступает вектор $\mathbf{v} \in \{0,1\}^{N_c}$ ($N_c$ — количество кандидатов), для которого можно потребовать, чтобы его вес был равен единице. Основной сложностью такого расширения схемы для нескольких кандидатов является возможность доказательства, что голос в отправляемом бюллетене правильно сформирован.
- Так как голос уже не элемент из $\{0, 1\}$, то для данной схемы разработано новое доказательство корректности голоса в публикуемом бюллетене, именуемое в дальнейшем VProof. Соответственно, доказательство OR-proof заменено на VProof.
- Используется более эффективное амортизированное доказательство открытия.

В основе схемы лежат такие криптографические конструкции, как доказательства с нулевым разглашением и схема обязательства (commitment scheme).

## 1. Криптографические конструкции

В эффективных криптографических схемах на решётках вычисления обычно проводятся в кольце $R_q = Z_q[X]/(X^d+1)$ для простого $q$ и целого $d$, являющегося степенью двойки.

Для различных $q, d$ многочлен $X^d + 1$ может разлагаться в кольце $Z_q$ на произведение многочленов меньшей степени. Пусть $l | d$ и $q - 1 = 2l \bmod 4$, тогда, согласно [3, Theorem 2.3],

$$X^d + 1 = \prod_{i \in Z_q^*} (X^{d/l} - Z_i),$$

где $X^{d/l} - Z_i$ является неприводимым над $Z_q$ многочленом, а $Z_i$ пробегает все $2l$ корней из единицы. В $Z_q$ не существует элементов, порядок которых больше $2l$.

Подобное разложение позволяет работать с многочленами аналогично Китайской Теореме об остатках. Определим такое отображение NTT, которое переводит многочлен $m \in R_q$ в набор многочленов $\mathrm{NTT}(m) = (m_0, \ldots, m_{l-1})$, где

$$m_i = m \bmod (X^{d/l} - Z^{2i+1}).$$

Многочлены $m_0, \ldots, m_{l-1}$ будем называть NTT-коэффициентами $m$. Вектор $\mathbf{v}$ можно разбить на блоки из $l$ коэффициентов и представить его в виде многочленов $m_1, \ldots, m_{dN_c/l} \in R_q$, таких, что NTT-коэффициенты $m_i$ являются $i$-м блоком вектора $\mathbf{v}$ (последний блок дополняется нулями). В таком представлении NTT-коэффициентами являются многочлены нулевой степени.

**Определение 1** [4]. Для открытой случайной матрицы $B_0 \in R_q^{n \times m}$ и открытых

случайных векторов $\mathbf{b}_1,\ldots,\mathbf{b}_n \in R_q^{k+n}$, а также секретного короткого вектора $\mathbf{r} \in \chi^{(k+\chi+n)}$ из распределения шума $\chi$ обязательством к сообщениям $m_1,\ldots,m_n \in R_q$ является

$$\mathbf{t}_0 = B_0\mathbf{r},\ t_1 = \langle \mathbf{b}_1, \mathbf{r}\rangle + m_1,$$

$$t_n = \langle \mathbf{b}_n, \mathbf{r}\rangle + m_n,$$

где размер открытых векторов и матрицы зависит от количества сообщений $n$ и параметров $k$ и $A$, от которых зависит сложность задач M-SIS и M-LWE соответственно (стоит отметить, что сложность зависит и от других параметров, например $d$ и $\chi$).

Чтобы открыть данное обязательство, достаточно опубликовать вектор $\mathbf{r}$, для которого выполняется равенство $\mathbf{t}_0 = B_0\mathbf{r}$. Сообщения $m_i$ находятся как $t_i - \langle \mathbf{b}_i, \mathbf{r}\rangle$. Задача нахождения $m_i$ из обязательства сводится к задаче M-LWE, задача получения другого открытия $\mathcal{E}^*$ —к M-SIS. Наиболее эффективные схемы получаются при таком выборе параметров, что обе задачи имеют примерно одинаковую стойкость.

Схема обладает важным гомоморфным свойством: при сложении обязательств получается обязательство к сообщению, равному сумме исходных сообщений, однако в этом случае используется вектор $\mathbf{r}$ с большими коэффициентами, из-за чего стойкость одной из задач ниже. То есть параметры в этом случае необходимо выбрать так, чтобы как исходное обязательство, так и их сумма были безопасными. Соответственно при суммировании большого числа обязательств схема может стать неэффективной.

Иногда возникает необходимость доказать, что опубликовавший обязательство действительно может предоставить короткий $\mathbf{r}$ (не опубликовывая его), которое открывает обязательство. Такое доказательство называется доказательством открытия (opening proof).

**Определение 2.** Амортизированным доказательством открытия для обязательств $(\mathbf{t}_0 \| \mathbf{t}_1 \| \ldots \| \mathbf{t}_n)_i$, $i = 1,\ldots,p$, является протокол между доказывающим и проверяющим, в результате которого проверяющий убеждается, что доказывающий знает $\mathbf{r}_i'$, такие, что $\mathbf{ct}_{0,i} = B_0\mathbf{r}^*$ для короткого обратимого многочлена $c$ и вектора $\mathbf{r}^*$ с несколько большими по сравнению с $\mathbf{r}_i$ коэффициентами.

В результате амортизированного доказательства открытия доказывается более слабое относительно желаемого утверждение. Выбирать параметры необходимо так, чтобы найти такие $\mathbf{r}_i'$ было трудно. Так как для всех обязательств используется один и тот же фиксированный многочлен $c$, эти обязательства можно гомоморфно складывать. В работе используется амортизированное доказательство открытия из [5, Section 3], которое является более эффективным по сравнению с используемым в [1].

Доказательство VProof, позволяющее доказать, что голос является правильно сформированным в предоставленном обязательстве, реализуется на основе доказательства произведения [6] и доказательства неструктурированной линейной связи (unstructured linear relation) [7].

Доказательство произведения для обязательства к сообщениям $m_1, m_2, m_3$ направлено на доказательство $m_1 \cdot m_2 = m_3$. Модифицируем его таким образом, чтобы доказывать $m_i(m_i - 1) = 0$ (эта модификация достаточно простая и не влияет на безопасность

доказательства, однако конкретные детали опустим). При умножении многочленов из $R_q$ их NTT-коэффициенты умножаются покоординатно. В итоге для каждого NTT-коэффициента $m$ выполняется

$$m(m - 1) = 0 \pmod{X^{d/l} - Z_j},$$

а так как $X^{d/l} - Z_j$ является неприводимым многочленом, то $m$ равняется либо 0, либо 1. В итоге для обязательства можно доказать, что NTT-коэффициенты его сообщений являются двоичной строкой. Так как вектор $\mathbf{v}$ дополняется нулями до кратности $l$, то для $m_n$ уравнение изменяется на $m_n(m_n - m^0) = 0$, где NTT-коэффициенты $m^0$ сначала единицы, а потом нули, причём количество нулей равно $l - (N_c \bmod l)$. То есть в итоге доказывается принадлежность NTT-коэффициентов $\{0,1\}^{N_c}$.

С помощью доказательства неструктурированной линейной связи для открытой матрицы $A \in Z_q^{n \times l}$ и открытого вектора $\mathbf{u} \in Z_q^n$ можно доказать $A\mathbf{v} = \mathbf{u}$. Нас интересует случай $a = 1$, $A = (1 \ldots 1)$, $\mathbf{u} = (1)$, то есть сумма коэффициентов вектора $\mathbf{v}$ должна быть равна единице.

Доказательство VProof можно воспринимать как одновременное применение этих двух доказательств. Стоит заметить, что доказательство неструктурированной линейной связи используется для классического понимания голосования, то есть выбор ровно одного кандидата из многих. Это доказательство можно опустить, тогда правильным голосом будет считаться голос за любое подмножество кандидатов. Или можно в качестве $A$ и $\mathbf{u}$ брать более сложные конструкции для обеспечения каких-то нетривиальных требований на голоса.

Доказательства произведения и неструктурированной линейной связи в оригинальных работах представлены как интерактивные протоколы, для которых доказаны свойства корректности и полноты, а также нулевого разглашения, если проверяющий является честным. Приведём (неформальную) теорему о свойствах интерактивного протокола для VProof.

**Теорема 1.** Интерактивный протокол для доказательства VProof обладает следующими свойствами:

- Полнота (Completeness): честный доказывающий убеждает честного проверяющего с вероятностью, близкой к единице.
- Корректность (Soundness): существует извлекатель знания (knowledge extractor), который, имея доступ к детерминированному доказывающему $P^*$, представленному в виде чёрного ящика с возможностью перемотки, либо выдаёт открытие обязательства к сообщению $m^*$, являющемуся корректным голосом, либо решение задачи M-SIS.
- Нулевое разглашение с честным проверяющим (honest verifier zero-knowldge): существует симулятор, который способен симулировать успешные взаимодействия между доказывающим и проверяющим. Способность различать реальное взаимодействие от симулированного сводится к решению задачи M-LWE.

Свойство нулевого разглашения применяется только в случае честного проверяющего, это ограничение можно нивелировать, преобразовав интерактивный протокол в неинтерактивный с помощью замены проверяющего на случайный оракул.

Строгая формулировка теоремы 1, а также её доказательство аналогичны работам [6, 7].

## 2. Набросок схемы электронного голосования

В данной работе разработана схема электронного голосования со множеством голосующих, администраций (authority) и кандидатов. В наброске мы опишем схему для $n = 1$. Схема легко расширяется для большего числа сообщений, но усложняется индексация.

Чтобы опубликовать бюллетень, голосующий $i$ делает следующее:

- Пусть $m_i G R_q$ – сообщение, являющееся правильным голосом.
- Голосующий разделяет голос между $N_a$ администрациями: $x^{(1)},\ldots, x^{N_a} \in R_q$:
$$\sum_{j=1}^{N_a} x_i^{(j)} = m_i .$$
- Голосующий создаёт $N_a$ обязательств к $x_j$ с секретными векторами $r_j$
- Используя VProof, он доказывает, что обязательство к $m_i$ для секретного вектора
$$\sum_{j=1}^{N_a} r_i^{(j)}$$
содержит в себе корректный голос.
- Голосующий зашифровывает $r_{ij)}$ с помощью открытого ключа $j$-й администрации и публикует его вместе со всеми обязательствами и доказательством.

Сумма всех случайных многочленов $x_i^{(0)}$ является финальным результатом голосования. Эта сумма находится по частям: каждая $j$-я администрация находит сумму $\sum_i x_i^{(0)}$ и публикует промежуточную сумму.

Порядок действий каждой администрации:

- Администрация расшифровывает все секретные векторы пользователей, предназначенных для неё.
- Амортизированно доказывает открытие обязательств для этих секретных векторов.
- Администрация находит сумму этих обязательств и сумму соответствующих секретных векторов и публикует эти суммы вместе с амортизированным доказательством открытия.

При сложении обязательств коэффициенты секретного вектора растут, что снижает безопасность схемы и может привести к неэффективному выбору параметров. Для решения этой проблемы вводится параметр $u$. Администрация может складывать не более $u$ обязательств. Так как администрация знает все сообщения, она может создать новое обязательство (со «свежим» секретным вектором) к сообщению, являющемуся суммой сообщений в этих $u$ обязательствах. Дальше необходимо доказать, что сообщение в свежем обязательстве корректно, для этого используется доказательство открытия к нулю для обязательства, равного разности свежего обязательства и сумме $u$ старых. Доказательство открытия к нулю показывает, помимо $ct_0 = B_0 r^*$, ещё $ct_1 = \langle b_1, r^* \rangle$, то есть в этом обязательстве нулевое сообщение.

В итоге $u$ старых обязательств заменяются на одно новое. Этот процесс можно продолжать сколько угодно, пока не останется $u$ или меньше обязательств.

Порядок действий для подведения результатов голосования и его проверки:

- Для вычисления результата голосования необходимо сложить промежуточные суммы всех администраций.

— Для проверки результата необходимо проверить доказательства всех участников, а также правильность сложения администраций.

Конфиденциальность голосующего сохраняется, если хотя бы одна администрация является честной. Проверяемость результатов достигается благодаря доказательствам с нулевым разглашением. Взлом схемы подразумевает собой решение задачи M-SIS или M-LWE.

## Заключение

Разработана постквантовая схема электронного голосования на основе решёток для любого количества кандидатов. В схеме участвует множество администраций, конфиденциальность каждого голоса сохраняется до тех пор, пока хотя бы одна администрация остаётся честной. Проверить финальный результат голосования может любой участник, так как для этого необходимо проверить опубликованные голосующими и администрациями доказательства. Безопасность предложенной схемы основывается на сложности решения задач M-SIS и M-LWE.

ЛИТЕРАТУРА

1. Del Pino R., Lyubashevsky V., Neven G., and Seiler G. Practical quantum-safe voting from lattices // Proc. ACM SIGSAC Conf. Comput. Commun. Security. 2017. P. 1565-1581.
2. *Langlois A.and Stehle D.* Worst-case to average-case reductions for module lattices // Des. Codes Cryptogr. 2015. V. 75. P. 565-599.
3. *Lyubashevsky V. and Seiler G.* Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs // LNCS. 2018. V. 10820. P. 204-224.
4. *Baum C., Damgard I., Lyubashevsky V., et al.* More efficient commitments from structured lattice assumptions // LNCS. 2018. V. 11035. P. 368-385.
5. *Baum C., Bootle J., Cerulli A., et al.* Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits // LNCS. 2018. V. 10992. P. 669-699.
6. *Attema T., Lyubashevsky V., and Seiler G.* Practical product proofs for lattice commitments // LNCS. 2020. V. 12171. P. 470-499.
7. *Esgin M., Nguyen N., and Seiler G.* Practical exact proofs from lattices: New techniques to exploit fully-splitting rings // Adv. Cryptology — ASIACRYPT 2020. P. 259-288.

УДК 519.7 DOI 10.17223/2226308X/14/22

# ОБ ARX-ПОДОБНЫХ ШИФРСИСТЕМАХ НА БАЗЕ РАЗЛИЧНЫХ КОДИРОВОК НЕАБЕЛЕВЫХ РЕГУЛЯРНЫХ 2-ГРУПП С ЦИКЛИЧЕСКОЙ ПОДГРУППОЙ ИНДЕКСА 2

Б. А. Погорелов, М. А. Пудовкина

В большинстве блочных шифрсистем операции наложения ключа описываются с помощью преобразований из аддитивной группы векторного пространства $(V_m, +)$ над полем GF(2), аддитивной группы $(Z_{2^m}, +)$ кольца вычетов $Z_{2^m}$, либо их комбинации. В шифрсистемах типа ARX одновременно используются преобразования трёх типов, где дополнительно введена операция циклического сдвига. В работе обсуждается возможность использования для этих целей неабелевых групп. Рассматриваются подстановочные свойства неабелевых 2-групп с циклической подгруппой индекса 2, т. е. близких к подстановочному представлению группы $(Z_{2^m}, +)$ и перспективных с точки зрения синтеза блочных шифрсистем. С целью сокращения числа различных групп, используемых в одной шифрсистеме, целесообразно вместе с группой применять различные её вариации (естественные кодировки элементов, правые и левые регулярные представления). Описываются свойства групп, порождённых такими вариациями, включая условия их импримитивности, а также совпадения с симметрической группой.

**Ключевые слова:** *ARX-шифрсистемы, примитивные группы, группа диэдра, группа обобщённых кватернионов, полудиэдральная группа, модулярная максимально-циклическая группа.*

В раундовых преобразованиях большинства блочных шифрсистем обычно используются преобразования из аддитивной группы $(V_m, +)$ $m$-мерного векторного пространства $V_m$ над полем GF(2), реже – из аддитивной группы $(Z_{2^m}, +)$ кольца вычетов $Z_{2^m}$. В ряде шифрсистем используются комбинации таких групп (IDEA, SAFER), действующих параллельно или последовательно. Ещё один класс составляют ARX-шифрсистемы (Addition-Rotation-Xor). Они реализуются с помощью большого числа простых преобразований соответственно из подстановочных представлений групп $(Z_{2^m}, +)$, $(V_m, +)$ и циклического сдвига координат. Известными представителями ARX-шифрсистем являются TEA, XTEA [1], RC5 [2], RC6 [3], SIMON, SPECK [4].

Естественным развитием этого подхода представляется рассмотрение неабелевых групп, «ближайших» к указанным, а также различных подстановочных представлений таких групп, в том числе связанных с различными кодировками элементов группы. Ранее в работах авторов описаны подстановочные свойства групп с циклической подгруппой индекса 2 [5], классы преобразований на указанных группах [6, 7], а также рассмотрены вопросы марковости [8].

Из теоремы 12.5.1 [9] следует, что неабелевыми группами порядка $2^m$ с циклической подгруппой индекса 2 являются только четыре группы, удовлетворяющие следующим порождающим соотношениям:

– группа диэдра $D_{2^m}$, $m > 3$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{-1}u;$$

– обобщённая группа кватернионов $Q_{2^m}$, $m > 3$,

$$a^{2^{m-1}} = e,\ u^2 = a^{2^{m-2}},\ ua = a^{-1}u;$$

– модулярная максимально-циклическая группа $M_{2^m}$, $m > 4$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{1+2^{m-2}}u;$$

– полудиэдральная группа $SD_{2^m}$, $m > 4$,

$$a^{2^{m-1}} = e,\ u^2 = e,\ ua = a^{-1+2^{m-2}}u.$$

Обозначим через $H_m$ одну из четырёх групп: $H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\}$. Элементы группы $H_m$ будем записывать как $u^{\varepsilon_1} a^{\varepsilon_2}$, где $\varepsilon_1 \in \{0,1\}$; $\varepsilon_2 \in \{0,\ldots, 2^{m-1} - 1\}$. Пусть $\wedge_{rr} : H_m \to S(H_m)$, $\wedge_{lr} : H_m \to S(H_m)$ – соответственно правое и левое регулярные подстановочные представления, заданные для всех $i \in \{0, \ldots, 2^{m-1} - 1\}$, $x \in H_m$ условиями

$$\wedge_{rr}(a_i) : x \to xa_i, \qquad \wedge_{rr}(ua_i) : x \to xua_i,$$
$$\wedge_{lr}(a_i) : x \to a_i x, \quad \wedge_{lr}(ua_i) : x \to (ua_i)^{-1} x.$$

Пусть $Z_{2^m}^+$, $V_m^+$ — правые подстановочные представления аддитивных групп кольца $Z_{2^m}$ и $m$-мерного векторного пространства $V_m$ над полем GF(2).

Напомним (см., например, [10]), что транзитивная группа подстановок $G \leq S(X)$ называется импримитивной, если существует сохраняемое $G$ нетривиальное разбиение $\mathbf{W}$ множества $X$ на равномощные блоки, т. е.

$$g(W) = \{g(a) \mid a \in W\} \in \mathbf{W} \text{ для всех } g \in G,\ W \in \mathbf{W}.$$

Группа $G_m = (V^+, Z_{2^m}^+)$ импримитивна с $r$-й системой импримитивности $\mathbf{W}^{(r,m)} = \{W_0^{(r,m)}, \ldots, W_{2^r-1}^{(r,m)}\}$, где

$$W_t^{(r,m)} = \{j \in \{0,\ldots,2^m-1\} : j \equiv t \pmod{2^r}\},\ t = 0,\ldots,2^r-1,\ r = 0,\ldots,m.$$

Группа $G_m$ возникает в связи с разными криптографическими приложениями. Её строение описано, например, в [11, 12]. Максимальной подгруппой в $S_{2^m}$, сохраняющей каждое разбиение $\mathbf{W}^{(0,m)}, \mathbf{W}^{(1,m)}, \ldots, \mathbf{W}^{(m,m)}$, является силовская 2-подгруппа $P_m \in Syl_2(S_{2^m})$, описываемая операцией сплетения $P_m = P_2 \circ P_{m-1}$ и содержащая $G_m$.

Возможны различные способы задания отображения $\nu : H_m \to \{0,\ldots,2^m-1\}$, кодирующего элементы группы $H_m$ целыми числами из множества $\{0,\ldots,2^m-1\}$, которые удобны для использования в криптографических приложениях.

Для $c \in \{r_r, l_r\}$ отображению $\nu$ сопоставим естественное изоморфное вложение $\nu : \lambda_c(H_m) \to S_{2^m}$, такое, что элементу $b \in \lambda_c(H_m)$ ставится в соответствие подстановка $\nu(b) \in S(\{0,\ldots,2^m-1\})$, заданная условием

$$\nu(b) : \nu(a) \to \nu(b(a)) \text{ для всех } a \in H_m.$$

Тем самым каждому элементу $a \in H_m$ и его образу $b(a) \in H_m$ сопоставляются соответственно элементы $\nu(a), \nu(b(a)) \in \{0,\ldots,2^m-1\}$, которые однозначно задают подстановку $\nu(b)$ на $\{0,\ldots,2^m-1\}$. Далее отображение $\nu$ будем называть *кодировкой*.

Напомним [10], что у импримитивной группы существуют нетривиальные естественные (подстановочные) гомоморфизмы. Кроме того, импримитивность группы, порождённой криптографическими преобразованиями, в частности раундовыми функциями, может привести к уязвимости шифрсистемы относительно метода гомоморфизмов [13, 14]). В связи с этим описание кодировок $\nu$, для которых группы, порождённые комбинациями групп $\nu(\rho_{r_r}(H_m))$, $\nu(\rho_{l_r}(H_m))$ и $Z_{2^m}^+$, являются примитивными, представляет интерес с точки зрения криптографических приложений, включая синтез ARX-шифрсистем и их вариаций.

Пусть $c \in \{l_r, r_r\}$. В данной работе приведены необходимые и достаточные условия на отображение $\nu$, при которых справедливо включение $\iota(\lambda_c(H_m)) \leq P_m$ или равенство $(Z_{2^m}, \nu(\lambda_c(H_m))) = S_{2^m}$. Для преобразования обращения $s \in H_m$, $s : a \to a^{-1}$, и регулярного представления $\nu(\lambda_c(H_m))$ получены необходимые и достаточные условия справедливости включения $h\nu(s), \nu(\lambda_c(H_m))\iota \leq P_m$.

**Теорема 1.** Пусть $m > 4$, $H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\}$, биективные отображения $\nu_d^{(m)} : H_m \to \{0, 1, \ldots, 2^m-1\}$, $d \in \{1, 2, 3\}$, заданы условиями:

$$\nu_1^{(m)} : x \to \begin{cases} 2i, & \text{если } x = a^i, \\ 2i+1, & \text{если } x = ua^i, \end{cases}$$

$$\nu_2^{(m)}: x \wedge \begin{cases} i, & \text{если } x = a^i, \\ i + 2^{m-1}, & \text{если } x = ua^i, \end{cases}$$

$$\nu^{(m)}: x \wedge \begin{cases} i, & \text{если } x = a^i, \\ -i - 1, & \text{если } x = ua^i, \end{cases}$$

где $x \in H_m$, $i \in \{0,1,\ldots,2^{m-1} - 1\}$. Тогда имеют место следующие свойства:

1) для $\wedge_{rr}(H_m)$

$$\nu(\wedge_{rr}(H_m)) \in P_m,$$

$$\nu(s)(\wedge_{rr}(H_m)) \in P_m \text{ для } H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\}, \nu(\wedge_{rr}(H_m)) \in P_m \text{ для } H_m \in \{D_{2^m}, M_{2^m}\}.$$

Кроме того,

а) $\nu(z_+, \nu_{2^m}(H_m)) = S_{2^m}$ для каждой $H_m \in \{Q_{2^m}, SD_{2^m}\}$;

б) $Z_{+m}$, $(\wedge_{rr}(H_m)) \wedge = S_{2^m}$, $Z_{+m}$, $\nu(\wedge_{rr}(H_m)) \wedge = S_{2^m}$ для каждой $H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\}$.

2) Для $\wedge_{lr}(H_m)$

$$\nu(\wedge_{lr}(H_m)) \in P_m,$$

$$\nu(s)(\wedge_{lr}(H_m)) \in P_m \text{ для } H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\},$$

$$\nu(\wedge_{lr}(H_m)) \in P_m \text{ для } H_m = M_{2^m},$$

$$\wedge_m(\wedge_{lr}(H_m)) \in P_m \text{ для } H_m \in \{D_{2^m}, SD_{2^m}\}.$$

Кроме того, а)

$$D_{Z_{+m}} \wedge_m \text{ б) } (\wedge_{lr}(H_m)) = S_{2^m} \text{ для каждой } H_m \in \{D_{2^m}, Q_{2^m}, SD_{2^m}\};$$

$$DZ_{+,}\nu^{(m)} \quad (p_{lr}(H_m)) = S_{2^m} \text{ для каждой } H_m \in \{M_{2^m}, Q_{2^m}\}.$$

Заметим, что группа $Z_{2^m}$ порождена полным циклом $(0, \ldots, 2^m - 1)$. При доказательстве теоремы 1 использовано свойство, что примитивная группа, содержащая полный $2^m$-цикл, изоморфна симметрической группе $S_{2^m}$ или естественному подстановочному представлению степени $2^m$ проективной группы $PGL(2, p)$, $p = 2^m - 1$ – простое число [15].

ЛИТЕРАТУРА


1. Wheeler D. J. and Needham R. M. TEA, a Tiny Encryption Algorithm // LNCS. 1995. V. 1008. P. 363-366.
2. *Rivest R. L.* The RC5 encryption algorithm // LNCS. 1995. V. 1008. P. 86-96.
3. *Rivest R. L., Robshaw M. J. B., Sidney R., and Yin Y. L.* The RC6 Block Cipher. V1.1, AES Proposal. 1998. http://www.rsa.com/rsalabs/aes.
4. *Beaulieu R., Shors D., Smith J., et al.* The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive. 2013. https://eprint.iacr.org/2013/404.
5. *Погорелов Б. А., Пудовкина М. А.* Подстановочные представления неабелевых 2-групп с циклической подгруппой индекса 2 // Матем. вопр. криптогр. 2021. Т. 12. (в печати)
6. Погорелов Б. А., Пудовкина М. А. Вариации ортоморфизмов и псевдоадамаровых преобразований на неабелевой группе // Прикладная дискретная математика. Приложение. 2019. №12. С. 24-27.
7. Погорелов Б. А., Пудовкина М. А. О классе степенных кусочно-аффинных подстановок на

неабелевой группе порядка $2^m$, обладающей циклической подгруппой индекса два // Прикладная дискретная математика. Приложение. 2019. № 12. С. 27-29.

8. Погорелов Б. А., Пудовкина М. А. Неабелевость группы наложения ключа и свойство ®w-марковости алгоритмов блочного шифрования // Матем. вопр. криптогр. 2020. Т. 11. № 4. С. 3-22.
9. Холл М. Теория групп. М.: ИЛ, 1962. 468 с.
10. Dixon J. D. and Mortimer B. Permutation Groups. Berlin: Springer Verlag, 1996. 346 p.
11. Grossman E. Group Theoretic Remark on Cryptographic System Based on Two Types of Additions. Math. Sc. Dept. IBM Watson res. Center Yorktown Heights, 1974.
12. Погорелов Б. А., Пудовкина М. А. Надгруппы аддитивных регулярных групп порядка $2^m$ кольца вычетов и векторного пространства // Дискретная математика. 2015. Т. 27. № 3. С. 74-94.
13. Бабаш А. В., Шанкин Г. П. Криптография. М.: СОЛОН-Р, 2002. 512 с.
14. Paterson K. G. Imprimitive permutation groups and trapdoors in iterated block ciphers // LNCS. 1999. V. 1636. P. 201-214.
15. *Погорелов Б. А.* Примитивные группы подстановок, содержащие $2^r$-цикл // Алгебра и логика. 1980. Т. 19. №2. С. 236-247.

УДК 519.7 DOI 10.17223/2226308X/14/23

# ПОРОЖДЕНИЕ ДОПОЛНИТЕЛЬНЫХ ОГРАНИЧЕНИЙ В ЗАДАЧАХ АЛГЕБРАИЧЕСКОГО КРИПТОАНАЛИЗА ПРИ ПОМОЩИ SAT-ОРАКУЛОВ[15]

А. А. Семёнов, К. В. Антонов, И. А. Грибанова

Описывается новая техника, предназначенная для дополнения исходной системы ограничений в задаче алгебраического криптоанализа новыми ограничениями. Порождаемые ограничения могут иметь форму линейных уравнений над полем из двух элементов в случае, если задача криптоанализа сведена к квадратичной системе над GF(2). Если же рассматриваемая задача сведена к SAT, то порождаемые ограничения имеют вид эквивалентностей или единичных резольвент. Для обеих ситуаций мы показываем, что порождаемые ограничения могут снижать оценки трудоёмкости криптоанализа.

**Ключевые слова:** *алгебраический криптоанализ, проблема булевой выполнимости (SAT), квадратичные системы уравнений над GF(2), SAT-оракул.*

## 1. Предварительные результаты

Везде далее под термином «ограничение» понимается либо линейное уравнение над GF(2), либо дизъюнкт. Рассматривается задача обращения функции вида

$$f: \{0,1\}^n \blacksquare \{0,1\}^m \qquad (1)$$

заданной некоторым алгоритмом $A_f$: то есть требуется, зная $A_f$ и произвольное $Y \in \text{Range } f \subseteq \{0,1\}^m$, найти такое $a \in \{0,1\}^n$, что $f(a) = Y$.

В алгебраическом криптоанализе [1] задача обращения (1) сводится к проблеме поиска решений алгебраических уравнений над некоторым конечным полем либо к проблеме выполнимости булевой формулы, обычно в конъюнктивной нормальной форме (КНФ). Везде далее рассматривается поле GF(2). Такая сводимость в теории является эффективной (следствие теоремы Кука — Левина [2, 3]). Более того, существует ряд программных систем, реализующих данную сводимость в отношении

[15]Грибанова И. А. поддержана стипендией Президента РФ (СП-3545.2019.5).

функций вида (1), заданных в виде императивных или функциональных программ. Упомянем здесь системы CBMC [4], Cryptol+SAW [5], Transalg [6], а также систему, описанную в [7]. Во всех представленных далее вычислительных экспериментах использовалась система Transalg. Данная система, получая на вход описание функции вида (1) на С-подобном языке, строит шаблонную КНФ $C_f$ [8]. Неформально говоря, КНФ $C_f$ представляет работу алгоритма $A_f$ на всех возможных входах из $\{0, 1\}^n$. Более точно, пусть $a = (a_1,\ldots, a_n)$ —произвольный набор из $\{0,1\}^n$, рассмотрим следующую КНФ:

$$C_f(a) = x^{a_1} \wedge \ldots \wedge x^{a_n}_n \wedge C_f, \qquad (2)$$

где обозначение $x^\sigma$ понимается в том же смысле, что ив [9]. Если применить к (2) правило распространения единичных дизъюнктов (Unit Propagation Rule, UP [10]), то за линейное от длины записи $C_f$ время по UP будут выведены значения всех переменных, входящих в $C_f$, в том числе и значения переменных $y_1, \ldots, y_m$, кодирующих выход функции (1). Каждой выводимой по UP переменной соответствует некоторая элементарная операция, выполняемая алгоритмом $A_f$, и, таким образом, применение UP к (2) можно рассматривать как способ вычисления $f(a)$.

Рассмотрим теперь произвольное $Y \in \mathrm{Range}\, f$, $Y = (Y_1, \ldots, Y_m)$, и построим следующую КНФ:

$$C_f(Y) = y^{Y_1}_1 \wedge \ldots \wedge y^{Y_m}_m \wedge C_f.$$

Поскольку $y \in \mathrm{Range}\, f$, то $C_f(y)$ выполнима, а из выполняющего её набора эффективно извлекается такой $a \in \{0,1\}^n$, что $f(a) = Y$ [8].

Разберём процесс построения $C_f$ в рамках процедур, используемых в системе Transalg. В данной системе вычисление функции $f$ на произвольном входе из $\{0, 1\}^n$ представляется в виде последовательности простых операций с ячейками памяти специальной абстрактной машины (АМ). Каждой такой операции сопоставляется булева формула следующего вида:

$$y = g(x_i,\ldots,x_s). \qquad (3)$$

Здесь $y$ — булева переменная, которая вводится на рассматриваемом шаге трансляции программы $A_f$; $x_1,\ldots, x_s$ —переменные, введённые на предыдущих шагах работы программы. Формула (3) соответствует вычислению значения некоторого оператора от битов, находящихся в ячейках памяти АМ, с которыми связаны переменные $x_1,\ldots, x_s$.

**Определение 1.** Функцию $g(x_1,\ldots, x_s)$, находящуюся в правой части произвольного соотношения вида (3), будем называть t-гейтом. Переменные, фигурирующие в (3), будем называть переменными рассматриваемого t-гейта.

Современные символьные трансляторы типа CBMC или Transalg позволяют задать функцию (1) в виде специального графа $G_f$, который есть, по сути, схема из функциональных элементов над базисом $\{, \wedge\}$. Граф $G_f$ известен как AIG (And Invertor Graph) [11]. Если произвольный гейт $g$ в $G_f$ — AND-гейт, то с $g$ связывается формула вида $y = x_1 \wedge x_2$, если $g$ — NOT-гейт (Invertor), то формула вида $y = \neg x_1$: переменная $y$ приписана рассматриваемому гейту, а переменные $x_1, x_2$ —гейтам, данные с которых подаются на вход $g$. Заданные так формулы имеют тот же смысл, что

и (3). Если все формулы вида $\wedge_л$ и $\wedge_-$ перевести в КНФ над множествами входящих в них переменных, а потом соединить все полученные КНФ конъюнкцией, то получится КНФ $C_f$, аналогичная по свойствам КНФ $C_f$. Будем называть $C_f$ шаблонной КНФ, порождённой графом $G_f$.

С другой стороны, мы можем сопоставить формулам $\wedge_л$ и $\wedge_-$ алгебраические уравнения над полем GF(2) = $h\{0,1\}, ф, Ai: e_л: X_1 Л x_2 ф y = 0$ и $e_- X_1 ф y = 1$ соответственно. Между множествами решений таких уравнений и множествами наборов, выполняющих формулы $\wedge_л$ и $\wedge_-$ существует очевидная биекция: пусть $a$ — набор, выполняющий формулу $\wedge_л$ или $\wedge_-$; если рассматривать компоненты набора $a$ как элементы поля GF(2), то $a$ является решением уравнения $e_л$ или $e_-$. Учитывая данный факт, везде далее будем обозначать переменные, входящие в формулы вида $\wedge_л$, $\wedge_-$ и в уравнения $e_л$, $e_-$, одинаковыми буквами.

Объединим все уравнения вида $e_л$, $e_-$, построенные по графу $G_f$, в систему, которую обозначим через $E_f$ и назовём шаблонной системой для функции $f$. Очевидно, что $E_f$ состоит из уравнений над GF(2) степени не более 2 и, таким образом, является MQ-системой (Multivariate Quadratic equation system [12]). Для системы $E_f$ справедливы свойства, похожие на свойства шаблонной КНФ $C_f$: 1) если подставить в $E_f$ произвольный набор $a E \{0,1\}^n$ и применить простые правила преобразования уравнений [13], рассматриваемые как правила вывода, то итогом такого вывода будут значения всех переменных, входящих в $E_f$, и, в том числе, такой набор $y_1 = 7_1, \bullet\bullet\bullet, y_m = 7_m$, что $f(a) = Y, 7 = (7_1, \bullet\bullet\bullet, 7_m)$; 2) если подставить в систему $E_f$ произвольный $Y E \mathrm{Range} f$, то полученная система $E_f(7)$ является совместной и из любого её решения можно эффективно выделить такой $a E \{0,1\}^n$, что $f(a) = 7$.

## 2. Применение SAT-оракулов для порождения дополнительных ограничений в задаче обращения (1)

В данной части мы развиваем идеи из [14] в нескольких направлениях, а именно: мы описываем новый подход, в рамках которого SAT-оракулы используются для порождения новых соотношений между переменными, присутствующими как в $C_f$, так и в $E_f$: в случае $C_f$ генерируемые соотношения имеют вид формул $x = y$, $x = —y$ либо единичных дизъюнктов. В случае $E_f$ мы строим новые линейные уравнения над GF(2). В отличие от подхода из [14], информация о функции $f$ используется более полно.

В основе всех приведённых далее результатов лежит следующее простое наблюдение: если применить какой-либо эффективный на практике SAT-решатель, основанный на алгоритме CDCL, к шаблонным КНФ вида $C_f$ или $C_f$, то этот решатель очень быстро (обычно за доли секунды) сгенерирует такую пару $(a, 7)$, что $f(a) = 7$.

Пусть g — некоторый t-гейт либо гейт в графе $G_f$. Заметим, что если g — NOT-гейт в $G_f$ и ему приписаны переменные x, y и связывающее их соотношение $x = —y$, то мы можем заменить все вхождения литерала $y (—y)$ на вхождения литерала $—x (x)$, избавившись тем самым от переменной y в $C_f$. С учётом сказанного будем рассматривать в графе $G_f$ только AND-гейты. Пусть g — произвольный AND-гейт с приписанной ему переменной y и входам g приписаны переменные $x_1$, $x_2$. Свяжем с g булеву функцию $5_g$, принимающую значение 1 на любом наборе переменных из {$x_1$, $x_2$, y}, на котором истинна формула $y = x_1 Л x_2$. Как известно, вклад, который даёт гейт

g в $C_f$ в результате преобразований Цейтина, — это следующая КНФ:

$$C_g : (x_i \vee -y) \wedge (X_2 \vee -y) \wedge (-X_1 \vee -X_2 \vee y).$$

Другой способ получения $C_g$ заключается в построении СКНФ $C_g$ по таблице, задающей функцию $fi_g$, и переходе от $C_g$ к $C_g$ в результате минимизации.

Пусть теперь g — произвольный AND-гейт в $G_f$ либо произвольный t-гейт типа (3). Функция $fi_g$, таблица $T(fi_g)$ и СКНФ $C_g$ для произвольного t-гейта g определяются так же, как и для AND-гейта. Пусть $T(fi_g)$ — таблица, образованная строками $T(fi_g)$, оставшимися после вычёркивания строк, по которым была построена КНФ $C_g$ .

**Пример 1.** Пусть g — AND-гейт, тогда таблица $T(fi_g)$ имеет следующий вид:

| $x_1$ | $x_2$ | $y$ | $^{s}\partial$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 |

Несложно понять, что для любого $a \in \{0,1\}^n$ применение UP к КНФ вида (2) выведет набор значений переменных гейта g (t-гейт или AND-гейт в $G_f$), являющийся одной из строк таблицы $T(fi_g)$.

Зафиксируем некоторое $k$, $1 \le k \le m$, и выберем конкретные $k$ выходов функции $f$, которым в $C_f$ или $C_f$ соответствуют переменные $y_{j_1},\ldots,y_{j_k}$, $J = \{j_1,\ldots,j_k\} \subseteq \{1,\ldots,m\}$.

**Определение 2.** Для фиксированного $J = \{j_1,\ldots,j_k\}$ определим функцию $f^J : \{0,1\}^n \to \{0,1\}^k$ следующим образом: на вход $f^J$ получает произвольный $a \in \{0,1\}^n$, значение $f^J(a)$ образовано компонентами с номерами $j_1,\ldots,j_k$ в наборе $Y = f(a)$. Произвольную функцию вида $f^J$ назовём селектором ранга $k$ (или кратко k-селектором) для $f$ .

Очевидно, что для произвольного $k$, $1 \le k \le m$, существует различных $k$ k-селекторов для $f$.

Основной технический результат работы [14] состоит в следующем. Рассмотрим произвольный AND-гейт g и КНФ _ _ _ ~ .

$$x^{\wedge} \wedge x_{2^2} \wedge y_3 \wedge C_f, \qquad (4)$$

где $(a_1a_2a_3)$—произвольный набор значений переменных $x_1,x_2,y$ из таблицы $T(fi_g)$. Применим какой-либо эффективный SAT-решатель к КНФ (4). Оказывается, что (4) не является трудной для современных полных SAT-решателей, даже если $f$ — криптографически стойкая функция. Ещё одно наблюдение состоит в том, что для многих AND-гейтов для некоторых строк таблицы $T(fi_g)$ SAT-решатель быстро доказывает невыполнимость КНФ (4). Как показано в [14], в этом случае мы можем добавить к системе $E_f$ новое линейное уравнение над GF(2).

Основную новизну настоящей работы составляет идея добавлять к КНФ типа (4) ещё и значения некоторых селекторов малого ранга $k$. То есть, грубо говоря, мы подставляем в (4) значения некоторых, но не всех бит выхода и применяем к такой КНФ SAT-решатель. Если он доказывает невыполнимость рассматриваемой КНФ, то это означает, что набор $(a_1a_2a_3)$ значений переменных $x_1, x_2, y$ ни при каком входе не совместим с конкретными значениями тех бит выхода функции f , которые

присутствуют в выбранном селекторе. Таким образом, для конкретного AND-гейта g можно перебрать все селекторы малого ранга (например, для $k \in \{1,2,3\}$), вызывая для каждого значения конкретного селектора и каждой строки таблицы $T(6_g)$ SAT-оракул O. Каждый раз, когда O доказывает невыполнимость соответствующей КНФ, получаем новое линейное уравнение над GF(2). Рассмотрим произвольный $y \in \mathrm{Range}\, f$. Очевидно, что для любого $\kappa$ можно представить Y как набор селекторов ранга $\kappa$. Например, для $\kappa = 2$

и $y \in \{0,1\}^m$ можно рассмотреть различных селекторов и их значений (двухбитовых векторов), определяемых набором $y$. Следовательно, рассматривая задачу поиска прообраза $y$ при отображении $f$, мы можем использовать все линейные уравнения, которые были построены SAT-оракулом для соответствующих селекторов.

По аналогии с использованием $\kappa$-селекторов для вывода линейных уравнений, дополняющих систему $E_f$, можно выводить при помощи селекторов и новые соотношения на переменные, присутствующие в шаблонной КНФ $C_f$. Рассмотрим соотношение (3) для произвольного t-гейта $\partial$ и пусть $T(6_g)$ —таблица (сокращение таблицы, задающей $6_g$) указанного вида, построенная для $\partial$. Пусть $(a_1,\ldots, a_{s+1})$ —произвольная строка таблицы $T(6_g)$. Рассмотрим шаблонную КНФ $C_f$, в которую подставим произвольные значения некоторого $\kappa$-селектора, и обозначим результирующую КНФ через $C_f$. Применим SAT-оракул $O$ к следующей КНФ:

$$X_p \wedge \ldots \wedge x'_{y^{\wedge}+1} \wedge C_f. \qquad (5)$$

Если O доказал невыполнимость (5), то это означает, что при фиксированном значении выбранного селектора ни на каком входе функции $f$ переменные $x_1,\ldots, x_s, y$ не примут значения $a_1,\ldots, a_{s+1}$. Соответственно такая строка вычёркивается из таблицы $T(6_g)$. В рассмотренных тестах таким способом могут быть вычеркнуты несколько строк таблицы при конкретном значении селектора. Результатом может быть, например, следующая ситуация (оставшиеся строки таблицы $T(6_g)$):

| $x_{3265}$ | $x_{2820}$ | $x_{2998}$ | $x_{3176}$ | $\wedge_\partial$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 |

В данном примере рассмотрена $T(6_g)$, полученная для некоторого t-гейта функции $g_{MID4\text{-}48}$ из [15]. Изначально таблица $T(6_g)$ состояла из 16 строк, а таблица $T(6_g)$ — из 8. После проверки SAT-оракулом всех строк таблицы $T(6_g)$ на совместность с шаблонной КНФ осталось 4 строки. Из этого фрагмента таблицы видно, что переменная $x_{3265}$ равна 0 при любом входе рассматриваемой функции. Кроме этого, для любого входа истинна формула $x_{2820} = x_{2998}$. Таким образом, все вхождения переменной $x_{2998}$ можно заменить вхождениями $x_{2820}$.

Если для конкретного селектора получены такого рода соотношения, мы можем хранить полученную информацию в специальной таблице и использовать её при обращении конкретных $y \in \mathrm{Range}\, f$, рассматривая $y$ как набор значений соответствующих селекторов.

Для тестирования описанной техники проведён ряд вычислительных экспериментов. Во всех экспериментах задействовался кластер Иркутского суперкомпьютерного центра [16]. Рассмотрены две криптографические функции.

В первой серии экспериментов мы рассмотрели 10-раундовую версию легковесного шифра Simon [17], конкретно — 64-битный вариант Simon, сокращённый до 10 раундов (в оригинальной версии 32 раунда). Исследовалась задача поиска 64-битного ключа по трём известным блокам открытого текста и шифртекста (напомним, что в шифре Simon используются 32-битные блоки). Решая данную задачу, мы искали линеаризующие множества в том же стиле, как это сделано в работах [13, 18]. Перебирались селекторы ранга $\kappa 63$. Предварительный расчёт с вызовом SAT-оракула для конкретных гейтов и конкретных значений селекторов занимал несколько суток работы кластера [16]. Затем с использованием данной информации решалась задача оптимизации целевой функции, описанной в [18]. Как итог была построена атака на рассматриваемый шифр с оценкой трудоёмкости примерно в 150 раз меньше, чем атака, аналогичная [18]. Результаты приведены в следующей таблице:

| Атака | Мощность линеаризующего множества | Оценка вероятности линеаризации | Оценка сложности атаки (число систем ЛУ) |
|---|---|---|---|
| 1 | 62 | 1 | $1{,}38 \cdot 10^{19}$ |
| 2 | 55 | 0,298 | $3{,}63 \cdot 10^{17}$ |
| 3 | 54 | 0,557 | $9{,}70 \cdot 10^{16}$ |

Здесь 1 — атака, использующая только технику из [18]; 2 — атака, использующая селекторные ограничения, но линеаризующее множество строится только на переменных ключа; 3 — атака, использующая селекторные ограничения, дополненная расширенным поиском линеаризующего множества (к переменным ключа добавляются некоторые переменные, функционально зависящие от ключа).

Во второй серии экспериментов мы рассмотрели задачу обращения полнораундовой функции сжатия алгоритма хеширования MD4 с использованием техники ослабляющих ограничений, описанной в [15, 19, 20]. Однако снижение трудоёмкости атаки за счёт использования информации от селекторов составило всего около 20 %. Отметим, что в этих экспериментах не использовалась информация от селекторов на этапе оптимизации функции, оценивающей трудоёмкость IBS-атаки. Возможно, именно поэтому достигнутые на данном этапе результаты не столь успешны, как с шифром Simon. Указанный недостаток мы планируем устранить в ближайшем будущем.

Авторы выражают глубокую благодарность Гладушу Андрею Игоревичу за помощь в проведении вычислительных экспериментов.

ЛИТЕРАТУРА

1. Bard G. Algebraic Cryptanalysis. Springer, 2009.
2. Cook S. A. The complexity of theorem-proving procedures // Proc. 3rd Ann. ACM Symp. Theory Comput. 1971. P. 151-158.
3. Левин Л. А. Универсальные задачи перебора // Проблемы передачи информации. 1973. Т. 9. № 3. С. 115-116.
4. Clarke E., Kroening D., and Lerda F. A tool for checking ANSI-C programs // LNCS. 2004. V. 2988. P. 168-176.
5. Erkok L., Carlsson M., and Wick A. Hardware/software co-verification of cryptographic algorithms using Cryptol // Proc. 9th Intern. Conf. FMCAD. IEEE, 2009. P. 188-191.
6. Otpuschennikov I., Semenov A., Gribanova I., et al. Encoding cryptographic functions to SAT using Transalg system // Frontiers Artificial Intell. Appl. 2016. V. 285. P. 1594-1595.
7. Калгин К. В., Софронова Д. А. Компактный транслятор алгоритмов в булевы формулы для

применения в криптоанализе // Прикладная дискретная математика. Приложение. 2020. №13. С. 135-136.
8. Semenov A., Otpuschennikov I., Gribanova I., et al. Translation of algorithmic descriptions of discrete functions to SAT with application to cryptanalysis problems // Log. Methods Comput. Sci. 2020. V. 16. Iss. 1. P.29:1-29:42.
9. Яблонский С. В. Введение в дискретную математику. М.: Наука, 1986.
10. Dowling W. F. and Gallier J. H. Linear-time algorithms for testing the satisfiability of propositional horn formulae //J. Log. Program. 1984. No. 1(3). P. 267-284.
11. Biere A. The AIGER And-Inverter Graph (AIG) format version 20071012. Tech. Report 07/1. Institute for Formal Models and Verification, Johannes Kepler University. 2007.
12. Kipnis A. and Shamir A. Cryptanalysis of the HFE public key cryptosystem by relinearization // LNCS. 1999. V. 1666. P. 19-30.
13. Семёнов А. А., Антонов К. В., Отпущенников И. В. Поиск линеаризующих множеств в алгебраическом криптоанализе как задача псевдобулевой оптимизации // Прикладная дискретная математика. Приложение. 2019. № 12. С. 130-134.
14. *Антонов К.В., Семёнов А.А.* Применение SAT-оракулов для генерации дополнительных линейных ограничений в задачах криптоанализа некоторых легковесных шифров. Прикладная дискретная математика. Приложение. 2020. № 13. С. 114-119.
15. *Грибанова И. А., Семёнов А. А.* Об аргументации отсутствия свойств случайного оракула у некоторых криптографических хеш-функций // Прикладная дискретная математика. Приложение. 2019. № 12. С. 95-98.
16. ЦКП Иркутский суперкомпьютерный центр СО РАН. http://hpc.icc.ru.
17. *Beaulieu R., Shors D., Smith J., et al.* The Simon and Speck lightweight block ciphers // Proc. 52nd Ann. Design Automation Conf. New York, USA, 2015. P. 175:1-175:6.
18. *Антонов К. В., Семёнов А. А.* Применение метаэвристических алгоритмов псевдобулевой оптимизации к поиску линеаризующих множеств в криптоанализе криптографических генераторов // Материалы 6-й Междунар. школы-семинара «Синтаксис и семантика логических систем». Иркутск: ИГУ, 2019. С. 13-18.
19. *Gribanova I. and Semenov A.* Using automatic generation of relaxation constraints to improve the preimage attack on 39-step MD4 // Proc. 41st Intern. Convention Inform. Commun. Technol. Electr. Microelectr. (MIPRO). IEEE, 2018. P. 1174-1179.
20. *Gribanova I. and Semenov A.* Parallel guess-and-determine preimage attack with realistic complexity estimation for MD4-40 cryptographic hash function // Материалы конф. «Параллельные вычислительные технологии (ПаВТ) 2019» (Калининград, 2-4 апреля 2019). С. 8-18.

УДК 621.391.7 DOI 10.17223/2226308X/14/24

## CHOOSING PARAMETERS FOR ONE IND-CCA2 SECURE McEliece MODIFICATION IN THE STANDARD MODEL

Y. V. Kosolapov, O. Y. Turchenko

The paper is devoted to choosing parameters for one IND-CCA2-secure McEliece modification in the standard model. In particular, the underlying code, plaintext length and one-time strong signature scheme are suggested. The choice of parameters for the scheme was based on efficiency, on the one hand, and security, on the other. Also, experiments for the suggested parameters are provided using the NIST statistical test suite.

**Keywords:** *post-quantum cryptography, McEliece-type cryptosystem,* IND-CCA2- *security, NIST statistical test suite.*

### 1. Introduction

The development of post-quantum cryptosystems resistant to adaptive chosen ciphertext attacks (IND-CCA2 secure cryptosystems) is currently relevant. In

particular, NIST hold competitions for the formation of post-quantum cryptography standards [1]. One of the most successful candidates [2] is based on the idea of random oracle. However, since random oracle is only theoretical function, then the construction of IND-CCA2 secure post-quantum cryptosystems without random oracles (standard model) is also an interesting task. One of the ways to construct such scheme is to modify McEliece cryptosystem [3]. For instance, in [4-6] authors modified McEliece cryptosystem using correlated products method [7]. This paper is devoted to choosing practical parameters for cryptosystem from [5].

## 2. Cryptosystem from [5]

Let $n$, $t$ be natural, $[n] = \{1,...,n\}$, $B \subset [n]$, $2^{[n]}$ is the set of all subsets of $[n]$, $F_2$ be a Galois field of cardinality $2$. The support of the vector $\mathbf{v} = (v_1,...,v_n) \in F_n$ is the set $supp(\mathbf{v}) = \{i : v_i \neq 0\}$ and the Hamming weight of this vector is a number $wt(\mathbf{v}) = |supp(\mathbf{v})|$. If $S$ is a finite set, then $s \xleftarrow{R} S$ denotes the operation of picking an element at random and uniformly from $S$. Denote by $E_{n,t,e}$ the subset of $F_n$ such that any vector $\mathbf{e} = (e_1,..., e_n) \in E_{n,t,e}$ has Hamming weight $t$ and $e_i = 0$ for any $i \in B$. We will write $E_{n,t}$ when $B = 0$. For the vector $\mathbf{v} \in F_k$ and the ordered set $\omega = \{\omega_1,... ,\omega_t\} \subset [k]$, where $\omega_1 < ... < \omega_t$, we consider the projection operator $\pi_L : F_k \to F_t$ acting according to the rule: $\pi_L(\mathbf{v}) = (v_{\omega_1},... ,v_{\omega_t})$. For $\omega$, consider a subset $G(\omega)$ of symmetric group $S_k$ acting on the elements of the set $[k]$:

$$G(\omega) = \{\pi \in S_k : \pi(1) = \omega_1,..., \pi(t) = \omega_t\}.$$

With every permutation $\pi$ from $G(\omega)$ we associate a permutation $(k \times k)$-matrix $R_\pi$.

Now we consider construction from [5]. Recall that a public key cryptosystem is a triplet of algorithms, i.e., $E = (K, E, D)$, where $K$ is a generation algorithm, $E$ is an encryption algorithm, $D$ is a decryption algorithm. We will write $\{\mathbf{m}\}_{pk}$ as encryption of the message $\mathbf{m}$ with the key $pk$ and $\{\mathbf{c}\}_{sk}$ as decryption of the ciphertext $\mathbf{c}$ on the secret key $sk$. For McEliece cryptosystem, we denote such triplet $E$ as McE.

In the cryptosystem $E$ [5], key generation algorithm $K_s$ takes as input two security parameters $N, s \in N$ and outputs a public-key $pk$ and a secret key $sk$ of the form

$$pk = ((pk_i^0, pk_i^1))_{i=1}^s, \qquad sk = ((sk_i^0, sk_i^1))_{i=1}^s,$$

where $pk_b, sk_b$ are generated by $K_{McE}$, $b \in \{0,1\}$, $i \in [s]$. The encryption algorithm $E_s$ takes as input a message $\mathbf{m} = (\mathbf{m}_1 \| \ldots \| \mathbf{m}_s)$, where $\mathbf{m}_i \in F_2^t$, and a public-key $pk$. Then $E_s$ generates two keys $\mathbf{dsk}, \mathbf{vk}$ for one-time strong unforgeable signature scheme, where $\mathbf{vk} = (vk_1, \ldots, vk_s)$, and outputs ciphertext

$$c = \mathbf{c} \| \mathbf{vk} \| a,$$

where $\mathbf{c} = \mathbf{c}_1 \| \ldots \| \mathbf{c}_s$ and $a$ is a signature of vector $\mathbf{c}$ with the key $\mathbf{dsk}$. Each $\mathbf{c}_i$ has the form

$$\mathbf{c}_i = c_1 \| \mathbf{c}_2 = \{(\mathbf{m}_i \| \mathbf{r}_i)R_n\}_{pk_{vk_i}} \| \{(\mathbf{m}_i \| \mathbf{r}_i \oplus \mathbf{1})R_n\}_{pk}, \qquad (1)$$

where $\mathbf{m}_i \in F_2$, $ш \in C_R$ [k], $|ш| = l$, $\mathbf{r}_i \in R\ F_{k-l}$, $n \in R\ G(ш)$. The error vectors $\mathbf{e}^1$ and $\mathbf{e}^2$ generated in McE-encryption in the left and right parts, respectively, are chosen such that $\mathbf{e}_1 \in R\ E_{n,t}$, $\mathbf{e}_2 \in R\ E_{n,t,supp(e1)}$. Decryption algorithm $D_s$ takes as input a secret-key sk and

a ciphertext $\mathbf{c}$, and outputs either a message $\mathbf{m} \in F_2^l$ or the error symbol $\pm$. On the first step, $D^{\wedge}$ checks signature of the message. If check fails, then $D_s$ outputs $\pm$, otherwise it computes $\mathbf{m} = \mathbf{m}_1 \| \ldots \| \mathbf{m}_s$, where

$$\mathbf{m}_i = \mathrm{Dec}_{\mathrm{ffi}}(\{\mathbf{cffi}), n_i = [k] \setminus \mathrm{supp}(\{\mathbf{c}_1\}M_{kv}E_i - \{c^{\wedge}).$$

If $n_i = \ldots = n_s$, then $D^{\wedge}$ outputs $\mathbf{m}$ else $\pm$.

Let us introduce additional notions. Denote public key $pk^{vk}$ from (1) as matrix $G_i$, $\mathbf{1}$ as all-ones vector from $\{0,1\}^{k_1}$, and $\mathbf{0}$ as all-zeroes vector from $\{0,1\}^{l}$. Then for matrix $G_i$ and secret permutation $(k \times k)$-matrix $R_n$, $n \in G(w)$, define $(l \times n)$-matrix $G^l$ and $(k - l \times n)$-matrix $G^2$ such that

$$G^{1} = R_n G_i.$$

Then we can write

$$\begin{aligned} \mathbf{c}_i = \mathbf{c}^1 \| \mathbf{c}^2 &= \{(\mathbf{m}_i \| \mathbf{r}_i) R_n G_i \oplus \mathbf{e}^1\} \| \{(\mathbf{m}_i \| \mathbf{r}_i \oplus \mathbf{1}) R_n G_i \oplus \mathbf{e}^1\} = \\ &= \{\mathbf{m}_i G^1 \oplus \mathbf{r}_i G^2 \oplus \mathbf{e}^1\} \| \{\mathbf{m}_i G^1 \oplus (\mathbf{r}_i \oplus \mathbf{1}) G^2 \oplus \mathbf{e}^2\}. \end{aligned} \quad (2)$$

Now one can suggest security parameters.

## 3. Security parameters and experiments

### 3.1. Security parameters

Let us consider the general security parameters of the system: underlying linear $[n, k, d]$-code $C$, plaintext length $l$ and one-time strong signature scheme. Since $(pk^b, sk^b) = = K_{McE}(N)$, $b \in \{0,1\}$, $i \in [s]$, then one can use known results of evaluating the code parameters of the original McEliece cryptosystem. In general, in [8] it is recommended to choose cryptosystem parameters with at least 86 security bits (for 2021 year). So, according to table 1.1 from [9] it is suggested to use $[4096, 3604, 83]$-code with 129 security bits. Then to prevent finding $u$ from $c^1 \oplus \mathbf{c}^2 = (\mathbf{0} \| \mathbf{1}) R_n G_i \oplus \mathbf{e}^1 \oplus \mathbf{e}^2 = \mathbf{1} G^2 \oplus \mathbf{e}^1 \oplus \mathbf{e}^2$ (see (2)) we recommend to choose $l$ with a restriction $14 \le l \le k - 14$. Particularly, if $l = 3604 - 14$, then the adversary has to enumerate $\binom{3590}{3604}$ variants (about 129 bits) to find $\mathbf{III}$ from $\mathbf{1}G^2$.

It is proposed to use an one-time strong signature scheme, on the one hand, resistant to quantum attacks, on the other hand, having a small public key size (since the number of repetitions $s$ is equal to the size of the verification key). In [10] authors compared different signature schemes. So, according to table 2 from [10] we suggest to use Stern signature as a one-time strong signature scheme with a small public key size (347 bits).

### 3.2. Experiments

The theoretical proof of the security of the cryptosystem under consideration is based on the randomness of vectors $\mathbf{1}G^2 \oplus \mathbf{e}^1 \oplus \mathbf{e}^2$ and $\mathbf{r}_i G^2 \oplus \mathbf{e}^1$. Thus, the aim of experiments is to find a dependence of randomness of these vectors on the parameter $l$. It is important to note that in [11] authors consider similar vector to $\mathbf{r}_i G^2 \oplus \mathbf{e}^1$. Based on time complexity for the "low weight codeword" attack, the authors suggest to use specific $l$. In our case, to implement such

attack, an adversary has to find the set Ш to determine the matrix $G_{i^2}$. For $l$ proposed above, the time complexity will be at least $2^{129}$.

The experiments are carried out as follows. The NIST statistical test suite [12] is used to test the randomness of vectors. The encryption algorithm of our construction is implemented using C# language. To generate random vectors, we use a cryptographic generator from namespace System.Security.Cryptography of C#. Since the aim of experiments is to find the dependence of randomness of cyphertexts on the parameter $l$, we generated several sets of random vectors from $\{0, 1\}^k$ having special weight. In the case when we test randomness of vector $\mathbf{r}_i G_{i^2} \oplus \boldsymbol{e}^j$, we generate random vectors from $\{0,1\}^k$ having weight less or equal $k - l$. In case when we test randomness of vector $\mathbf{1}G_{i^2} \oplus \boldsymbol{e}^j \oplus \mathbf{e}^2$, we generate random vectors from $\{0, 1\}^k$ having weight exactly $k - 1$. In particular, we generate 10000 vectors for each message type and parameter $l$. For the purity of the experiment, we also present the number of test passes for random vectors $\mathbf{v}$ from $\{0, 1\}^k$ generated by cryptographic generator with fixed weight. The results of experiments are presented in the Table. Symbol "*" means that $\mathbf{r}_i$ have weight exactly 1 (otherwise $\mathrm{wt}(\mathbf{r}_i) = 0$ and $\mathbf{r}_i G_{i^2} \oplus \mathbf{e}_{i^1} = \mathbf{e}_{i^1}$).

Number of tests passed out of 10 000 conducted

| $k - l$ | $\mathbf{v}$, $\mathrm{wt}(\mathbf{v}) = k - l$ | | $\mathbf{r}_i G_{i^2} \oplus \mathbf{e}^1$, $\mathrm{wt}(\mathbf{r}_i)$ 6 $k - l$ | | $\mathbf{1}G_{i^2} \oplus \mathbf{e}_{i^1} \oplus \mathbf{e}_{i^2}$ | |
|---|---|---|---|---|---|---|
| | Average | Minimum | Average | Minimum | Average | Minimum |
| 1 | 714 | 0 | 9850* | 9630* | 9843 | 9610 |
| 14 | 1528 | 0 | 9852 | 9626 | 9852 | 9648 |
| 66 | 1859 | 0 | 9851 | 9636 | 9850 | 9611 |
| 112 | 2097 | 0 | 9852 | 9582 | 9860 | 9651 |
| 225 | 2103 | 0 | 9854 | 9625 | 9854 | 9650 |
| 450 | 2697 | 0 | 9851 | 9594 | 9847 | 9623 |
| 901 | 2756 | 0 | 9844 | 9606 | 9852 | 9602 |
| 1700 | 7302 | 598 | 9850 | 9601 | 9851 | 9620 |
| 1802 | 9881 | 9532 | 9849 | 9600 | 9844 | 9625 |
| 2703 | 2041 | 0 | 9848 | 9613 | 9853 | 9620 |
| 3604 | 714 | 0 | 9843 | 9576 | 9862 | 9406 |

Thus, the results obtained show that the considered ciphertexts pass similar number of tests for all possible values of the parameter $l$.

REFERENCES

1. NIST. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.
2. Classic McEliece: conservative code-based cryptography. https://classic.mceliece.org/nist/mceliece-20171129.pdf.
3. McEliece R. J. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report, 1978, pp. 42-44.
4. Dottling N., Dowsley R., Quade J. M., and Nascimento A. C. A. A CCA2 secure variant of the McEliece cryptosystem. IEEE Trans. Inform. Theory, 2012, vol. 58(10), pp. 6672-6680.
5. Kosolapov Y. V. and Turchenko O. Y. Efficient S-repetition method for constructing an IND-CCA2 secure McEliece modification in the standard model. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2020,

vol. 13, pp. 80-84.
6. Persichetti E. On a CCA2-secure variant of McEliece in the standard model. Provable Security, 2018, vol. 11192, pp. 165-181.
7. Rosen A. and Segev G. Chosen-ciphertext security via correlated products. Proc. 6th Theory of Cryptography Conf., San Francisco, CA, USA, March 15-17, 2009, pp. 419-436.
8. Lenstra A. K. and Verheul E. R. Selecting cryptographic key sizes // J. Cryptology, 2004, vol. 14, pp. 446-465
9. Bernstein D. J., Chou T., and Schwabe P. McBits: Fast constant-time code-based cryptography. LNCS, 2013, vol. 8086, pp. 250-272.
10. Barreto A. and Misoczki R. A New One-Time Signature Scheme from Syndrome Decoding. IACR Cryptology ePrint Archive, 2010.
11. Nojima R., Imai H., Kobara K., et al. Semantic security for the McEliece cryptosystem without random oracles. Designs, Codes, Cryptogr., 2008, vol. 49, pp. 289-305.
12. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf.

UDC 003.26 DOI 10.17223/2226308X/14/25

# AN IMPROVEMENT OF CRYPTOGRAPHIC SCHEMES BASED ON THE CONJUGACY SEARCH PROBLEM[16]

V. A. Roman'kov

The key exchange protocol is a method of securely sharing cryptographic keys over a public channel. It is considered as important part of cryptographic mechanism to protect secure communications between two parties. The Diffie — Hellman protocol, based on the discrete logarithm problem, which is generally difficult to solve, is the most well-known key exchange protocol. One of the possible generalizations of the discrete logarithm problem to arbitrary noncommutative groups is the so-called conjugacy search problem: given two elements g, h of a group G and the information that $g^x = h$ for some x e G, find at least one particular element x like that. Here $g_x$ stands for $x^{-1}gx$. This problem is in the core of several known public key exchange protocols, most notably the one due to Anshel et al. and the other due to Ko et al. In recent years, effective algebraic cryptanalysis methods have been developed that have shown the vulnerability of protocols of this type. The main purpose of this short note is to describe a new tool to improve protocols based on the conjugacy search problem. This tool has been introduced by the author in some recent papers. It is based on a new mathematical concept of a marginal set.

**Keywords:** cryptography, key exchange protocol, conjugacy search problem, marginal set, algorithm.

## 1. Introduction

The first detailed proposal for a key exchange protocol, due to Diffie and Hellman [1], was based on the discrete logarithm problem for a finite field. This protocol is one of the earliest practical examples of public key exchange implemented within the field of cryptography. It was followed by few alternative proposals for key exchange protocols, all based on commutative algebraic structures.

Noncommutative cryptography is the area of cryptology where the cryptographic primitives, methods, and systems are based on algebraic structures like semigroups, groups and rings which are noncommutative. One of the earliest applications of a noncommutative algebraic structure for cryptographic purposes

[16]The research was supported by a grant from the Russian Science Foundation (project no. 19-71-10017).

was the use of braid groups to develop the Commutator key exchange protocol by Anshel, Anshel and Goldfeld (AAG) [2] and the noncommutative key exchange protocol on braids by Ko et al. [3]. Later, several other noncommutative structures like nilpotent and polycyclic groups, and matrix groups have been identified as potential candidates for cryptographic applications.

In [4], the author introduced the method of linear decomposition applicable in algebraic cryptanalysis. In [5], this method was further developed by the author and A. G. Myasnikov, see also [6]. In [7], this method was supplemented by the nonlinear decomposition method. These applications are called linear and nonlinear decomposition attacks respectively. They are deterministic, provable and polynomial-time. These methods were widely applied in cryptanalysis of dozens of protocols of algebraic cryptography, see monograph [8] and references therein. The linear decomposition attack can be applied to protocols based on matrix groups over arbitrary (finite or infinite) fields. The nonlinear decomposition attack is applicable to protocols based on groups that are not necessary matrix, or do not use matrix representations. The main distinguishing feature of these methods is that they reveal secret exchanged keys from open data without calculating the secret parameters used in the algorithm. Thus, we show that in this case, contrary to the common opinion, the typical computational security assumptions are not very relevant to the security of the schemes, i.e., one can break the schemes without solving the algorithmic problems on which the assumptions are based.

In [9] (see also [10]), B. Tsaban et al. introduced a method for obtaining provable polynomial-time solutions of problems in noncommutative algebraic cryptography called the linear span-method, or simply the span-method. This method is probabilistic. This method is a fundamental base for algebraic span cryptanalysis, a general approach for provable polynomial-time solutions of computational problems in groups of matrices over finite fields, and thus in all groups with efficient matrix representations over finite fields. This approach is widely applicable, in particular, it is applicable to the protocols mentioned above.

The main aim of this note is to describe the idea of using the concept of marginal sets to enhance the protocols based on the conjugacy search problem. In [11], the author presented an improved version of the AAG protocol based on this idea, see also [12] with some versions of AAG and Ko et al. protocols. In [13], the author proposed a new more strong version of the Diffie – Hellman non-commutative key exchange protocol of Ko et al. These new versions are resistant against attacks by methods of linear algebra. They are based on new hard algorithmic problems using a notion of a marginal set. In particular, they are resistant against attacks by the methods of Tsaban, and against the authors methods of the linear and nonlinear decompositions.

Notations: $\mathbf{N}$ – the set of nonnegative integers, $S_n$ – symmetric group of degree $n$, $g^h = hgh^{-1}$ – conjugate, $F_q$ – field of order $q$, $M(n, F_q)$ is the algebra of $n \times n$ matrices over $F_q$.

## 2. The marginal sets

The introducing concept of marginal set formally generalizes the well-known concept of the marginal subgroup, but it is worth noting that this generalization is very different from the original concepts.

The marginal subgroup is determined by the word, but the marginal subset is determined by the word and its chosen value. The set of all marginal subsets is not closed under algebra- and group-theoretic operations. It can be very wild.

For brevity, we give definitions only for the case of algebra.

Let $F$ be a free associative algebra with unity on a countably infinite set $\{x_1, x_2, \ldots\}$ and let $w = w(x_1,\ldots,x_k) \in F$. If $g_1,\ldots,g_k$ are elements of the algebra $M$, we define the value of the word $w$ at $g = (g_1,\ldots,g_k)$ to be $w(g) = w(g_1,\ldots,g_k)$.

A subset $N \subset M$ is said to be *w-marginal* in $M$ if

$$w(g_1,\ldots,g_k) = w(u_1g_1,\ldots,u_kg_k)$$

for all $g_i \in G$, $u_i \in N$, $1 \le i \le n$. Obviously, all $w$-marginal subsets constitutes the maximal marginal subset $w^*(M)$, which is a submonoid in $M_k$.

We introduce a new concept that significantly extends the marginality property.

**Definition 1.** For $k \in \mathbb{N}$, let $w = w(x_1,\ldots,x_k)$ be an algebra word, $M$ be an algebra and $g = (g_1,\ldots,g_k)$ be a tuple of elements of $M$. We say that a tuple $c = (c_1,\ldots,c_k) \in M^k$ is a *marginal tuple* determined by $w$ and $g$ if

$$w(c_1g_1,\ldots,c_kg_k) = w(g_1,\ldots,g_k).$$

We will write $c \pm w(g)$ in this case. A set $C \subset M_k$ is said to be *marginal* with respect to $w$ and $g$ if $c \pm w(g)$ for every tuple $c \in C$. We write $C \pm w(g)$ in this case.

Now we give a very simple and efficient algorithm for constructing a marginal set $C \pm w(g_1,\ldots,g_k)$. This method does not depend on the structure of $M$.

Let $w(g_1,\ldots,g_k) \in M$ be any value of $w(x_1,\ldots,x_k)$. Note that some elements $g_i, g_j$ can be equal to each other, that is, $g_i = g_j$. Consider an equation of the form

$$w(z_1g_1,\ldots,z_kg_k) = w(g_1,\ldots,g_k) \qquad (1)$$

such that there is $z_i$ that can be expressed in the form

$$z_i = z_i(z_1,\ldots,z_{i-1},z_{i+1},\ldots,z_k,g_1,\ldots,g_k). \qquad (2)$$

Then for any substitution $z_j = f_j$, $f_j \in M$, $j = 1,\ldots,i-1,i+1,\ldots,k$, we get a new marginal tuple

$$(f_1,\ldots,f_{i-1},z_i(f_1,\ldots,f_{i-1},f_{i+1},\ldots,f_k,g_1,\ldots,g_k),f_{i+1},\ldots,f_k) \in M^k \qquad (3)$$

with respect to $w$ and $gc$.

To hide the word $w$ in (1) and elements $f_1,\ldots,f_k, g_1,\ldots,g_k$, (2) can be rewritten by expressing all the constituent elements through parameters and the generating elements $m_1,\ldots,m_s$ of the algebra $M$. The formula (2) can be changed as follows. Let us introduce into consideration the set of parameters $y_1,\ldots,y_q$ with arbitrary values in $M$. Let $z_j = = z_j(y_1,\ldots,y_q,m_1,\ldots,m_s)$ be an arbitrary presentation for $j = 1,\ldots,i-1,i+1,\ldots,k$. Then $z_i = z_i^0(y_1,\ldots,y_q,m_1,\ldots,m_k)$ be the rewritten presentation (2) of $z_i$. These parametric presentations can be published. This form of representation does not make it easy to recover the word $w$ in (1).

Every solution of (1) can be included in a marginal set $C$, $C \pm w(g)$. We also can multiply a marginal tuple $c = (c_1,..., c_k)$ to any tuple $u = (u_1,..., u_k) \in w^*(M)^k$, and get new marginal tuple $ccuc = (u_1c_1, \ldots, u_kc_k)$.

## 3. An improved version of the conjugacy search problem

Recall the classical definition.

**Definition 2.** *Conjugacy Search Problem* (CSP). For a group $G$, we are asked to find an element $x$ from $u, v \in G$ satisfying $v = u^x \in G$.

The version suggested below uses any private expression of the element $g$ in the form of a word. Such view allows the use of a marginal set for given expression, defined below. It also becomes possible to apply multipliers that are not changed by the used transformation (conjugation). These methods protect the protocol from the attacks by methods of linear algebra. They change the underlying problem to a much more complex one. Let's move on to a description of the proposed changes. They are partially presented in [11-13].

Assumptions. Let $F$ be an arbitrary field (in particular $F_q$). Let $G \leq M(n, F)$ be a matrix group and $B$ be a finitely generated subgroup of $G$. Fix an element $g \in G$ $M = Alg(G)$ (the algebra generated by $G$ in $M(n, F)$). We assume that all the data above is public. We set $Fix(B) = \{o \in G : o^b = o$ for all $b \in B\}$.

Algorithm. Data selection and transmission.

Firstly we describe Alice's action:

- Alice chooses a tuple $g = (g_1,..., g_k) \in M_k$ and a ring word $u = u(x_1,..., x_k)$ such that $g = u(g_1, \ldots, g_k)$. This data is private.
- Alice takes arbitrary private elements $g_{k+1}, \ldots, g_m \in M$ (these elements are called *virtual)* to obtain $g = (g_1,...,g_k,g_{k+1},...,g_m) \in M_m$. She also chooses a private tuple of elements $h = (h_1, \ldots, h_k) \in Fix(B)^k$ and adds this tuple by random private elements $h_{k+1}, \ldots, h_m$ of $M$ to get $h = (h_1, \ldots, h_k, h_{k+1}, \ldots, h_m) \in M^m$. Alice gets $gh = gh = (g_1 h_1,...,g_k h_k, g_{k+1}h_{k+1},..., g_mh_m) \in M_m$. Then she picks up a private random permutation $n \in S_m$ and publishes the tuple

$$gh_n = (g_{n(l)}h_{n(l)}, \ldots ,g_{n(m)}h_{n(m)}).$$

- Alice constructs a marginal set $C \subset M^k$, $C \pm u(g_1,... ,g_k)$, adds each $c = (c_1,..., c_k) \in C$ by arbitrary elements $c_{k+1}, ...,c_m$ to get $c = (c_1,... , c_k, c_{k+1},..., c_m)$ and publishes $C_n \{c_n (c_{n(1)}, \ldots , c_{n(m)}) \blacksquare c \in C_n\}$.

Bob's action is similar. Now we restrict ourselves by considering the improved version of the conjugacy search problem, not some specific protocol.

*Algorithm. Data processing:*

- Bob chooses a random element $b \in B$.
- Bob chooses a random tuple $c_n \in C_n$ and calculates $c_n(gh)_n$. Then he computes

$$(c_n (gh)_n )_b = ((c_{n(1)}g_{n(1)} h_{n(1)} )^b, ..., (c_{n(m)}g_{n(p)}h_{n(p)})b)$$

and sends the result to Alice.

*Algorithm. The key generation.* Alice's action:

– Alice uses $n^{-1}$ to remove virtual elements and get from $(c_n(gh)_n)^b$ the tuple

$$(ccgc)^{b^c}h.$$

– She multiplies the result to $h^{-1} = (h_1^{-1}, \ldots, h_k^{-1})$ and gets $ccg^b$.

– Alice computes

$$u(ccg^b) = u(ccg)^b = u(gc)^b = g^b.$$

In many protocols Alice obtains the shared key as

$$K = (g^b)^a = g^{ab},$$

where $a \in G$ is her private element commuting with $b$.

Cryptanalysis. One cannot directly apply known method to calculate $b$. Indeed, for this one need in a pair of the form $r, r^b$ $(r \in M)$, but instead one has $r, (cr)^b$ $(c \in M)$.

Instead, one can try to find the word $u^0(x_1, \ldots, x_k)$ (one can be change $k$), indexes $i_1, \ldots, i_k$ and elements $h_i \in \mathrm{Fix}(B)$ $(i = 1, \ldots, k)$ so that

$$u^0(g_{i_1}h_{i_1}h^0_1, \ldots, g_{i_k}h_{i_k}h_k) = g.$$

But even if successful, this does not guarantee that the following equality holds:

$$u^0((g_{i_1}h_{i_1}h^0_1)^b, \ldots, (g_{i_k}h_{i_k}h_k)^b) = g^b,$$

because the marginality of $C$ depends of the word $u(x_1, \ldots, x_k)$ and in general is not true for another word that presents $g$.

REFERENCES


1. Diffie W. and Hellman M. I. New directions in cryptography. IEEE Trans. Inform. Theory, 1976, vol. 22, pp. 644-654.
2. Anshel I., Anshel M., and Goldfeld D. An algebraic method for public-key cryptography. Math. Res. Lett., 1999, vol. 6, no. 3, pp. 287-291.
3. Ko K. H., Lee S. J., Cheon J. H., et al. New public-key cryptosystem using braid groups. LNCS, 2000, vol. 1880, pp. 166-183.
4. Roman'kov V. A. Algebraicheskaya kriptografiya [Algebraic Cryptography]. Omsk, Omsk State University Publ., 2013, 136 p. (in Russian)
5. Myasnikov A. G. and Roman'kov V. A. A linear decomposition attack. Groups, Complex., Cryptol., 2015, vol. 7, no. 1, pp. 81-94.
6. Roman'kov V. A. Kriptoanalis nekotorih shem ispolzujushih avtomorfizmi [Cryptanalysis of some schemes applying automorphisms]. Prikladnaya Discretnaya Matematika, 2013, no. 3, pp. 35-51. (in Russian)
7. Roman'kov V. A. A nonlinear decomposition attack. Groups, Complex., Cryptol., 2016, vol. 8, no. 2, pp. 197-207.
8. Roman'kov V. A. Essays in Algebra and Cryptology: Algebraic Cryptanalysis. Omsk, Omsk State University Publ., 2018. 207 p.
9. Tsaban B. Polynomial-time solutions of computational problems in noncommutative-algebraic

cryptography. J. Cryptol., 2015, vol. 28, no. 3, pp. 601-622.
10. Ben-Zvi A., Kalka A., and Tsaban B. Cryptanalysis via algebraic span. LNCS, 2018, vol. 10991, pp. 255-274.
11. Roman'kov V. A. An improved version of the AAG cryptographic protocol. Groups, Complex., Cryptol., 2019, vol. 11, no. 1, pp. 35-42.
12. Roman'kov V, A. Algebraic cryptanalysis and new security enhancement. Moscow J. Combinat. Number Theory, 2020, vol. 9, no. 2, pp. 123-146.
13. Roman'kov V. A. An improvement of the Diffie-Hellman noncommutative protocol. Designs, Codes, Cryptogr., to appear.

Секция 4

# МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.056 DOI 10.17223/2226308X/14/26

## О КОНФИДЕНЦИАЛЬНОСТИ ТРАНЗАКЦИЙ В ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМАХ УЧЁТА ТОКЕНОВ

Л. Р. Ахметзянова, А. А. Бабуева, С. Н. Кяжин, В. А. Попов

Предлагается трёхуровневая модель функционирования децентрализованной системы, выделяется уровень, на котором выполняются протоколы формирования и валидации конфиденциальных транзакций. Приводится особенность обеспечения конфиденциальности транзакций в децентрализованных системах учёта токенов — потребность проверять выполнение различных условий для содержимого транзакций без получения доступа к нему. Выявляются классы неклассических (и нестандартизированных в России) криптографических механизмов, часто используемых в децентрализованных системах, в которых обеспечивается конфиденциальность транзакций. Показывается неуниверсальность существующих формальных определений таких систем, вследствие чего на текущий момент задача формализации свойства конфиденциальности транзакций в общем случае является открытой.

**Ключевые слова:** децентрализованная система, конфиденциальность, токен, доказательство с нулевым разглашением, гомоморфное шифрование, обязательство, коллективная подпись, кольцевая подпись.

### Введение

Рассмотрим класс информационных систем с реестром, где под реестром понимается совокупность данных, структурированных и хранимых в целях их учёта, поиска, обработки и контроля [1]. Среди таких систем выделим те, для которых реестр представляет собой таблицу соответствия идентификаторов пользователей и цифровых объектов, удостоверяющих некоторые права этих пользователей. Такие цифровые объекты будем называть токенами, такие системы — системами учета токенов, изменения, предлагаемые к внесению в реестр (таблицу) — транзакцией.

Транзакция в системе учёта токенов может быть интерпретирована как выпуск, уничтожение или перевод токенов от одного пользователя к другому. Отметим, что токены могут быть взаимозаменяемыми (в таком случае можно учитывать не каждый токен в отдельности, а лишь их количество; если в системе обрабатывается несколько величин, принято говорить о типе токенов) или невзаимозаменяемыми. В качестве примера системы учёта токенов можно привести систему электронных платежей, где реестр представляет собой таблицу соответствия идентификаторов пользователей и цифровых объектов, удостоверяющих право требования денежных средств.

В соответствии с политиками (настройками) системы можно выделить следующие роли уполномоченных пользователей:

— регистратор — может вносить изменения в реестр;

— наблюдатель — может осуществлять чтение из реестра;

— валидатор — может подтверждать корректность транзакций.

Если в системе имеется единственный пользователь-валидатор, то при её использовании возникает **проблема доверия** к этому валидатору. Например, для упомянутой системы электронных платежей отправители и получатели денежных средств вынуждены доверять оператору электронной платёжной системы, который принимает решение о корректности предлагаемых изменений. В случае существования подобной проблемы доверия может быть целесообразным использование децентрализованной системы, в которой имеется несколько пользователей-валидаторов, которые совместно (согласно установленным алгоритмам) принимают решение о корректности транзакций. Тогда требование доверия перекладывается с одного уполномоченного пользователя на нескольких.

В общем случае для подтверждения корректности транзакций необходима проверка выполнения некоторых условий, зависящих от состояния реестра. Если в системе несколько пользователей-валидаторов, то у каждого из них может быть своя версия состояния реестра, для которой они проверяют выполнение соответствующих условий. Таким образом, возникает потребность использования распределённого реестра, т. е. реестра, который физически распределён между уполномоченными пользователями, и обеспечения при этом согласованности его состояния.

В настоящей работе предлагается выявить особенности обеспечения конфиденциальности транзакций в децентрализованных системах учёта токенов.

## 1. О систематизации свойств децентрализованных систем

Децентрализованные системы представляют собой распределённый программно-технический комплекс, внутри которого функционирует большое количество различных протоколов. Сложность таких систем приводит к тому, что задача их синтеза и анализа также становится крайне трудоёмкой. Для упрощения этой задачи целесообразно строить модели функционирования децентрализованных систем, позволяющие разделять сложную систему на отдельные блоки и анализировать части системы независимо, т. е. проводить так называемый модульный анализ. По этой же причине важна систематизация свойств, выполнение которых требуется от каждой отдельной части системы.

В литературе наиболее глубокие модели децентрализованных систем предложены в работах [2, 3], однако с точки зрения особенностей обеспечения конфиденциальности транзакций, на наш взгляд, они обладают избыточной детализацией. В настоящей работе предлагается следующая **трёхуровневая модель функционирования децентрализованной системы**:

- нижний уровень (уровень консенсуса);
- средний уровень (уровень транзакций);
- верхний уровень (уровень приложений).

**Нижний уровень** оперирует с реестром как с целостным объектом (набором данных, структура которого не имеет значения). Цель протоколов, функционирующих на нижнем уровне, — обеспечить согласованность состояния реестра между несколькими уполномоченными пользователями. На нижнем уровне выполняются протоколы достижения консенсуса.

**Средний уровень** определяет структуру реестра и, как следствие, структуру транзакции. На среднем уровне выполняются:

- протокол формирования транзакции (выполняется независимо от состояния реестра, часто используется термин «оффчейн»);
- алгоритм валидации транзакции (выполняется пользователем-валидатором локально с использванием имеющейся у него версии состояния реестра).

На **верхнем уровне** выполняются протоколы решения конкретных бизнес-задач,

которые интерпретируют транзакции.

Таким образом, ограничение на класс систем, указанное во введении (системы учёта токенов), реализуется на среднем уровне.

Уровни взаимодействуют между собой следующим образом:

— выполняется протокол верхнего уровня, действия пользователей приводят к формированию входных данных для транзакции;
— на среднем уровне выполняется протокол формирования транзакции, а также алгоритм валидации транзакции, принимающий на вход транзакцию и состояние реестра, в результате формируется предлагаемое новое состояние реестра; транзакция является входными данными для протокола достижения консенсуса;
— на нижнем уровне выполняется протокол достижения консенсуса, в результате чего обновляется состояние реестра.

При этом подразумевается выполнение свойства инкапсуляции:

— обеспечение свойств системы на более низком уровне не зависит от обеспечения свойств на более высоких уровнях;
— обеспечение свойств системы на более низком уровне необходимо для обеспечения свойств на более высоких уровнях.

Стоит отметить, что при исследовании систем свойства протоколов одного уровня могут рассматриваться независимо от свойств протоколов другого.

Свойства протоколов верхнего уровня определяются бизнес-задачей, поэтому их можно рассматривать только для конкретных классов систем, решающих одинаковую задачу. На нижнем уровне существует множество протоколов достижения консенсуса (см., например, методические рекомендации [1] и обзорную работу [4]). Несмотря на различие этих протоколов, в [5] сформулированы единые (универсальные) свойства протоколов нижнего уровня: consistency, future self consistency, $\wedge$-chain quality, $g$-chain growth.

Для протоколов среднего уровня на текущий момент нет ни общего определения, ни строго определённых свойств безопасности. В литературе представлено большое количество самых разных протоколов, которые изначально разрабатывались под конкретные бизнес-задачи, накладывающие свои ограничения на вид этих протоколов и требуемые свойства.

Для класса систем с токенами можно выделить общие свойства корректности функционирования системы — **невозможность неполномочного выпуска, уничтожения и перевода токенов**. Для рассмотренного примера платежей это свойство можно интерпретировать как невозможность передать денежные средства, принадлежащие другому пользователю, а также создать или уничтожить их, не имея соответствующих полномочий. Существуют также свойства, которые не связаны напрямую с корректным функционированием системы. Например, может возникнуть потребность в обеспечении следующих свойств:

— конфиденциальность транзакции (содержимое транзакции неизвестно для пользователей-наблюдателей и пользователей-валидаторов, кроме тех, чьи идентификаторы входят в содержимое данной транзакции);
— анонимность участников (сторонний наблюдатель не может сопоставить участников протокола формирования транзакции и реальных пользователей системы).

Данные свойства могут быть связаны друг с другом. Для примера платежей содержимое транзакции может быть интерпретировано как «отправители», «получатели» и «суммы переводов». При этом пользователи, интерпретируемые как отправители и получатели, могут самостоятельно формировать транзакцию, то есть быть участниками протокола формирования транзакции. В таком случае, если будет

обеспечено свойство анонимности участников, но не будет обеспечена конфиденциальность транзакций, то информация об отправителях и получателях из транзакции может быть полезной для злоумышленника с точки зрения нарушения анонимности участников.

Обеспечение свойства конфиденциальности транзакций в децентрализованных системах имеет следующую отличительную особенность. Поскольку для выполнения алгоритма валидации транзакции пользователям-валидаторам, как правило, необходимо знать о её содержимом, но при этом среди валидаторов могут присутствовать такие, которым, согласно свойству конфиденциальности, должны быть неизвестны указанные данные, то возникает потребность проверять выполнение различных условий для содержимого транзакций без получения доступа к нему.

Свойство анонимности участников представляет меньший интерес, поскольку протокол формирования транзакции выполняется «оффчейн» и никаких особенностей обеспечения данного свойства в случае децентрализованных систем не имеется.

## 2. О криптографических механизмах обеспечения конфиденциальности транзакций

Поскольку обеспечение конфиденциальности транзакций напрямую связано с изменениями алгоритма валидации транзакции, то свойство конфиденциальности транзакций нельзя рассматривать независимо от свойств невозможности неполномочного выпуска, уничтожения и перевода токенов. В связи с этим необходимо рассматривать не механизмы обеспечения конфиденциальности транзакций в отдельности, а системы, в которых обеспечивается конфиденциальность транзакций в целом.

Существует достаточно много систем, в которых конфиденциальность транзакций обеспечивается с помощью криптографических механизмов (например, zCash [6, 7], CryptoNote [8], RingCT [9], AZTEC [10], MW [11, 12], Zether [13], патент Alibaba [14]). Некоторые системы, кроме криптографических механизмов, используют доверенную вычислительную среду (например, Ekiden [15], HLF Private Chaincode [16]).

Несмотря на то, что данные системы необходимо анализировать как единое целое, в процессе исследования (как в рамках анализа, так и в рамках синтеза) систем возникает естественное желание декомпозировать системы на отдельные криптографические механизмы. В результате обзора систем удалось выявить следующие наиболее часто используемые классы неклассических криптографических механизмов:

- схема гомоморфного шифрования (в [13, 14] используется для сокрытия количества токенов);
- схема обязательства/commitment (в [6, 7, 9, 10, 11, 14] используется для сокрытия количества токенов);
- схема кольцевой подписи (в [8, 9] используется для «перемешивания» идентификаторов пользователей или токенов);
- протокол доказательства с нулевым разглашением (в [6, 7, 9, 10, 11, 13, 14] используется для валидации транзакции без доступа к ее содержимому);
- схема агрегируемой/коллективной подписи (в [11] является вспомогательным механизмом, позволяющим упростить использование других механизмов).

При этом стоит сделать замечания:

- указанный список не является полным, другие примеры систем могут использовать другие криптографические механизмы;
- использование перечисленных механизмов в системах, обеспечивающих конфиденциальность транзакций, косвенно подтверждает недостаточность использования

классических криптографических механизмов (стандартизированных в РФ).

## 3. О формализации свойств децентрализованных систем

В связи со сложностью систем, в которых обеспечивается конфиденциальность транзакций, применение только методов криптоанализа, основанных на поиске методов взлома и обычно применяемых к базовым примитивам, становится недостаточным. В случае высокоуровневых протоколов, включающих в себя множество базовых криптографических механизмов, критичные уязвимости могут возникать не в базовых механизмах, а в порядке их использования.

В зарубежной литературе для анализа криптографических протоколов используются методы криптоанализа, основанные на теоретико-сложностных сведениях (парадигмы game-based [17], UC [18]) или применении автоматизированных средств формальной верификации [19]. Эти методы предполагают первоначальную разработку и формализацию моделей противника, включающих в себя описание угроз, возможностей противника и его ресурсов. Разработка релевантных моделей противника, наиболее полно с точки зрения практики отражающих аспекты свойств безопасности и возможностей противника, является одной из центральных задач данной области.

На текущий момент не существует устоявшегося формального определения системы, в которой обеспечивается конфиденциальность транзакций, и, следовательно, соответствующих общих формальных моделей противника для них. В литературе представлено много различных определений систем и моделей противника (например, [7, 12, 20, 21]), которые по-разному формализуют одни и те же свойства безопасности. Данное обстоятельство, а именно отсутствие единой системы оценивания криптографических качеств протоколов, приводит к снижению качества криптоанализа и увеличению риска появления уязвимостей в реальных системах.

Например, согласно [12], децентрализованная система учёта взаимозаменяемых токенов, в которой обеспечивается конфиденциальность транзакций, определяется следующими алгоритмами:

- Setup — алгоритм генерации общедоступных параметров системы, необходимых для её функционирования, и инициализации реестра;
- Mint — алгоритм формирования конфиденциальной транзакции выпуска токенов;
- Send, Rcv — алгоритмы формирования конфиденциальной транзакции перевода токенов (первый алгоритм выполняется отправителем, второй — получателем);
- Ldgr — алгоритм обновления состояния реестра, включающий в себя механизмы валидации транзакции.

В данном определении авторы разделили протокол формирования конфиденциальной транзакции на алгоритмы Send, Rcv. В общем случае это не всегда возможно — процесс формирования транзакции перевода зачастую предполагает выполнение протокола (может быть, интерактивного) между получателем и отправителем. Таким образом, приведённое определение не является общим и не позволяет явно разделить систему на модули (подпротоколы) для анализа релевантности моделей противника и проведения теоретико-сложностных оценок. Итак, считаем необходимым сформировать универсальные строгие определения систем (возможно, отдельно для разных классов систем).

В работе [12] даются также формальные определения свойств невозможности неполномочного выпуска токенов, невозможности неполномочного перевода токенов и конфиденциальности количества токенов, участвующих в транзакции, и доказывается, что система MW удовлетворяет им. Однако поскольку определения свойств связаны с формальным определением системы, они также не являются общими.

## Заключение

В работе показана актуальность задачи разработки децентрализованных систем учёта токенов, в которых обеспечивается конфиденциальность транзакций, несмотря на существование примеров таких систем.

Первоначальным этапом при решении этой задачи видится систематизация моделей противника, предложенных в [7, 12, 20, 21], путём выявления соотношений между ними, а именно: осмысление формально определяемых угроз и типов атак и определение того, какие модели являются более сильными, более слабыми или вообще несоотносимыми друг с другом (так как учитывают различные свойства безопасности). В силу того, что рассматриваемые системы и предложенные для них модели являются достаточно новыми и, как следствие, малоизученными, не менее важным представляется этап анализа моделей на предмет их релевантности и достаточности с точки зрения целевых свойств безопасности и при необходимости их дальнейшая доработка, например, путём расширения рассматриваемых типов атак.

После разработки релевантной модели противника необходимо проанализировать системы, предложенные в [6-16], на предмет выполнения свойств безопасности, соответствующих модели. Если среди перечисленных систем не окажется той, для которой выполняются данные свойства, то в качестве следующего этапа необходимо доработать эти системы, например, путем замены используемых криптографических механизмов на более эффективные/стойкие (при необходимости — разработать такие механизмы).

Например, предположим, что протокол MW является стойким в релевантной модели противника при условии использования стойких криптографических механизмов. В таком случае может потребоваться его адаптация к исследованным российским криптографическим алгоритмам. Так, в частности, актуальной становится задача разработки схемы агрегируемой/коллективной подписи на основе стандартизированной в РФ схемы подписи [22] (попытка построения такой схемы сделана в [23]) и анализ её стойкости в модели EUF-CMA.

ЛИТЕРАТУРА

1. Методические рекомендации ТК 26 МР 26.4.001-2018 «Информационная технология. Криптографическая защита информации. Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров». М.: Технический комитет по стандартизации «Криптографическая защита информации», 2018.
2. Zhang R., Xue R., and Liu L. Security and privacy on blockchain // ACM Computing Surveys. 2019. V. 52. No. 3. Art. 51. 34p.
3. Sai A. R., Buckley J., Fitzgerald B., and Le Gear A. Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review. 2020. https://arxiv.org/pdf/2009.12542.pdf
4. Nijsse J. and Litchfield A. A taxonomy of blockchain consensus methods // Cryptography. 2020. V.4. No. 4. Art. 32. 15p.
5. Pass R., Seeman L., and Shelat A. Analysis of the blockchain protocol in asynchronous networks // EUROCRYPT 2017. Springer, 2017. P. 643-673.
6. Zcash Protocol Specification. 2021. https://github.com/zcash/zips/blob/master/protocol/protocol.pdf
7. Ben Sasson E., Chiesa A., Garman C., et al. Zerocash: Decentralized anonymous payments from bitcoin // IEEE Symp. Security Privacy. San Jose, CA, 2014. P. 459-474.
8. CryptoNote v 2.0. 2013. https://cryptonote.org/whitepaper.pdf
9. Yuen T. H., Sun S.-F., Liu J. K., et al. RingCT 3.0 for blockchain confidential transaction: Shorter size and stronger security // LNCS. 2020. V. 12059. P. 464-483.
10. AZTEC Protocol. 2018.

https://github.com/AztecProtocol/AZTEC/blob/master/AZTEC. pdf
11. Poelstra A. Mimblewimble. 2016. https://download.wpsoftware.net/bitcoin/wizardry/ mimble-wimble.pdf
12. Fuchsbauer G., Orru M., and Seurin Y. Aggregate cash systems: a cryptographic investigation of Mimblewimble // LNCS. 2019. V. 11476. P. 657-689.
13. Bunz B., Agrawal S., Zamani M., and Boneh D. Zether: Towards privacy in a smart contract world // LNCS. 2020. V. 12059. P. 423-443.
14. Zhang W. and Ma B. Blockchain Data Protection using Homomorphic Encryption. US Patent 2019/0253235 A1.
15. Cheng R., Zhang F., Kos J., et al. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts // IEEE Europ. Symp. Security Privacy. 2019. P. 185-200.
16. Brandenburger M., Cachin C., Kapitza R., and Sorniotti A. Blockchain and trusted computing: Problems, pitfalls, and a solution for Hyperledger Fabric. 2018. https://arxiv. org/pdf/1805.08541.pdf
17. Hevia A. Introduction to Provable Security. Advanced Crypto School, Florianopolis, 2013.
18. Canetti R. Universally composable security: a new paradigm for cryptographic protocols // 42nd IEEE Symp. Found. Comput. Sci. IEEE, 2001. P. 136-145.
19. Cremers C. and Mauw S. Operational Semantics and Verification of Security Protocols. Springer Verlag, 2012. 174 p.
20. Guan Z., Wan Z., Yang Y., et al. BlockMaze: An efficient privacy-preserving account-model blockchain based on zk-SNARKs // IEEE Trans. Dependable Secure Comput. IEEE, 2020. https://eprint.iacr.org/2019/1354.pdf.
21. Mitani T. and Otsuka A. Confidential and auditable payments // LNCS. 2020. V. 12063. P. 466-480.
22. Межгосударственный стандарт ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». М.: Стандартинформ, 2018.
23. Молдовян Н. А. Теоретический минимум и алгоритмы цифровой подписи. СПб.: БХВ-Петербург, 2010. 304с.

УДК 004.056.5, 004.94 DOI 10.17223/2226308X/14/27

# О ПРИЁМАХ ПО ДОРАБОТКЕ СОГЛАСОВАННОГО ОПИСАНИЯ МРОСЛ ДП-МОДЕЛИ ДЛЯ ОС И СУБД С ЦЕЛЬЮ ЕГО ВЕРИФИКАЦИИ ИНСТРУМЕНТАМИ Rodin И ProB

П. Н. Девянин, М. А. Леонова

Рассматриваются приемы согласованного описания мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в операционных системах семейства Linux (МРОСЛ ДП-модели) в математической и формализованной нотациях с целью обеспечения возможностей для, во-первых, её совместной верификации дедуктивным методом и методом проверки моделей (model checking) с применением инструментов Rodin и ProB соответственно, во-вторых, моделирования на формализованном языке метода Event-B взаимодействующих между собой систем с собственными развитыми механизмами управлениями доступом, таких, как ОС и СУБД, что необходимо для соответствия описанию модели в математической нотации.

**Ключевые слова:** формальная модель управления доступом, верификация, Event-B, требования доверия, Astra Linux Special Edition.

## Введение

В средствах защиты информации (СЗИ), таких, как ОС или СУБД, механизм управления доступом выполняет одну из основных функций по обеспечению их безопасности. Для достижения доверия к корректности этого механизма, создания условий для научного обоснования выполнения им заданных для СЗИ требований безопасности уже многие десятилетия разрабатываются формальные модели

управления доступом [1-3].

Изначально эти модели формировались на математическом языке (в математической нотации), вместе с этим по мере увеличения объёмов описания формальных моделей, в связи с необходимостью устранения в них ошибок, для описания формальных моделей стали применяться формализованные (машиночитаемые) языки (формализованная нотация), например язык формального метода Event-B [4]. При этом для автоматизированной проверки корректности и верификации описания моделей в формализованной нотации начали использоваться соответствующие инструменты, например инструмент дедуктивной верификации Rodin [5].

В настоящее время требования по разработке формальных моделей управления доступом и их верификации стали частью актуальных нормативных документов, определяющих требования доверия к сертифицированным СЗИ. Так, согласно утверждённым Приказом ФСТЭК России № 76 от 02.06.2020 во второй редакции «Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» [6], механизм управления доступом СЗИ должен разрабатываться на основе формальной модели управления доступом (начиная с четвёртого уровня доверия), которая должна быть верифицирована с применением инструментальных средств (начиная с третьего уровня доверия). Кроме того, для стандартизации применяемых для этого методов и технологий недавно утверждены два национальных стандарта ГОСТ Р 59453.1-2021 и ГОСТ Р 59453.2-2021 [7, 8].

Поскольку разрабатываемая ООО «РусБИТех-Астра» (ГК Astra Linux) операционная система специального назначения (ОССН) Astra Linux Special Edition [9, 10] в системе сертификации ФСТЭК России сертифицирована по высшему первому классу защиты (первому уровню доверия), её подсистема безопасности PARSEC создана на основе мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux (МРОСЛ ДП-модели) [3]. Её описание в математической нотации составляет более 500 страниц текста. Она имеет иерархическое представление, состоящее из восьми уровней — четырёх уровней для моделирования управления доступом непосредственно в ОССН и четырёх аналогичных уровней для штатной для ОССН СУБД PostgreSQL.

Отмеченные объём и сложность описания и, как следствие, проверки корректности МРОСЛ ДП-модели в математической нотации стали стимулом для её описания в формализованной нотации на языке метода Event-B и автоматизированной дедуктивной верификация с применением инструмента Rodin [11]. В этой нотации текущее представление модели также имеет значительный объём (более 15 тысяч строк кода). Кроме того, для повышения качества модели авторами освоена технология верификации формальной модели с применением метода проверки моделей (model checking), реализованном в инструменте ProB [12]. Всё перечисленное требует поиска приёмов и технологий согласованного для ОС и СУБД описания МРОСЛ ДП-модели в математической и формализованной нотациях, обеспечения условий для её автоматизированной верификации дедуктивным методом и методом проверки моделей. Анализу возникающих здесь проблем и выработанным авторами новым техническим приёмам для их решения посвящается настоящая работа.

## 1. Согласованное описание модели для ОС и СУБД в математической и формализованной нотациях

В формализованной нотации МРОСЛ ДП-модель разрабатывается в виде последовательности связанных между собой спецификаций, соответствующих уровням в её математической нотации, с использованием техники пошагового уточнения

(refinement) [13] на языке формального метода Event-B, что позволяет повысить качество модели и устранить возможные ошибки. В каждой спецификации элементам, задающим в рамках соответствующего уровня состояния моделируемой ОССН, в модели в формализованной нотации ставятся в соответствие переменные Event-B, а правилам перехода из состояний в состояния — события Event-B. Инварианты на переменные описывают свойства внутренней согласованности элементов соответствующей спецификации модели, в том числе свойства безопасности. При этом доказательство того, что любой переход из состояния в состояние, заданный событиями Event-B, сохраняет все инварианты состояния, а значит, корректности описания модели и выполнения в её рамках условий безопасности, осуществляется с применением инструмента дедуктивной верификации Rodin.

Накопленный опыт формирования МРОСЛ ДП-модели в формализованной нотации, проведённые авторами научные исследования по данному направлению выявили ряд недостатков в используемых для этого технологиях и приёмах, такие, как часто независимое друг от друга описание элементов модели для различных видов управления доступом, а также многократное дублирование одинаковых условий их выполнения, не соответствующее реализации проверок этих условий непосредственно в программном коде ОССН; сложность добавления уровней уточнений, моделирующих взаимодействующие с ОССН системы, ввиду того, что в изначально использованном подходе по формированию структуры элементов модели [11] не предусматривалось логического разделения элементов, предназначенных для моделирования различных, но взаимодействующих между собой механизмов управления доступом, например, реализуемых PARSEC в ОССН и СУБД PostgreSQL.

Для устранения данных недостатков предложен ряд приёмов [14]: логическое объединение проверок условий, заданных для мандатных управления доступом, контроля целостности и ролевого управления доступом путём применения тотальных функций формализованного языка метода Event-B, а также использование при построении структуры элементов модели подтипов формализованного языка метода Event-B, которые позволяют раздельно описывать такие существенные для моделирования управления доступом элементы, как субъекты (процессы), сущности (файлы, каталоги, базы данных), учётные записи пользователей, роли, информационные потоки.

В процессе добавления уровней уточнений были выявлены трудности, связанные с применяемой Rodin техникой refinement, а именно строго последовательное (линейное) уточнение уровней. Это не соответствует иерархическому представлению МРОСЛ ДП-модели в математической нотации, в котором каждый из уровней моделируемого механизма управления доступом взаимодействующей с ОССН системы уточняет предыдущий для неё уровень, а также соответствующий уровень аналогичного механизма самой ОССН (например, в модели уровень мандатного контроля целостности СУБД основан на уровнях ролевого управления доступом СУБД и мандатного управления доступом ОССН). Ещё одним ограничением, накладываемым логикой пошагового уточнения, является отсутствие возможности изменения значений определяемых инвариантами функций на любых уровнях спецификаций, кроме того, на котором они задаются, хотя это необходимо для корректного моделирования взаимодействия систем (например, возникновения информационных потоков между элементами ОССН и СУБД).

В результате потребовалось найти такой приём по уточнению уровней модели в формализованной нотации, который, с одной стороны, был бы логически согласован с порядком уточнения уровней иерархического представления модели в математической нотации, а с другой стороны, использовал бы имеющуюся в Rodin

технику refinement для сохранения возможности дедуктивной верификации модели. Этим решением стало последовательное уточнение уровней спецификаций модели для ОССН уровнями взаимодействующей с ней системы, но с переопределением на них необходимых для согласованности модели в математической и формализованной нотациях функций и событий. Например, переопределение на втором уровне модели для СУБД заданных на аналогичном уровне ОССН функций информационных потоков по памяти от субъектов к сущностям SEM F lows, от субъектов к субъектам SSMFlows, де-факто события создания информационного потока по памяти от субъекта к сущности при наличии субъекта-посредника f ind_entity _m, и задания новых функций dbSEM F lows, dbSSF lows, а также соответствующих де-факто событий для ОС os_f ind_entity и для СУБД db_f ind_entity (листинг 1).

```
os_f ind_entity
ANY
x, y, z, flow

WHERE
grd1: x ∈ Subjects
grd2: y ∈ Subjects
grd3: z ∈ Entities
grd4: flow ∈ P1({1,2})
//"1" - информационный поток по памяти, "2" - информационный поток по времени
grd5: 1 ∈ flow ^ z ∈ EHole
grd6: 1 ∈ flow ^ y ^ 1 ∈ dbSSFlows(x) Л z ^ 1 ∈ dbSEFlows(y)

THEN
act1: dbSEFlows(x) := dbSEFlows(x) U ({z} x flow)

db_f ind_entity
ANY
x, y, z, flow

WHERE
grd1: x ∈ Subjects
grd2: y ∈ Subjects
grd3: z ∈ Entities
grd4: flow ∈ P1({1,2})
grd5: 1 ∈ flow ^ z ∈ DBEHole
grd6: 1 ∈ flow ^ y ^ 1 ∈ dbSSFlows(x) Л z ^ 1 ∈ S_DBEFlows(y)

THEN
act1: S_DBEFlows(x) := S_DBEFlows(x) U ({z} x flow)
```

Листинг 1. Общие для ОС и СУБД де-факто события

Достоинством данного приёма является возможность сохранять уровни спецификаций для моделируемого механизма управления доступом ОССН отдельно от соответствующих уровней для других систем. При этом он обладает и явным недостатком, заключающимся в необходимости повторения уже проведённых доказательств и увеличении объёма кода описания модели в формализованной нотации.

## 2. Совместная верификация инструментами Rodin и ProB

Для повышения качества верификации МРОСЛ ДП-модели в формализованной нотации, расширения спектра применяемых для этого методов и инструментов, моделирования и в перспективе автоматизированного тестирования на соответствие этой

модели её реализации непосредственно в программном коде и настройках конфигурации механизма управления доступом ОССН осуществляется верификация модели с использованием инструмента проверки моделей ProB [12].

Как и для инструмента Rodin, здесь также выявлены трудности непосредственного применения ProB, связанные с большим объёмом описания модели в её формализованной нотации и использованием ряда способов представления модели на формализованной языке метода Event-B, не вызывавших затруднений при её дедуктивной верификации инструментом Rodin, но оказавшихся непригодными для применения ProB. Так, его работа часто завершалась с ошибкой вида timeout, вызванной превышением допустимого интервала времени, установленного для выполнения ProB переборных алгоритмов (ошибка такого вида является следствием проявления «комбинаторного взрыва»).

Это, в свою очередь, потребовало проведения исследований и разработки соответствующих приёмов [15], позволяющих осуществлять согласованную верификацию описания всех восьми уровней МРОСЛ ДП-модели в формализованной нотации инструментами проверки моделей ProB и дедуктивной верификации Rodin.

Примером одного из таких приёмов является использование нескольких несущих множеств (глобальных типов, над которыми не допускаются операции объединения, пересечения, разности, дополнения, какие-либо дополнительные ограничения на эти множества могут быть заданы только аксиомами), но с сохранением подхода по применению подтипов [14]. С комбинаторной точки зрения полезно рационально определять типы, уходя от использования одного глобального типа для всех элементов модели, но и сохраняя преимущества применения подтипов там, где это необходимо (например, разделяя глобальные типы для сущностей и ролей и при этом используя отдельные подтипы глобального типа ролей для обычных, административных и запрещающих ролей).

Примером способа представления модели на формализованном языке метода Event-B, не вызывавшего затруднения при её дедуктивной верификации инструментом Rodin, но оказавшегося непригодными для применения ProB, является также описанный в [11] способ, позволяющий применять при доказательствах математическую индукцию, что в Rodin сделать непосредственно невозможно. Данный способ заключается во внесении в контекст первого уровня (ролевого управления доступом) формализованной нотации хорошо известной в математике аксиомы (листинг 2), где $\mathbb{N}$ – множество натуральных чисел, включая нуль. При этом в событиях, требующих доказательства инварианта с применением индукции, добавляются специальный параметр-функция и ряд охранных условий, проверяющих условия истинности инварианта, используя описанную аксиому. Например, в событии передачи административных прав доступа grant_admin_rights параметром-функцией depth задаются потомки роли *role* (роли, стоящие ниже неё в иерархии) и охранными условиями grd16-grd19 проверяются отношения уровней целостности данных потомков (листинг 3), т. е. роль, находящаяся выше в иерархии, должна иметь уровень целостности не ниже уровней целостности её потомков.

```
InductionAxiom: ∀s · s ⊆ ℕ ∧ 0 ∈ s ∧ (∀n · n ∈ s ⇒ n + 1 ∈ s) ⇒ ℕ ⊆ s
```

Листинг 2. Задание аксиомы индукции

```
invariant RParents4: ∀r, p · r ∈ Roles ∧ p ∈ RParents(r) ⇒ RoleInt(r) ⊆
```

```
   RoleInt(p) grant_admin_rights

   ANY
   depth

   WHERE
   grd16: depth ∈ N ^ P(dom(admRights))
   grd17: ∀r · r ∈ dom(admRights) ⇒ ∃i · i ∈ N ∧ r ∈ depth(i))
   grd18: depth(0) = {role}
   grd19: ∀i · i ∈ N ⇒ (∀r · r ∈ depth(i + 1) ⇒ ∃p · p ∈ depth(i) ∧ p ∈ RParents(r)))
theorem grd20: ∀i · i ∈ N ∧ (∀r · r ∈ depth(i) ⇒ RoleInt(r) ⊂ RoleInt(admRole)) ⇒
(∀r · r ∈ depth(i + 1) ⇒ RoleInt(r) ⊆ RoleInt(admRole))
   theorem grd21: ∀i · i ∈ N ⇒ (∀r · r ∈ depth(i) ⇒ RoleInt(r) ⊂ RoleInt(admRole))
```

Листинг 3. Задание потомков роли в иерархии с использованием индукции

При попытке задать контекст первого уровня и подобрать параметры для событий, включающих в себя данную структуру, ProB завершает работу с ошибкой вида timeout. Приёмом, позволяющим, с одной стороны, сохранить полноту дедуктивной верификации модели инструментом Rodin, а с другой — иметь возможность её верификации по методу проверки моделей с применением ProB, является задание параметра-функции в виде тотальной функции, один из инвариантов-истинности которой должен описывать шаг индукции. Далее при доказательстве сохранения в соответствующих событиях основанных на индукции инвариантов использовать такую тотальную функцию. Например, для задания потомков роли без явного использования индукции применяются инварианты DescendantsRT ype, DescendantsR1, DescendantsR2, N oCyclesF orRoles, задающие функцию потомков роли, и инвариант DescendantsR6, описывающий соответствующее шагу индукции условие, при котором уровень целостности роли должен быть не ниже уровня целостности каждого ее потомка (листинг 4).

```
   DescendantsRType: DescendantsR ∈ Roles ^ P(Roles)
   DescendantsRl: ∀r,d · r ∈ Roles ∧ d ∈ Roles ^ (d ∈ DescendantsR(r) ^
d = r ∨ (d = r ∧ (∃k · k ∈ KidsR(r) ∧ d ∈ DescendantsR(k))))
   DescendantsR2: ∀r,d · r ∈ Roles ∧ d ∈ Roles ^ (d ∈ DescendantsR(r) ^ DescendantsR(d)
⊂ DescendantsR(r))
   NoCyclesForRoles: ∀r,d · r ∈ Roles ∧ d ∈ Roles ∧ d ∈ DescendantsR(r) ∧
d = r ^ r ∈ DescendantsR(d)
   DescendantsR6: ∀r, p · r ∈ Roles ∧ p ∈ Roles ∧ r ∈ DescendantsR(p) ^ RoleInt(r) ⊂
RoleInt(p)
```

Листинг 4. Задание потомков роли в иерархии с использованием тотальной функции

## Выводы

В результате проведённых исследований расширен спектр технических приёмов, позволяющих осуществлять согласованное описание для ОС и СУБД уровней иерархического представления МРОСЛ ДП-модели в математической и формализованной нотациях на языке метода Event-B. Эти приёмы базируются на выражении в последовательном уточнении уровней модели на основе техники refinement свойств исходного иерархического представления модели и на применении тотальных функций вместо непосредственного использования аксиомы математической индукции. В итоге эти приёмы создали дополнительные условия для успешной верификации модели в формализованной нотации по дедуктивному методу инструментом Rodin и методу проверки моделей инструментом ProB. Предложенные приёмы могут быть полезны при разработке других формальных моделей управления доступом и их верификации с применением соответствующих инструментов.

ЛИТЕРАТУРА


1. Bell D. E. and LaPadula L.J. Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976.
2. Biba K. J. Integrity Considerations for Secure Computer Systems. Bedford, Mass.: MITRE Corp., 1975.
3. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. 3-е изд., перераб. и доп. М.: Горячая линия — Телеком, 2020. 352 с.
4. Abrial J.-R. Modeling in Event-B: System and Software Engineering. Cambridge University Press, 2010.
5. Abrial J.-R., Butler M., Hallerstede S., et al. Rodin: An open toolset for modelling and reasoning in Event-B // Intern. J. Software Tools for Technology Transfer. 2010. V. 12. No. 6. P. 447-466.
6. Выписка из Требований по безопасности информации, утвержденных приказом ФСТЭК России № 76 от 02.06.2020. https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty/2126- vypiska-iz-trebovanij-po-bezopasnosti-informatsii-utverzhdennykh-prikazom- fstek-rossii-ot-2-iyunya-2020-g-n-76.
7. ГОСТ Р 59453.1-2021 «Защита информации. Формальная модель управления доступом. Ч. 1. Общие положения». М.: Стандартинформ, 2021. 35 с.
8. ГОСТ Р 59453.2-2021 «Защита информации. Формальная модель управления доступом. Ч. 2. Рекомендации по верификация формальной модели управления доступом». М.: Стандартинформ, 2021. 23 с.
9. Операционная система специального назначения Astra Linux Special Edition. https:// astralinux.ru/products/astra-linux-special-edition/
10. Буренин П. В., Девянин П. Н., Лебеденко Е. В. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition: учеб. пособие для вузов / под ред. П. Н. Девянина. 3-е изд., перераб. и доп. М.: Горячая линия — Телеком, 2019. 404 с.
11. Девянин П. Н., Ефремов Д. В., Кулямин В. В. и др. Моделирование и верификация политик безопасности управления доступом в операционных системах. М.: Горячая линия — Телеком, 2019. 214 с.
12. Leuschel M. and Butler M. ProB: an automated analysis toolset for the B method // Int. J. Softw. Tools Technol. Transf. 2008. No. 10(2). P. 185-203.
13. Abrial J.-R. and Hallerstede S. Refinement, decomposition, and instantiation of discrete models: Application to Event-B // Fundamenta Informaticae. 2007. V. 77. Iss. 1-2. P. 1-28.
14. Девянин П. Н., Леонова М. А. Применение подтипов и тотальных функций формального метода Event-B для описания и верификации МРОСЛ ДП-модели // Программная инженерия. 2020. Т. 11. №4. С. 230-241.
15. Девянин П. Н., Леонова М. А. Приёмы по доработке описания модели управления доступом ОССН Astra Linux Special Edition на формализованном языке метода Event-B для обеспечения ее автоматизированной верификации с применением инструментов Rodin и ProB // Прикладная дискретная математика. 2021. № 52. С. 83-96.


УДК 004.75 DOI 10.17223/2226308X/14/28

## МЕТОД ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ НА ОСНОВЕ zk-SNARK[17]

Д. О. Кондырев

[17] Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2019-1613, и лаборатории криптографии JetBrains Research.

Представлен метод обеспечения конфиденциальности данных с возможностью проверки корректности на основе протокола доказательства с нулевым разглашением zk-SNARK. Разработанный метод позволяет создавать алгоритмы на основе zk-SNARK в смарт-контрактах Ethereum, используя высокоуровневые базовые криптографические схемы.

**Ключевые слова:** распределённые системы, блокчейн, доказательство с нулевым разглашением, zk-SNARK, платформа Ethereum.

Среди технических проблем, препятствующих внедрению технологии распределённых реестров, масштабируемость и конфиденциальность являются особенно существенными. В настоящий момент ведутся активные исследования, направленные на поиск решения проблемы конфиденциальности.

Особенно остро эта проблема встаёт в открытых распределённых реестрах (таких, как блокчейн-системы). В таких реестрах все данные сохраняются в открытом виде и доступны всем участникам, что не всегда приемлемо при создании промышленных программных систем. Кроме того, идентификация пользователей происходит по адресу их аккаунта. Таким образом, существует возможность отслеживать действия пользователя путём анализа транзакций, в которых участвует конкретный адрес, и сопоставления адреса аккаунта и пользователя.

В работе предложен метод обеспечения конфиденциальности данных с возможностью проверки корректности. В основе метода лежит криптографический протокол неинтерактивного доказательства знания с нулевым разглашением zk-SNARK [1]. Данная работа развивает результаты, полученные в [2].

В качестве базовой системы для реализации метода выбрана платформа Ethereum — блокчейн-система общего назначения, поддерживающая смарт-контракты.

В zk-SNARK процедура проверки доказательства состоит из операций на эллиптических кривых. В частности, верификатор требует скалярного умножения и сложения на группе эллиптических кривых, а также вычислительно более сложной операции — билинейного спаривания. Ethereum предоставляет реализацию этих операций в виде предварительно скомпилированных контрактов. С их помощью есть возможность реализовать схемы на основе доказательства с нулевым разглашением в коде смарт-контрактов. Используя только встроенные инструменты, приходится оперировать низкоуровневыми примитивами, что не позволяет реализовать сложные алгоритмы.

Для возможности создавать произвольные криптографические схемы, в основе которых лежит zk-SNARK, были разработаны сторонние инструменты, такие, как ZoKrates [3]. Эти решения позволяют реализовать схему в виде кода на довольно высокоуровневом языке, который затем компилируется в код смарт-контрактов. Однако такой подход имеет ряд ограничений, которые не позволяют применять его для схем произвольного размера и сложности.

Для решения проблем существующих подходов предлагается добавить поддержку более высокоуровневых криптографических примитивов, выраженных в виде систем ограничений ранга 1 (R1CS — rank-1 constraint systems), непосредственно в код Ethereum-клиента. Таким образом, мы добавляем механизм задания произвольных схем непосредственно в коде смарт-контрактов. При таком подходе нет необходимости напрямую использовать операции над эллиптическими кривыми, вместо этого новые алгоритмы строятся как комбинация добавленных примитивов. Кроме того, такой подход оказывается более вычислительно эффективным за счёт реализации непосредственно в Ethereum-клиенте.

В качестве базовых примитивов добавлены схемы, реализующие логические операции (AND, OR, NOT) и операции сравнения. Их реализация выполнена на основе libsnark — криптографической библиотеки с открытым исходным кодом, которая

обеспечивает эффективные реализации конструкций zk-SNARK [4].

В Ethereum-клиент добавлены соответствующие операции для возможности вызова этих методов как из кода контрактов, так и вне блокчейна. Для этого модифицирована виртуальная машина Ethereum, куда были добавлены функции создания схемы, генерации доказательства и его верификации.

Схема, описанная разработчиком в коде смарт-контракта, транслируется в набор добавленных примитивов. Далее на их основе формируется система ограничений ранга 1 (R1CS), с которой работают алгоритмы генерации и верификации доказательства zk-SNARK.

Для каждой новой схемы необходима генерация новой пары ключей доказательства и верификации. Их генерация выполняется вне блокчейна, поскольку в алгоритме генерации используется параметр безопасности, зная который, можно создавать некорректные доказательства, которые будут приняты верификатором как корректные.

Таким образом, создана система, которая позволяет разработчикам реализовывать произвольные алгоритмы на основе добавленных базовых схем непосредственно в коде смарт-контрактов. Метод позволяет сократить размер кода смарт-контрактов и, кроме того, оказывается более вычислительно эффективным.

ЛИТЕРАТУРА

1. Ben-Sasson E., Chiesa A., Genkin D., et al. SNARKs for C: Verifying program executions succinctly and in zero knowledge // CRYPTO'2013. LNCS. 2013. V. 8043. P. 90-108.
2. Кондырев Д. О. Разработка метода сокрытия приватных данных для системы тендеров на основе технологии блокчейн // Прикладная дискретная математика. 2020. № 48. С. 63-81.
3. Eberhardt J. and Tai S. ZoKrates — scalable privacy-preserving off-chain computations // IEEE Intern. Conf. Blockchain. Halifax, Canada, 2018. P. 1084-1091.
4. https://github.com/scipr-lab/libsnark — libsnark: a C++ library for zkSNARK proofs.

УДК 004.021 DOI 10.17223/2226308X/14/29

# ДЕОБФУСКАЦИЯ CONTROL FLOW FLATTENING СРЕДСТВАМИ СИМВОЛЬНОГО ИСПОЛНЕНИЯ

В. В. Лебедев

Метод обфускации Control Flow Flattening заменяет в коде программы все условные и безусловные переходы на переход в специальный управляющий блок — диспетчер, который определяет, куда на самом деле будет передано управление в программе. Это делает невозможным исследователю быстро определить, в какой последовательности исполняется код в программе. Предлагается алгоритм восстановления исходной логики программ, обфусцированных этим методом. В основе алгоритма лежит символьное исполнение.

**Ключевые слова:** реверс-инжиниринг, символьное исполнение, обфускация, control flow flattening.

## Введение

Control Flow Flattening [1] — техника обфускации, с помощью которой скрываются ветвления в коде. Вместо последовательного выполнения базовых блоков (линейных участков кода) каждому из них присваивается определённый номер. Вместо прямого перехода на следующий блок номер этого блока записывается в управляющий регистр, затем делается переход в специальный управляющий блок — диспетчер,

который, исходя из номера блока, делает на него переход (рис. 1). В коде на языке Си это выглядит как switch внутри цикла while (рис. 2).

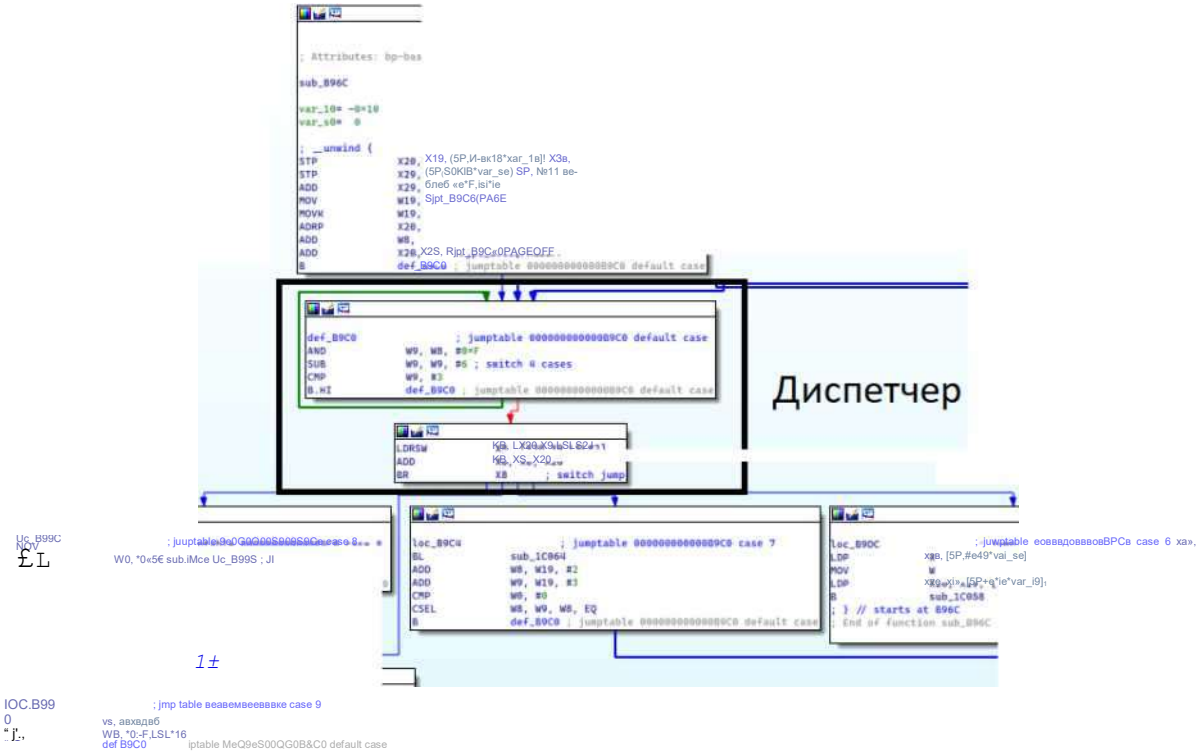



Рис. 1. Граф потока исполнения обфусцированной функции

```
_int64 sub_B96CC)
{
  char v0; // w8

  vG = 7;
  while (13
  {
    switch ( v0 8 0xF )
    {
      case 6:
        return sub_lC058(lLL);
      case 7:
        if ( (unsigned int)sub_lC064() )
          w9 = 8;
        else
          w9 = 9;
        continue;
      case 8:
        sub_lD0C0(94LL);
        goto LABEL_2;
      case 9:
LABEL_2:
        vG = 6;
        break;
      default:
        continue;
    I
  }
```

Рис. 2. Декомпилированная обфусцированная функция

## 1. Алгоритм деобфускации Control Flow Flattening

За основу алгоритма деобфускации взята концепция символьного исполнения [2]. Оно применяется для построения множества $Jumps$ – его элементами являются кортежи вида $(a_i, x_i, b_i)$, где $a_i$ – адрес, откуда был совершён переход на диспетчер; $x_i$ – значение управляющего регистра, при котором диспетчер перейдёт на адрес $b_i$. Затем множество Jumps преобразуется в набор патчей – информацию об адресах, инструкции по которым нужно заменить в исполняемом файле (алгоритм 1).

**Алгоритм 1.** Деобфускация Control Flow Flattening

**Вход:** обфусцированный исполняемый файл вместе с адресом функции, которую необходимо деобфусцировать; функция обнаружения диспетчера $f: State \wedge \wedge (s,e,c)$, где $State$ — символьное состояние; $s$ – адрес первой инструкции диспетчера, $e$ – адрес последней инструкции диспетчера, $c$ – название управляющего регистра. Функция $f$ определена частично для некоторых значений $State$.

**Выход:** Набор патчей, упрощающих исполняемый файл. Может содержать адреса, которых изначально нет в программе, для них нужно создать новый исполняемый сегмент.

1: $Jumps = 0$.

2: Символьно исполнять программу с заданного адреса. При исполнении игнорировать вызовы других функций. Если символьные состояния, возможные для исполнения, отсутствуют, перейти на п. 8.

3: Если обнаружен диспетчер (функция $f$ определена для текущего состояния), получить: адрес $a$, с которого был совершён переход на него, и текущее символьное состояние (регистры и память) $State_0$ вместе с множеством потенциальных значений $X$ управляющего регистра (УР). Так как исполнение символьное, УР в $State_0$ содержит некоторое символьное выражение, которое может быть конкретизировано в множество $X$ допустимых значений УР.

4: Для каждого $x_i \in X$ изменить УР в $State_0$ на $x_i$, получив тем самым $State_{0i}$.

5: Для каждого $State_{0i}$ продолжать символьное исполнение до тех пор, пока не дойдём до адреса $b_i$, не относящегося к диспетчеру. Должно быть выполнено условие: для любого $State_{0i}$ существует единственный $b_i$ (так как исполнение символьное, возможных $b_i$ может быть больше одного, но $b_i$ должен зависеть только от значения УР, а оно зафиксировано на шаге 4, поэтому нарушение данного условия свидетельствует о нарушении ограничений, накладываемых на деобфусцируемый код).

6: Добавить все возможные варианты $(a, x_i, b_i)$ к множеству $Jumps$.

7: Перейти на п. 2.

8: // Символьное исполнение закончено, имеется множество $Jumps$, содержащее все возможные переходы для всех обнаруженных диспетчеров.

9: Сгенерировать патчи для каждого уникального $a$, такого, что $(a, x_i, b_i) \in Jumps$: если для заданного $a$ существует единственная пара $(x_i, b_i)$, заменить инструкцию по адресу $a$ на безусловный переход по адресу $b_0$. Если пар $(x_i, b_i)$ несколько, создать новый исполняемый сегмент программы и заменить инструкцию по адресу $a$ на переход в него. Сгенерировать в новом сегменте логику сравнения УР с

каждым $x_i$ и делать переход на $b_i$, если и только если УР равен $x_i$.

## 2. Накладываемые ограничения на код исполняемого файла

1) Необходимые для работы диспетчера данные находятся либо в read-only памяти, либо инициализируются в той же функции, в которой находится диспетчер.
2) Значения управляющих регистров не зависят от функций, вызываемых внутри деобфусцируемой функции, а также от других функций, не связанных с ней.
3) В каждом диспетчере адрес перехода должен зависеть от управляющего регистра, и только от него.
4) Диспетчер представляет собой непрерывный участок кода.
5) Если в исполняемом файле есть «мёртвый код», который в действительности никогда не будет исполнен, он будет деобфусцирован, как и обычный код. Его обнаружение и удаление выходит за рамки данной работы.

## 3. Похожие работы

1) Automatic Deobfuscation of Android Native Binary Code [3] — нацелен конкретно на обфускатор OLLVM. Предлагаемый подход более общий и не делает никаких предположений относительно структуры обфусцированной функции.
2) SATURN [4] — не делает совсем никаких предположений относительно кода, вместо этого пытается оптимизировать программу целиком и рекомпилировать её. Такой подход может вносить нежелательные изменения в участки кода программы, свободные от обфускации.

## 4. Преимущества данного алгоритма

1) Частичное символьное исполнение — не нужно исполнять код целиком. За один раз исполняется только одна функция, даже если она содержит вызовы других функций. Такой подход позволяет работать с очень объёмными программами, на полное символьное исполнение которых требуется слишком много времени и ресурсов.
2) Не делает никаких предположений относительно структуры функции, в отличие от деобфускаторов, которые работают с OLLVM. Все предположения делаются только относительно диспетчеров.

## 5. Практическая реализация

Алгоритм 1 реализован на языке Python на основе фреймворка для символьного исполнения angr [5]. Реализация поддерживает исполняемые файлы для архитектуры AArch64. Тесты проводились для библиотек Android-приложений, в которых наиболее актуально частичное символьное исполнение, так как в коде присутствует большое количество вызовов Java Native Interface, символьное исполнение которых является проблемой. Наибольшую трудность представляло автоматическое обнаружение диспетчеров и обработка случаев с каскадным расположением диспетчеров, при котором один диспетчер делает переход на другой.

ЛИТЕРАТУРА

1. Wang C., Hill J., Knight J., and Davidson J. Software Tamper Resistance: Obstructing Static Analysis of Programs. Technical Report. University of Virginia, USA, 2000.
2. Boyer R. S., Elspas B., and Levitt K. N. SELECT — a formal system for testing and debugging programs by symbolic execution // Proc. Intern. Conf. Reliable Software. Los Angeles, California: Association for Computing Machinery, 1975. P. 234-245.
3. Kan Z., Wang H., Wu L., et al. Automated Deobfuscation of Android Native Binary Code. 2020. https://arxiv.org/pdf/1907.06828.pdf.

4. Peter Garba, Matteo Favaro SATURN — software deobfuscation framework based on LLVM // 3rd Intern. Workshop Software Protection, Nov 2019, London. https://arxiv.org/abs/1909.01752.
5. Shoshitaishvili Y., Wang R., Salls C., et al. SOK: (State of) The art of war: Offensive techniques in binary analysis // IEEE Symp. Security Privacy. 2016. P. 138-157.

УДК 004.056.5 DOI 10.17223/2226308X/14/30

# ПРИМЕНЕНИЕ РАСШИРЕНИЙ АРХИТЕКТУРЫ X86 В ЗАЩИТЕ ПРОГРАММНОГО КОДА

Р. К. Лебедев, И. А. Корякин

Предложен новый подход к защите программного кода от таких инструментов обратной разработки, как декомпиляторы и инструменты символьного исполнения программ. В рамках данного подхода разработан метод запутывания констант, основанный на использовании набора расширений AES-NI процессорной архитектуры x86. Метод реализован для компилятора Clang при помощи инфраструктуры LLVM и протестирован на таких инструментах обратной разработки, как IDA, Ghidra и angr.

**Ключевые слова:** защита программного кода, обратная разработка, декомпиляция, символьное исполнение, архитектура x86.

На сегодняшний день существует множество инструментов, облегчающих обратную разработку программного обеспечения, что увеличивает риски разработчиков, связанные с нарушением авторского права. Обратная разработка применяется для обхода защиты от копирования, заимствования программного кода конкурентами, поиска уязвимостей и многого другого.

К наиболее популярным инструментам обратной разработки относятся декомпиляторы, отладчики и инструменты символьного исполнения программ. В то время как для противодействия отладке существует множество способов, так как отладка ощутимо влияет на процесс выполнения программы, противодействие декомпиляторам и инструментам символьного исполнения не так распространено.

Для противодействия декомпиляторам обычно используются общие методы обфускации [1], не предотвращающие декомпиляцию, но делающие вывод декомпилятора длинным и менее удобным для прочтения аналитиком. В то же время декомпилированный код может оставаться полностью корректным, что позволяет злоумышленнику использовать его даже без понимания принципа действия.

Против инструментов символьного исполнения существуют специфические подходы, использующие проблему экспоненциального взрыва и односторонние функции [2—4]. Однако они влекут дополнительные накладные расходы, связанные с выполнением большого числа ветвлений или односторонних функций, что может делать их неприменимыми для защиты кода, чувствительного к размеру и производительности.

В данной работе предложен новый подход, не оказывающий значимого влияния на производительность программ и обеспечивающий полную неработоспособность распространённых декомпиляторов и инструментов символьного исполнения. Его основой является использование редких процессорных инструкций, поддержка которых может быть не реализована в инструментах обратной разработки.

Процессорная архитектура x86 имеет более тысячи различных инструкций [5]. В обычных программах используется лишь малая часть этого набора, поэтому инстру-

менты обратной разработки вполне могут поддерживать не все инструкции. Соответственно, если искусственно ввести такие инструкции в программу, это может привести к их неработоспособности.

Рассмотрено влияние на эти инструменты инструкций из набора расширений AES-NI, который используется для аппаратного ускорения операций шифрования AES и поддерживается всеми относительно современными процессорами как в 64-битной, так и в 32-битной версии архитектуры x86 [6]. Одной из основных инструкций этого набора расширений является инструкция AESENC, реализующая один раунд шифрования AES:

$$\mathrm{AESENC}(\mathrm{data}, \mathrm{key}) = \mathrm{MixColumns}(\mathrm{ShiftRows}(\mathrm{SubBytes}(\mathrm{data}))) \oplus \mathrm{key}.$$

Здесь SubBytes, ShiftRows и MixColumns — соответствующие операции шифрования AES; data — шифруемый блок; key — раундовый ключ.

Данная инструкция нечасто используется в программном обеспечении (за исключением библиотек для реализации шифрования), поэтому инструменты обратной разработки могут обрабатывать её некорректно, что останется незамеченным в большинстве сценариев использования.

Для проверки этой гипотезы реализовано простое преобразование — запутывание констант в коде. Оно осуществляется путём замены исходного значения константы $\mathbf{x}$ выражением времени исполнения $\mathbf{x}_{\mathrm{obf}}$ следующего вида:

$$\mathbf{x}_{\mathrm{obf}} = \mathrm{AESENC}(\mathbf{x}^0, 0).$$

Это выражение будет подсчитываться всякий раз, когда программе понадобится значение $\mathbf{x}$. В свою очередь, $\mathbf{x}^0$ рассчитывается во время компиляции по следующей формуле:

$$\mathbf{x}^0 = \mathrm{AESDEC}(\mathbf{x}, 0).$$

Здесь AESDEC — операция, обратная AESENC.

Преобразование реализовано на уровне промежуточного представления LLVM [7], что обеспечило возможность проверить эффективность метода на реальных программах, например написанных на языке Си (при помощи компилятора Clang).

Для проверки эффективности метода использовалась простая программа на языке Си, имитирующая проверку лицензионного ключа через сравнение ввода с константой (листинг 1), а также декомпиляторы IDA и Ghidra и инструмент символьного исполнения angr [8-10]. В результате ни IDA, ни Ghidra не смогли во время декомпиляции восстановить изначальное значение константы, причём в случае IDA операция сравнения вовсе исчезла, что ещё более затрудняет анализ. Инструмент символьного исполнения angr также не смог выполнить приложенную программу, сообщив об отсутствии поддержки инструкции AESENC.

```
1 #include <stdio .h>
2 int main () {
3 int k;
4 printf (" Please    enter secret key :") ;
5 scanf ("%d" , &k)    ;
6 if (k == 1337) printf (" Correct license key\n") ;
7 else printf ("Wrong license      key\n") ;
8}
```

Листинг 1. Тестовая программа

Таким образом, предложенный метод оказался эффективен против популярных инструментов обратной разработки. Полученные результаты могут быть в дальнейшем использованы для замены всех инструкций программы на альтернативные конструкции, использующие процессорные расширения, что может сделать защищаемую программу недоступной для декомпиляции и символьного исполнения до тех пор, пока в соответствующих инструментах не будет реализована полная поддержка всех расширений.

ЛИТЕРАТУРА

1. Junod P., Rinaldini J., Wehrli J., and Michielin J. Obfuscator-LLVM — software protection for the masses // 2015 IEEE/ACM 1st Intern. Workshop Software Protection. 2015. P. 3-9.
2. Wang Z., Ming J., Jia C., and Gao D. Linear obfuscation to combat symbolic execution // Proc. European Symp. Research Computer Security. 2011. P. 210-226.
3. Seto T., Monden A., Yucel Z., and Kanzaki Y. On preventing symbolic execution attacks by low cost obfuscation // 20th IEEE/ACIS Intern. Conf. Software Eng., Artif. Intelligence, Networking and Parallel/Distributed Comput. (SNPD). 2019. P. 495-500
4. Лебедев Р. К. Автоматическая генерация хэш-функций для обфускации программного кода // Прикладная дискретная математика. 2020. № 50. С. 102-117
5. https://intelxed.github.io/ — Intel XED. 2019.
6. https://software.intel.com/content/www/us/en/develop/articles/intel-advanced- encryption-standard-instructions-aes-ni.html — Intel® Advanced Encryption Standard Instructions (AES-NI). 2012.
7. Lattner C. and Adve V. LLVM: A compilation framework for lifelong program analysis & transformation // Intern. Symp. Code Generation and Optimization. 2004. P. 75-86
8. https://www.hex-rays.com/ida-pro/ — IDA Pro. 2021.
9. https://github.com/NationalSecurityAgency/ghidra — Ghidra Software Reverse Engineering Framework. 2021.
10. Shoshitaishvili Y., Wang R., Salls C., et al. SOK: (State of) The art of war: Offensive techniques in binary analysis // IEEE Symp. Security Privacy. 2016. P. 138-157.

УДК 004.052 DOI 10.17223/2226308X/14/31

# ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПОИСКА УЯЗВИМОСТЕЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ФАЗЗИНГА В ВИРТУАЛЬНЫХ МАШИНАХ JAVASCRIPT

М. С. Недяк

Описано расширение метода фаззинга виртуальных машин JavaScript, использующего мутации абстрактного синтаксического дерева. Рассматриваются результаты работы алгоритма, реализующего предложенное расширение.

**Ключевые слова:** фаззинг, JavaScript, автоматизированный поиск уязвимостей.

## Введение

Существуют различные подходы к фаззингу виртуальных машин JavaScript. Каждый из них имеет некоторые недостатки: малое покрытие кода, малое количество состояний программы, затронутых в течение фаззинга. Кроме того, сам процесс фаззин- га виртуальных машин требует большое количество вычислительных ресурсов и процессорного времени. Основная причина этих недостатков заключается в том, что виртуальная машина JavaScript требует на вход высокоструктурированный вход — программы, правильные синтаксически и семантически. Большинство текстов программ JavaScript, сгенерированных фаззером, не проходят дальше проверки

синтаксиса. Из-за этого увеличивается количество запусков виртуальной машины JavaScript, которые не дают новых результатов.

В работе предложено расширение метода фаззинга с генерацией абстрактного синтаксического дерева. В результате при проведении экспериментов:

1) значительно увеличена скорость нахождения новых путей в целевой программе;
2) увеличено общее количество состояний программы, которые проходит очередь фаззера.

## 1. Фаззинг с мутацией абстрактного синтаксического дерева

Рассмотрим принцип работы фаззера с мутацией абстрактного синтаксического дерева (рис. 1).

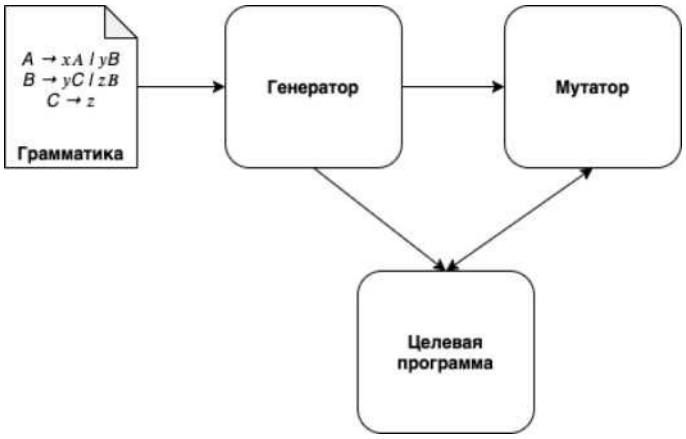



Рис. 1. Схема работы фаззера с мутацией абстрактного синтаксического дерева

Фаззер с мутацией абстрактного синтаксического дерева является комбинированным, то есть это фаззер, где используются и генерационные, и мутационные операции над входными данными программы. Объекты, которые отвечают за генерационные и мутационные операции, называются генератором и мутатором соответственно.

На вход генератору задаются правила грамматики, по которым он генерирует деревья, применяя эти правила в случайном порядке. Примеры фаззеров, которые используют данный подход: Domato [1], Dharma [2], Nautilus [3].

Такой подход генерирует синтаксически правильные тесты, однако их семантическая корректность не гарантируется. Такие тесты обычно не проходят дальше первых компонент виртуальной машины JavaScript — парсера или байт-кода компилятора.

Под семантической неправильностью подразумеваются следующие случаи:

1) При генерации дерева не контролируется тип контекста, например ключевое слово break может появляться только в конструкции switch-case или циклах (листинг 1).

```
1 function test () {
2       var d = 10 ;
3       break ;
4 }
```

Листинг 1. Семантическая неправильность. Пример 1

2) При генерации дерева не контролируются области видимости объявленных переменных. В примере (листинг 2) переменная d не видна вне функции test.

```
1 function test () {
2 var d = 10 ;
3}
4 d++;
```

Листинг 2. Семантическая неправильность. Пример 2

3) При генерации дерева не контролируются типы объявленных переменных; в третьем примере (листинг 3) происходит обращение к переменной d, как к массиву, в то время как она является числовой переменной.

```
1 function test () {
2 var d = 10 ;
3 d[i] = 42;
4}
```

Листинг 3. Семантическая неправильность. Пример 3

Во всех рассмотренных случаях выполнение кода остановится либо на этапе компиляции байт-кода, либо на этапе интерпретации байт-кода программы JavaScript. Где именно произойдет остановка, зависит от реализации виртуальной машины JavaScript.

## 2. Расширение метода фаззинга с мутацией абстрактного синтаксического дерева

### 2.1. Семантический анализ

Предлагается добавить семантический анализ при генерации и мутации абстрактных синтаксических деревьев. Семантический анализ включает в себя:

1) Контроль объявленных переменных. При генерации мутируемого дерева предлагается добавить контроль контекста.
   Контекст — множество названий переменных, классов, функций, которые объявлены и доступны для текущего узла.
2) Контроль типа контекста генерируемого дерева. Это значит, что мутация узла, которая содержит неприменимое в текущем контексте ключевое слово, невозможна.

### 2.2. Способ задания грамматики JavaScript

Предлагается задавать грамматику с помощью базы тестов — набора файлов, содержащих исходный код программ на языке JavaScript. Этими программами могут быть:

1) тесты функциональностей;
2) тесты найденных ошибок;
3) демонстрации найденных уязвимостей.

Так как любую программу на JavaScript можно представить абстрактным синтаксическим деревом, можно считать, что база тестов — это множество абстрактных синтаксических деревьев.

Будем говорить, что грамматика $A$ меньше или равна грамматике $B$, если мощность языка, порождаемого грамматикой $A$, меньше или равна мощности языка, порождаемого грамматикой $B$.

Из теории формальных грамматик [4] известно, что для всякого множества абстрактных синтаксических деревьев существует такая грамматика, что язык, порождённый ею, включает множество этих деревьев. При этом грамматика,

образованная множеством деревьев, меньше или равна грамматике всего языка. Другими словами, используя базу тестов, фаззер использует грамматику, построенную по множеству тестов; эта грамматика меньше или равна грамматике языка JavaScript.

С теоретической точки зрения база тестов имеет явные недостатки, потому что не всегда порождает грамматику, равную грамматике всего языка JavaScript. С практической точки зрения задание грамматики базой тестов имеет следующие преимущества:

1) Широта грамматики. В силу специфики реализаций виртуальных машин JavaScript, анализ применимости входной программы к грамматике языка происходит на поздних этапах исполнения, где грамматика задана неявно. Поэтому пользователям других фаззеров приходится вручную анализировать стандарты и примеры работы со стандартными модулями, чтобы включить их в свою грамматику. Так как правила грамматики задаются человеком, велика вероятность, что какие-то конструкции не будут генерироваться этими правилами.
2) Удобство задания грамматики. Тексты программ JavaScript сами по себе задают грамматику, в то время как с ручным заданием грамматики нужно изучать стандарт JavaScript и вручную прописывать правила. Например, при добавлении нового модуля JavaScript в грамматику не нужно анализировать работу с этим модулем, а достаточно добавить набор тестов для него.

## 3. Алгоритм

### Замена узла новым тестом из базы тестов

Метод замены узла в мутируемом дереве происходит по следующим шагам:

**1.** Запрос из базы тестов узла с таким же типом. В дереве-источнике находится узел, который имеет такой же тип, как заменяемый узел.

**2.** Анализ применимости узла в текущем контексте. Новый узел применим только тогда, когда он не содержит ключевых слов, которые неприменимы в текущем контексте.

**3.** Подготовка вставки узла в дерево:

а) замена идентификаторов переменных, если они:

— не объявлены в текущем контексте;

— не объявлены в новой ветке;

— не являются объектом runtime виртуальной машины JavaScript;

б) включение веток-функций, веток-классов в глобальный контекст из дерева-источника, если новая ветка вызывает функцию или создаёт класс, при этом они:

— не объявлены в мутируемом дереве;

— не являются объектом runtime виртуальной машины JavaScript.

Новые ветки-функции и ветки-классы также должны пройти подготовку вставки.

### Замена узла с обратной связью

Данная мутация является вариацией описанной — замены узла новым тестом из базы тестов, где вместо базы тестов используется очередь фаззера. Для того чтобы определить, что такое очередь фаззера, разберёмся, что такое путь.

Любую программу можно представить ориентированным графом, вершины которого соответствуют прямолинейному участку кода, а дуги — инструкциям перехода.

Такое представление программы называют графом потока управления — это множество всех возможных путей исполнения программы.

Путь — это множество вершин графа потока управления, которые были выполнены при запуске программы. Если тест выполнил новый путь, то он помещается в очередь фаззера.

Таким образом, очередь фаззера — это множество тестов, которые выполняют разные пути в программе.

## 4. Экспериментальная часть

Для сравнения эффективности работы фаззеров обычно говорят о метриках покрытия кода. Метрика покрытия кода может задаваться по-разному: это может быть количество выполненных строк кода или количество найденных путей в целевой программе.

В данной работе для сравнения эффективности используется скорость нахождения новых путей, определяемая как количество путей в отношении к количеству запусков. Эта метрика показывает, как часто достигаются новые состояния программы в процессе фаззинга.

Задача фаззинга — это нахождение аварийных завершений программы, некоторые из которых могут сигнализировать о наличии в ней уязвимости. Уязвимости программы содержатся не только в строках кода, но и в состояниях программы, которые могут привести к этой уязвимости. Поэтому используем ещё одну метрику — количество путей, сгенерированных фаззером.

Для сравнения эффективности разработанного фаззера был выбран фаззер Nautilus, который является фаззером с классическим подходом с мутацией абстрактного синтаксического дерева. Идея мутации с обратной связью была взята именно из этого фаззера, поэтому при сравнении с ним можно оценить, как предложенные улучшения алгоритма мутаций повлияли на эффективность подхода.

### 4.1. Фаззинг виртуальной машины SpiderMonkey

На рис. 2 представлен график скорости генерации новых путей при фаззинге виртуальной машины SpiderMonkey [5]. Можно заметить, что с количеством запусков скорость генерации новых путей Nautilus заметно ниже, чем у DFuzzer, реализующего предложенное расширение. При этом количество путей, сгенерированных за равное количество запусков, у разработанного фаззера больше.

Если посмотреть на график в приближении, то можно видеть, что в начале работы скорость генерации новых путей у фаззера Nautilus выше. Это обусловлено тем, что Nautilus использует генерационные методы для модифицирования входных данных целевой программы. Фаззер DFuzzer является мутационным, это значит, что на его входе задано начальное дерево, с которого он начинает мутации, в то время как генерационный фаззер сразу генерирует все возможные деревья по заданной грамматике.

В ходе экспериментов аварийных завершений виртуальной машины JavaScript SpiderMonkey не выявлено.

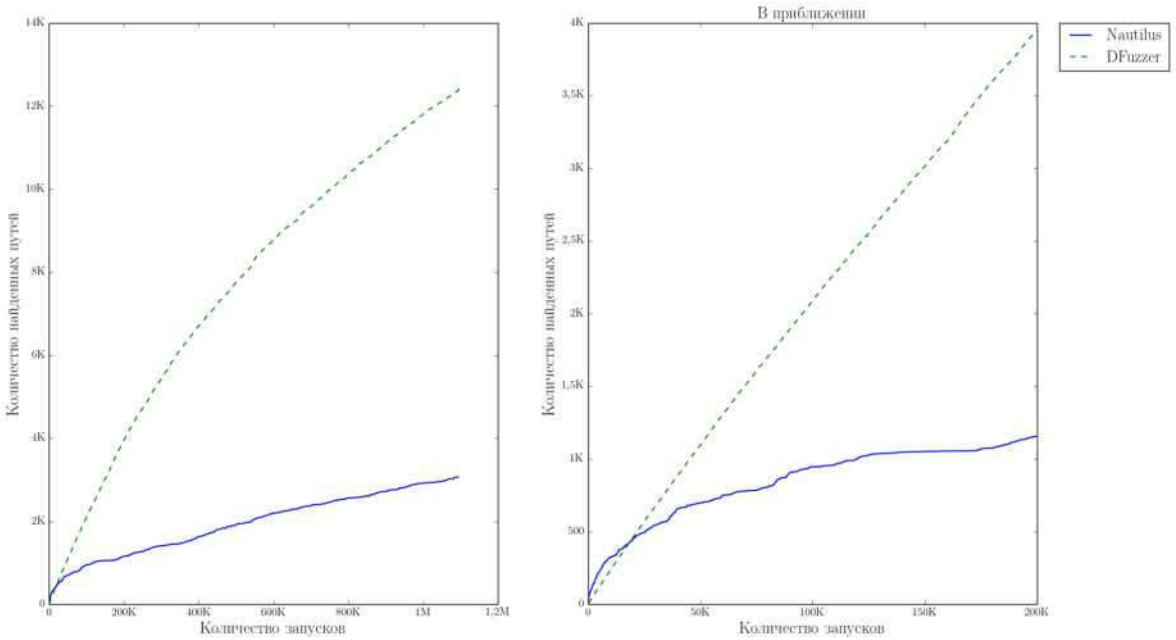



Рис. 2. Скорость генерации новых путей при фаззинге SpiderMonkey

4.2. Фаззинг виртуальной машины ChakraCore

При фаззинге виртуальной машины ChakraCore [6] (рис. 3) можно наблюдать схожую картину, что и при фаззинге виртуальной машны SpiderMonkey.

В ходе тестирования виртуальной машины ChakraCore выявлены аварийные завершения программы. Они будут проанализированы на наличие уязвимостей, и информация о них будет передана производителю.

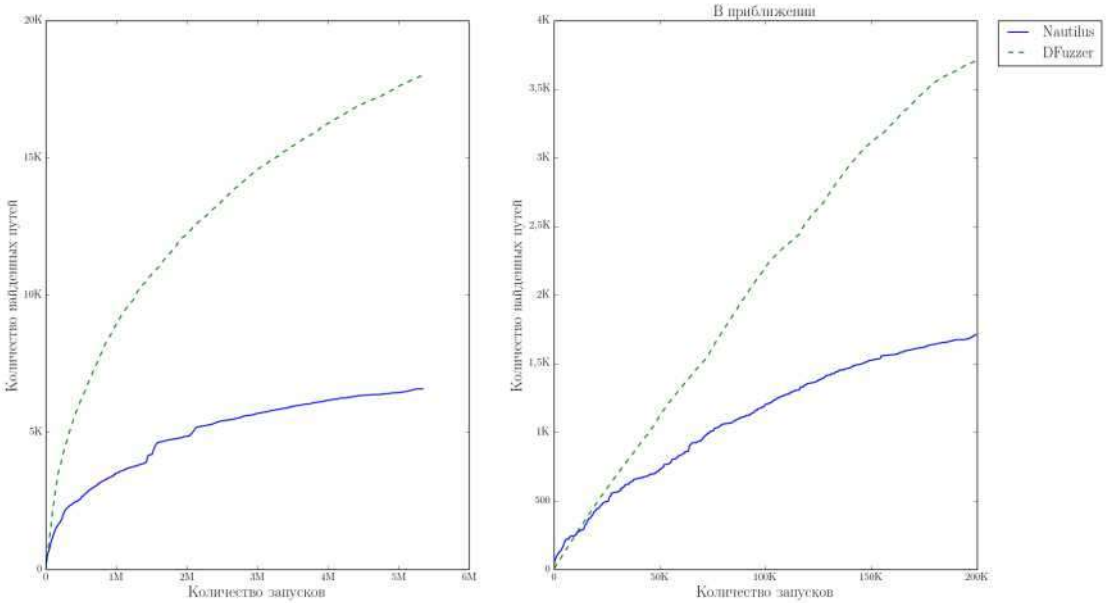



Рис. 3. Скорость генерации новых путей при фаззинге ChakraCore

## Заключение

Предложенное расширение является развитием современных подходов фаззинга

виртуальных машин JavaScript. В результате удалось существенно повысить эффективность тестирования на уязвимости, расширив метод фаззинга, использующего мутации абстрактных синтаксических деревьев, и значительно увеличить скорость обнаружения новых путей исполнения в тестируемой программе. Исходный код реализованного фаззера доступен для изучения и использования на портале github [7].

ЛИТЕРАТУРА

1. Domato Fuzzer. https://github.com/googleprojectzero/domato/blob/master/README. md. 2021.
2. Dharma Fuzzer. https://github.com/MozillaSecurity/dharma/blob/master/README.md. 2021.
3. Aschermann C. NAUTILUS: Fishing for Deep Bugs with Grammars. https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2018/12/17/NDSS19-Nautilus. pdf. 2021.
4. Aho A. V., Lam M. S., Sethi R., and Ullman J. D. Compilers: Principles, Techniques, and Tools. Addison Wesley, 2007.
5. Виртуальная машина JavaScript SpiderMonkey. https://developer.mozilla.org/en-US/ docs/Mozilla/Projects/SpiderMonkey. 2021.
6. Виртуальная машина JavaScript ChakraCore. https://github.com/chakra-core/ChakraCore. 2021.
7. https://github.com/MashaSamoylova/DFuzzer/blob/master/README.md. 2021.

УДК 004.056 DOI 10.17223/2226308X/14/32

# РАСШИРЕНИЕ И ИССЛЕДОВАНИЕ МЕТОДА СОКРЫТИЯ ИНФОРМАЦИИ DEEP STEGANOGRAPHY

А. А. Николаев

Программно реализован метод сокрытия информации с помощью нейронных сетей Deep Steganography. Предложено и реализовано расширение метода в виде добавления дополнительных скрытых слоёв в закодированное изображение для возможности передачи большего объёма информации. Исследованы качества и свойства предложенного метода сокрытия информации.

**Ключевые слова:** сокрытие информации, скрытые каналы, нейронные сети.

## 1. Сокрытие информации с помощью нейронных сетей

В настоящее время известны два основных метода сокрытия информации с помощью нейронных сетей: Deep Steganography [1] и HiDDeN [2]. Основным их различием является возможный тип передаваемых данных: в случае Deep Steganography в качестве секретного сообщения выступает изображение; в случае HiDDeN — любая битовая последовательность.

В работе исследуется расширение метода сокрытия информации с помощью нейронных сетей Deep Steganography.

Метод Deep Steganography впервые описан в работе [1]. Схема сокрытия и раскрытия секретного изображения состоит из трёх нейронных сетей, которые обучаются одновременно как единая сеть, но работают независимо друг от друга и могут быть разделены между отправителем и получателем. Данный метод позволяет

скрывать секретное изображение внутри изображения-контейнера с помощью подготовительной (prep network) и скрывающей (hiding network) сетей, которые находятся на стороне отправителя, и раскрывать секретное изображение на стороне получателя с помощью раскрывающей (reveal network) сети.

## 2. Расширение метода Deep Steganography

В результате реализации метода Deep Steganography разработано и предложено расширение метода в виде добавления дополнительных скрытых слоёв в закодированное изображение.

Основной принцип работы и роль сетей аналогичны оригинальному методу Deep Steganography, за исключением того, что вместо одной подготовительной и одной раскрывающей сети используются $n$ подготовительных и $n$ раскрывающих сетей — таким образом, модифицируется архитектура самой сети. Каждая из сетей позволяет закодировать в изображении-контейнере и раскрыть $n$ изображений соответственно. Число $n$ определяется допустимым уровнем искажений в контейнере и потребностью в необходимом числе секретных изображений, которое требуется закодировать и передать — при сокрытии большего числа сообщений в виде изображений исходное изображение- контейнер подвергается большим искажениям, чем при использовании меньшего числа сообщений.

Скрывающая сеть принимает на вход одно изображение-обложку и $n$-секретных изображений. Раскрывающие сети способны раскодировать набор секретных изображений (каждая сеть раскодирует свой слой, содержащий секрет).

Данное расширение позволяет передать больший объём скрытой информации за один сеанс передачи (при использовании одного медиаконтейнера) по сравнению с классическим методом.

В качестве основной библиотеки для разработки была использована TensorFlow. Для подготовки и тренировки модели в качестве тренировочного набора данных был выбран датасет Tiny ImageNet, который является уменьшенной версией дата- сета ImageNet. Датасет Tiny ImageNet содержит 200 категорий изображений, по 500 изображений размера 64x64 пикселя в каждой. Суммарно Tiny ImageNet содержит 100 000 изображений.

В качестве основной метрики оценки качества восстановления исходных изображений был выбран индекс структурного сходства (индекс SSIM, Structural Similarity Index Measure). Данный индекс позволяет определить структурную схожесть между двумя изображениями методом полного сопоставления. Значение, близкое к 1,0 (или 100 % в интерпретации), достигается только при полной аутентичности двух образцов.

Для анализа было выбрано 10 случайных наборов изображений из датасета Tiny ImageNet, каждый из которых включает в себя изображение-обложку и изображение-контейнер, а также $n$ изображений, подготовленных для сокрытия в контейнере. В экспериментах $n = 3$, что является оптимальным для сокрытия и передачи данных. Проведён полный процесс сокрытия и раскрытия изображений в каждом из наборов, данные представлены в таблице, где $I_0$ — индекс схожести обложки и контейнера; $I_k$ — индекс схожести секрета и восстановленного изображения для слоя $k$, $k = 1, 2, 3$; наивысшее значение индекса выделено полужирным шрифтом.

Таким образом, предложенное расширение позволяет восстановить секретное изображение в среднем с точностью 82 % для ближайшего к обложке слоя изображения

(третьего) и 56 % для наиболее глубоко скрытого слоя (первого).

| № п/п | $I_0$, % | $I_1$, % | $I_2$, % | $I_3$, % |
|---|---|---|---|---|
| 1 | 70 | 56 | 81 | 81 |
| 2 | 70 | 71 | 71 | 76 |
| 3 | 59 | 55 | 85 | 88 |
| 4 | 58 | 49 | 80 | 85 |
| 5 | 64 | 45 | 68 | 80 |
| 6 | 78 | 49 | 72 | 86 |
| 7 | 72 | 63 | 75 | 82 |
| 8 | 63 | 52 | 68 | 81 |
| 9 | 74 | 68 | 83 | 82 |
| 10 | 63 | 54 | 82 | 85 |
| Среднее | 67 | 56 | 76 | 82 |

Для оценки качества сокрытия данных в контейнере использован также программный инструмент StegSolve, позволяющий обнаружить артефакты и скрытую информацию в медиаконтейнерах. В результате анализа изображения-контейнера с помощью StegSolve восстановить скрытые изображения или обнаружить артефакты без раскрывающей сети не удалось, что свидетельствует о том, что данный метод имеет высокую надёжность передачи сообщений без возможности восстановления скрытых изображений участником, не имеющим доступа к раскрывающей сети.

ЛИТЕРАТУРА

1. Baluja S. Hiding Images in Plain Sight: Deep Steganography // Adv. Neural Inform. Processing Systems. 2017. No. 30. P. 1-11.
2. Zhu J., Kaplan R., Johnson J., and Fei-Fei L. HiDDeN: Hiding Data With Deep Networks. 2018. https://arxiv.org/abs/1807.09937.

УДК 519.23:519.6: 004.052 DOI 10.17223/2226308X/14/33

# АДАПТАЦИЯ МЕТОДА РОЗЕНБЛАТТА — ПАРЗЕНА ДЛЯ ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ

В. С. Никулин

Отсутствие исходной информации о законе распределения случайных величин и их реализация в момент, близкий к началу наблюдения, а также наличие цензурированных данных вызывает необходимость адаптации непараметрического метода Розенблатта — Парзена. Для компенсации смещения и устранения нарушения условия нормировки рассмотрен метод зеркального отображения исходных данных. При построении плотности распределения случайных величин предлагается учитывать цензурированные данные. Проведённая оценка точности показывает уменьшение ошибки при аппроксимации эмпирической плотности распределения адаптированным методом Розенблатта — Парзена. На примере экспериментальной оценки показателей надёжности вычислительной системы продемонстрирована практическая реализация адаптированного метода Розенблатта — Парзена. Построение плотности и функции распределения времени до отказа позволяет рассчитать основные показатели безотказности объекта: интенсивность отказов, вероятность безотказной работы, среднее время наработки на отказ.

**Ключевые слова:** экспериментальный анализ надёжности, малые выборки, вычислительные системы, метод Розенблатта — Парзена.

Экспериментальная оценка показателей надёжности сводится к построению плотности распределения времени отказа. Применение параметрических методов анализа статистической информации ограничено требованием необходимости знания закона распределения наблюдаемых случайных величин. Например, в теории надёжности показано, что наработки до отказа однотипных радиоэлектронных элементов подчиняются экспоненциальному закону, при этом характер отказов предполагается внезапным, а сумма случайных величин, описываемых экспоненциальным распределением, подчиняется гамма-закону [1]. Другие факторы, обосновывающие применение того или иного семейства распределений, отсутствуют. Решением проблемы отсутствия информации о виде закона распределения наблюдаемых случайных величин является использование непараметрических методов.

Среди непараметрических методов построения плотности распределения широкое распространение находят гистограммные, проекционные, ядерные и ортогональные оценки. Методы построения этих оценок известны и хорошо изучены для случаев, когда в отношении результатов наблюдений выполняется предположение, что в каждом испытании реализуется наблюдаемый признак. Например, если речь идёт об обработке статистических данных с целью определения характеристик надёжности, то в качестве обрабатываемой информации используются полные наработки объектов до отказа.

Однако на практике информация от функционирующих объектов имеет ряд ограничений. Например, в момент ввода объекта в эксплуатацию возникают отказы, связанные с отладкой работы оборудования. Данный процесс вызывает проблему смещения плотности распределения. Непосредственно при эксплуатации объектов стараются не допускать отказов за счёт предупредительных профилактических мероприятий, в связи с этим возникает проблема малых выборок по полным наработкам на отказ. В процессе анализа надёжности приходится сталкиваться с ситуациями, когда определённая часть объектов или систем не отказывает за период наблюдения, а другая часть отказывает, но моменты отказов неизвестны. Такой процесс называется цензурированием данных. Учитывая описанные проблемы, применение непараметрических методов в явном виде не представляется возможным для задачи экспериментальной оценки показателей надёжности.

В данной работе предлагается адаптация непараметрического метода Розенблатта — Парзена. Этот метод обладает рядом преимуществ относительно метода построения гистограмм, проекционных и экспоненциальных оценок [2]. Его достоинством является положительная определённость (при выборе неотрицательного ядра), что не выполняется для оценок на основе ортогональных разложений. Важным моментом является наличие теоретических наработок по учёту малых выборок и цензурированных данных [3, 4]. В общем виде метод Розенблатта — Парзена применяется для построения плотности распределения $f(t)$ по полным наработкам на отказ [5]:

$$f(t) = \mathrm{nh}\,\mathrm{P}\,\mathrm{K}\text{-}\qquad \frac{-\varepsilon_i}{h}\Bigg) \tag{1}$$

где $E_1,\ldots,E_i$ — полные наработки на отказ элемента; $K(x)$ —ядро (чётная нормированная функция); $h$ — параметр сглаживания; $n$ — объём выборки наработок.

Анализ методов определения $h$ показал, что значение данного параметра оказывает существенное влияние на вид оценки плотности распределения и её точность. При наличии малых выборок использование метода Сильвермана [6] для

первоначального определения значения параметра $h$ сохраняет универсальность метода построения плотности и не требует значительных вычислительных ресурсов. Формула вычисления

значения параметра $h$ имеет вид

$$h = 0{,}9 \min(b, \hat{}/1{,}34)\, n^{-1/5},$$

где $b$ — стандартное отклонение; $n$ — объём; $u$ — медиана выборки.

Выбор ядра обусловлен предпосылками, касающимися класса функции, которому принадлежит оцениваемая плотность, а также областью определения наработок на отказ. Рассмотрим функцию Гаусса в качестве первоначального ядра $f(t)$ [1]:

$$K^{(x)} = . \qquad /2.$$

## Адаптация метода Розенблатта — Парзена

Известно, что выбранная в качестве $K(x)$ функция Гаусса определена на области $(-то, то)$, а при проведении анализа надёжности наблюдаемой величиной является время с областью определения $[0, то)$. В этом случае при наличии наработок на отказ, близких к нулю, присутствует смещение плотности с нарушением условия нормировки $F(0) = 0$. Для компенсации смещения плотности предлагается применить метод зеркального отображения исходных данных [4]. При этом выражение (1)

$$f^{(t)} = nh \, P \, K^{n} \qquad t - E_i \qquad + K'C\text{-}+\hat{}\, h$$

примет следующий вид:

В случае цензурирования справа в качестве дополнительной исходной информации фигурирует массив из числа работоспособных элементов $V = (v_1, \ldots, v_s)$ на интервале $[l, то]$, где $l$ — правая граница интервала эксплуатации, на котором не зафиксированно отказов. Выражение для учёта цензурированных справа данных получено в [6]. Итоговое выражение для восстановления плотности распределения наработок на отказ можно записать так:

$$\bar{f}(\mathrm{R}) = T\,hn \quad P_K \qquad \frac{t - E_i}{} \qquad t + E_i \qquad + E\, V_j\, R\, K \qquad \frac{1/t - u/l}{} \qquad (2)$$

$$j=1 \quad t_0 \qquad \text{-----}d\text{----} \quad du$$

$$h$$

Здесь первое слагаемое отвечает за полные наработки на отказ с компенсацией смещения плотности, а второе — за цензурированные данные.

В целях экспериментальной проверки метода Розенблатта — Парзена и его адаптированного варианта проведена серия экспериментов с моделированием наработок по закону распределения Вейбулла с параметрами $m = 1{,}1$, $0 = 10_3$ с областью определения $[0, то)$. На смоделированных данных проведено исследование точности оценок. Выводы о точности основывались на вычислении ошибки оценивания $e_n$ в метрике $L_1$-пространства по выражению где $f(t)$ — смоделированная плотность распределения времени до отказа; $f(t)$ — экспериментальная плотность распределения времени до отказа.

По результатам эксперимента максимальная ошибка оценивания $e_n$ составляет: — 0,31 при расчёте $f(t)$ по выражению (1);

— 0,188 при расчёте $\bar{f}(t)$ по выражению (2).

Таким образом, адаптация метода Розенблатта — Парзена позволяет повысить точность восстанавливаемой плотности распределения за счёт компенсации смещения и учёта цензурированных данных. Применение предложенной адаптации целесообразно при отсутствии априорной информации о законе распределения случайных величин, наличии малых выборок, цензурированных данных и необходимости компенсации смещения.

Рассмотрим адаптированный метод Розенблатта — Парзена на примере оценки показателей надёжности вычислительной системы. Выражение (2) позволяет рассчитать основные показатели надёжности сложных систем. Как правило, надёжность объекта определяется надёжностью комплектующих элементов, поэтому для каждого элемента из состава объекта расчитываются следующие показатели:

— функция распределения времени на отказ:

$$F(t)=\int_0^T f(t)dt; \qquad (3)$$

— вероятность безотказной работы:

$$P(t)=1-F(t); \qquad (4)$$

— интенсивность отказов:

$$\frac{f(t)}{P(t)}; \qquad (5)$$

— средняя наработка времени между отказами:

$$T_{cp}=\frac{n}{\sum_{j=1} t_j}. \qquad (6)$$

Здесь $n$ — объём выборки наработок; $t_j$ — время штатного функционирования между $(j-1)$-м и $j$-м отказами.

В качестве объекта рассматривается вычислительная система из 20 параллельно функционирующих вычислительных узлов (элементов). Период полной подконтрольной эксплуатации объекта составляет $T = 35040$ ч (4 года). В период эксплуатации система мониторинга фиксирует информацию об отказах по каждому элементу. При заданном режиме функционирования отказ объекта наступает в результате отказа всех составных элементов. Полученная информация предварительно обрабатывается в соответствии с методикой подготовки данных [7] для последующей оценки плотности распределения времени до отказа и представляет:

— $\mathbf{E_T} = (E_1,\dots,E_i)$ — выборки полных наработок на отказ элементов за период $T$, где $E_i$ — время отказа оборудования;

— $\mathbf{V} = (v_1,\dots,v_s)$ —массив из числа работоспособных элементов на интервале $[1, \text{те}]$, где $l$ — правая граница периода $T$, на котором не зафиксировано отказов.

Для каждого элемента вычислительной системы по исходным данным и выражениям (3)-(6) рассчитаны основные показатели надёжности (с нижним индексом (el)) (таблица).

| № эл-та | *P(el)^* | A(el) (t) | Tcp(el) *(t)* | № эл-та | *P(el)(t)* | A(el) *(t)* | Tcp(el) (t) |
|---|---|---|---|---|---|---|---|
| 1 | 0,91 | 2,28e-04 | 4379 | 11 | 0,72 | 2,51e-04 | 3980 |
| 2 | 0,69 | 1,83e-04 | 5474 | 12 | 0,83 | 1,83e-04 | 5474 |
| 3 | 0,65 | 2,06e-04 | 4865 | 13 | 0,65 | 2,28e-04 | 4379 |
| 4 | 0,79 | 2,97e-04 | 3368 | 14 | 0,60 | 2,28e-04 | 4379 |
| 5 | 0,72 | 2,74e-04 | 3649 | 15 | 0,65 | 1,60e-04 | 6256 |
| 6 | 0,77 | 2,06e-04 | 4865 | 16 | 0,72 | 1,83e-04 | 5474 |
| 7 | 0,72 | 2,74e-04 | 3649 | 17 | 0,57 | 1,37e-04 | 7299 |
| 8 | 0,67 | 1,37e-04 | 7299 | 18 | 0,65 | 1,83e-04 | 5474 |
| 9 | 0,66 | 1,60e-04 | 6256 | 19 | 0,60 | 9,13e-05 | 10949 |
| 10 | 0,69 | 2,28e-04 | 4379 | 20 | 0,83 | 1,37e-04 | 7299 |

Связь показателей надёжности параллельно функционирующих элементов с показателями надёжности объекта определяется следующими выражениями: – вероятность безотказной работы:

$$P_{(ob)}(t) = 1 - \prod_{i=1}^{N} (1 - P_{(ei)}(t)_i); \qquad (7)$$

– интенсивность отказа:

$$A_{(ob)}(t) = P_{i=1}^{N_{\backslash el)}(t)} \underline{\quad} \qquad (8)$$

$$j=1 j$$

– средняя наработка времени между отказами:

$$T^{cp(ob)(t)} \qquad \text{УьД)} \bullet \qquad (9)$$

По данным из таблицы и выражениям (7)-(9) рассчитаны эксплуатационные показатели надёжности объекта:

– вероятность безотказной работы $P_{(ob)}(t) = 0{,}999$;

– интенсивность отказа объекта $A_{(ob)}(t) = 5{,}52\text{e-}05$;

– средняя наработка времени между отказами $T_{cp(ob)}(t) = 18108$.

По полученным оценкам построены кривые, представленные на рис. 1.

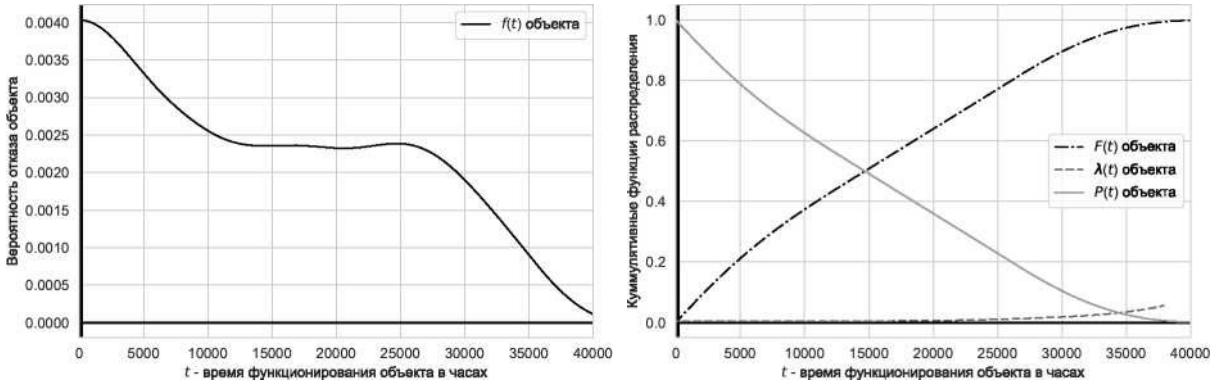



Рис. 1. Кривые, построенные по оценкам показателей надёжности объекта за период эксплуатации

Рассчитанные экспериментальные оценки показателей надёжности вычислительной системы необходимы для принятия управляющих решений при эксплуатации и сохранении работоспособности объекта.

ЛИТЕРАТУРА

1. Половко А. М., Гуров С. В., Основы теории надежности. 2-е изд. СПб.: БХВ-Петербург, 2008.
2. Захаров Д. Н., Никулин В. С., Анализ методов статистической оценки эксплуатационной надежности вычислительных комплексов //Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. №1. С. 64-69.
3. Чепурко В. А. Ядерная оценка параметра потока отказов. Диагностика и прогнозирование состояния сложных систем // Сб. научных трудов каф. АСУ НИЯУ МИФИ. 2004. № 15. С. 19-31.
4. Антонов А. В., Никулин М. С. Статистические модели в теории надежности. М.: Абрис, 2012. 390 с.
5. Parzen E. On estimation of a probability density function and mode // Ann. Math. Statistics. 1962. V. 33. P. 1065-1076.
6. Silverman B. Density estimation for Statistics and Data Analysis. London, N.Y.: Chapman & Hall/CRC, 1986.
7. Никулин В. С. Методика подготовки данных для интеллектуального анализа надежности вычислительных комплексов //Вестник СИБГУТИ. 2020. № 3(51). С. 26-37.

Секция 5

# ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ И ГРАФОВ

УДК 512.56, 519.7 DOI 10.17223/2226308X/14/34

## БАЗИСЫ НАД ПОЛЕМ GF(2), ПОРОЖДЁННЫЕ ПРИ ПОМОЩИ ОПЕРАЦИИ ШУРА — АДАМАРА

К. Л. Геут, С. С. Титов

Рассмотрена проблема построения, описания и применения базисов векторных пространств над полем из двух элементов, порождённых при помощи операции Шура — Адамара.

**Ключевые слова:** NSUCRYPTO, база матроида, базис векторного пространства, код Рида — Маллера.

Рассматривается векторное пространство $F_{r_2}$, состоящее из всех двоичных векторов длины $r$. Для любых $d$ таких векторов можно определить их покомпонентное произведение [1]. Пустое произведение (когда в нём нет элементов) равно вектору из всех единиц.

Пусть $s,d \in \mathbb{N}$, $s > d > 1$, $r = s^d$, $B$ – базис векторного пространства $F_{r_2}$ и $\bigcup_{i=0} i$ $F \subset F_2$ – семейство $s$ двоичных векторов, такое, что все возможные покомпонентные произведения до $d$ векторов из семейства $F$ (включая пустое произведение) образуют базис $B$ [2, 3].

Для векторов $a = (a_1, ..., a_n)$ и $b = (b_1, ..., b_n)$ из $F_{q^n}$ покоординатное умножение $a * b = (a_1b_1,..., a_nb_n)$ называется произведением Шура или произведением Адамара [4].

В задаче «Bases» [5] для данных $s, d$ и $r$ требуется описать все (или хотя бы некоторые) базисы $B$, для которых такое семейство $F$ существует, или доказать, что таких базисов нет. Предлагается дать также практическое применение таких базисов. Эту задачу естественно рассматривать на языке бинарных матроидов, элементами которых являются вектор-столбцы (или вектор-строки) некоторых матриц над полем GF(2), их циклов, подпространств, независимых множеств и, наконец, баз этих мат- роидов. В этой работе данная проблематика связывается с кодами Рида – Маллера порядка $d$, основанных на булевых функциях степени $d$ [6, 7], поскольку покомпонентное произведение векторов можно интерпретировать как конъюнкцию значений соответствующих аргументов булевой функции в полиноме Жегалкина (алгебраической нормальной форме, ANF). В связи с этой интерпретацией становятся естественными предлагаемые применения этих базисов в теории кодирования и схемах разделения секрета.

Покомпонентные произведения определённых в условии задачи векторов должны быть, очевидно, ненулевыми и линейно независимыми, в том числе – разными, поэтому можно считать их некоторыми $r$ вектор-строками в таблице некоторой булевой функции $f$, зависящей от $s$ аргументов $t^1, \ldots, t^s$ и степени не выше $d$ (после некоторой, может быть, перенумерации её аргументов), так что таблица истинности булевой

функции $f$ вместе со вспомогательными столбцами (для конъюнкций аргументов по два, три и т. д.) будет выглядеть так (табл. 1):

Таблица 1

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | $t^1$ | ... | $t_s$ | $t_1t^2$ | ... | $t_1t^s$ | ... | $t^1 \ldots t_d$ | ... | ... | $f$ |
| 1 | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 1 | $x_l$ | ... | $x_s x_1$ | ... | ... | $1s\ x_l x_l$ | ... | ... | ... | ... | $f_1$ |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 1 | $x_r$ | ... | $x^s s$ | ... | ... | $x_l$ $S\ x_r$ | ... | ... | ... | ... | $f_r$ |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |

Эту таблицу можно рассматривать как расширенную матрицу системы линейных уравнений над GF(2) с некоторой матрицей $B$ и правым столбцом $f$. Следовательно, базис получается тогда и только тогда, когда существует биекция между всеми булевыми функциями $f$, зависящими от $s$ аргументов $t^1, \ldots, t^s$ степени не выше $d$, и всем списком значений $f_1, \ldots, f_r$ на этих булевых векторах значений аргументов $x^1, \ldots, x^s$.

Рассмотрение булевых функций от $s$ аргументов степени вплоть до $d$ означает рассмотрение кода Рида — Маллера порядка $d$, список значений всех аргументов можно расположить в естественном порядке их двоичных представлений [2, 8].

Пусть $X$ и $Y$ — некоторые множества, $F$ — некоторое подмножество множества всех функций $f: X \to Y$. Естественно назвать подмножество $Z \subset X$ множеством единственности класса функций $F$, если для любой функции $g: Z \to Y$ существует единственная функция $f$ из класса $F$, такая, что её ограничение на $Z$ совпадает с $g$, то есть $f|_Z = g$.

В нашем случае $Y = \{0, 1\}$, $F$ — подмножество булевых функций степени $d$, $X = V_s$ — пространство булевых векторов длины $s$. Искомые базисы при этом оказываются множествами, однозначно определяющими булеву функцию степени не выше $d$ по любым заданным на этом множестве значениям функции.

Если транспонировать табл. 1 (без столбца значений функции), то получим матрицу, которую естественно назвать матрицей Рида — Маллера порядка $d$. Векторный матроид вектор-столбцов этой матрицы тоже естественно назвать матроидом Рида — Маллера, циклами которого являются минимальные по включению множества линейно зависимых векторов, а базами — искомые базисы как максимальные подматрицы с ненулевым определителем. При этом верхняя строка (имеющая нулевой номер) определителя состоит из одних единиц, а строки с первой по $s$-ю являются вектор-строками семейства $F$, определяющего базис $B$, составленный из всех строк этой подматрицы. Каждый вектор-столбец матрицы Рида — Маллера удобно обозначать номером $N$ двоичного представления набора аргументов $t^1 \ldots t^s$.

Например, для $s = 3$, $d = 2$ и $r = 7$ имеем матрицу Рида — Маллера, приведённую в табл. 2.

Можно предложить конструкцию для базисов $B$ с таким семейством $F$ для всех $s$, $d$, $s > d > 1$, на основе кодов Рида — Маллера порядка $d$, которая даёт серию искомых базисов для всех параметров $s, d, r$.

**Конструкция 1.** Определим семейство $F$ как множество столбцов матрицы Рида —

Маллера при следующем условии: слово $x_{i^1} \ldots x_{i^s}$ значений аргументов $t^1, \ldots, t^s$ имеет вес Хэмминга не больше $d$.

Таблица 2

| $N$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $t^1$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| $t^2$ | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| $t^3$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| $t_1t^2$ | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| $t_1t^3$ | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| $t^2t^3$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

Для примера в табл. 2 берутся все столбцы, кроме столбца 7, потому что в этой конструкции в базис входят те столбцы, у которых в строках $t^1, t^2, t^3$ имеется не более двух единиц.

Очевидно, что значения коэффициентов соответствующей функции $f$ определяются рекуррентно и однозначно, как и в доказательстве теоремы об ANF [8, теоремы 2.6 и 2.10]: коэффициент перед композицией для подмножества $T$ (мощности не больше $d$) в множестве $\{t^1, \ldots, t^s\}$ аргументов определяется как сумма значений $f$ и значений коэффициентов для всех подмножеств $R \subset T$, так что это множество $T$ — множество единственности [8] для семейства булевых функций степени не выше $d$ и, следовательно, базис. Обозначим этот базис через $B_0$.

Таким образом, трактовка искомого базиса как множества единственности полинома Жегалкина булевой функции степени не выше $d$ равносильна невырожденности некоторой подматрицы в полной матрице кода Рида — Маллера порядка $d$ (в соответствии с теоремой Кронекера — Капелли).

**Конструкция 2.** Поскольку полная аффинная группа является группой автоморфизмов кодов Рида — Маллера, её можно использовать для описания целого класса искомых базисов.

Рассмотрим полную аффинную группу, действующую на множестве вектор-столбцов $(t^1, \ldots, t^s)^T$. Ясно, что преобразования этой группы реализуют перестановки столбцов матрицы Рида — Маллера. В силу того, что эта группа является группой автоморфизмов, она переводит множество единственности в множество единственности, то есть базис в базис. Отсюда следует

**Утверждение 1.** Пусть $B_0$ — построенный в конструкции 1 базис. Тогда для любого аффинного преобразования векторов — значений аргументов $(t^1, \ldots, t^s)^T$ множество преобразованных вектор-строк базиса $B_0$ также образует базис.

Такие базисы можно использовать для построения кода Рида — Маллера, который определяется через порождающую матрицу, содержащую, в том числе, все возможные произведения $l$ строк [8, 9].

Так как количество и длины этих строк определяют параметры кода, то построение базиса определённой размерности регулирует кодирующие способности кода, построенного посредством такого базиса.

Однако существуют базисы, не получающиеся из базиса $B_0$ посредством аффинного преобразования, и их описание приводит к задаче аффинной классификации булевых

функций, которая решена для квадратичных булевых функций, т. е. для $d = 2$ [8].

Перечисление искомых базисов может быть произведено при помощи графа баз соответствующего матроида, поскольку он оказывается связным.

Пусть $M$ – матроид, $B_0$ и $B$ – две его базы: $B_0, B \in \mathfrak{B}$. Определим, что эти базы соединены ребром в графе $\Gamma(\mathfrak{B})$ баз этого матроида, если $|B_0 \triangle B| = 2$, где $\triangle$ означает симметрическую разность множеств:

$$B_0 \triangle B = (B_0 \setminus B) \cup (B \setminus B_0) = (B_0 \cup B) \setminus (B_0 \cap B).$$

Поскольку $|B \triangle B| = 0$ и $B_0 \triangle B = B \triangle B_0$, имеем симметричное антирефлексивное бинарное отношение на множестве $\mathfrak{B}$ баз матроида $M$, т. е. действительно получается граф с вершинами – элементами множества $\mathfrak{B}$.

Каковы свойства этого графа? Ясно, что если $M$ дискретен, т.е. в нем нет циклов, то семейство $\mathfrak{B}$ баз одноэлементно и ребер нет. Если в $M$ есть единственный цикл $C - E$ – множество всех элементов матроида $M$, то базами являются все подмножества в $E$ мощности $|E| - 1$, и граф представляет собой $(|E| - 1)$-элементную клику. Вне этих крайних случаев имеем $|B_0 \triangle B| = 2m$ – чётное число, поскольку $|B_0| = |B|$.

Пусть $|B_0 \triangle B| = 2m$, $m > 1$:

$$\underbrace{0 \ldots 0 z \ldots 0}_{B'} 0 \ldots 0$$

По аксиоме замены для каждого $b_0 \in B_0 \setminus B$ существует такой $b \in B \setminus B_0$, что $B_1 = (B_0 \setminus \{b_0\}) \cup \{b\}$ является базой. Вычисляем

$$|B_1 \triangle B| = |(B_1 \cup B) \setminus (B \cap B_1)| = |B_1 \cup B| - |B_1 \cap B| =$$
$$= (|B_0 \cup B| - 1) - (|B_0 \cap B| + 1) = (|B_0 \cup B| - |B_0 \cap B|) - 2 = 2(m - 1), \text{ при этом}$$

$$|B_1 \triangle B_0| = |B_1 \cup B_0| - |B_1 \cap B_0| = (|B_0| + 1) - (|B_0| - 1) = 2,$$

то есть $B_1$ и $B_0$ соединены ребром в графе $\Gamma(\mathfrak{B})$. Отсюда индукцией по $m$ получаем

**Утверждение 2.** Граф $\Gamma(\mathfrak{B})$ связен.

Первоначально этот результат был получен в работе [10] для максимальных совместных подсистем линейных неравенств и применён в алгоритме выделения всех максимальных совместных подсистем несовместной системы линейных неравенств [11].

ЛИТЕРАТУРА


1. Деундяк В. М., Косолапов Ю. В. О некоторых свойствах произведения Шура — Адамара для линейных кодов и их приложениях // Прикладная дискретная математика. 2020. №50. С. 72-86.
2. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
3. Чижов И. В. Обобщённые автоморфизмы кода Рида — Маллера и криптосистема МакЭлиса — Сидельникова // Прикладная дискретная математика. Приложение. 2009. № 1. С. 36-37.
4. Деундяк В. М., Косолапов Ю. В. О некоторых свойствах произведения Шура — Адамара для линейных кодов и их приложениях // Прикладная дискретная математика. 2020. № 50. С. 72-86.

5. International Olympiad in Cryptography NSUCRYPTO. https://nsucrypto.nsu.ru (дата обращения 30.10.2020).
6. Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида — Маллера // Дискретная математика. 1994. Т. 6. С. 3-20.
7. Ведунова М. В., Геут К. Л., Игнатова А. О. Преломляющие биекции в тройках Штейнера // Прикладная дискретная математика. Приложение. 2020. №13. С. 6-8.
8. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.
9. Высоцкая В. В. Квадрат кода Рида — Маллера и классы эквивалентности секретных ключей криптосистемы Мак-Элиса — Сидельникова // Прикладная дискретная математика. Приложение. 2017. № 10. С. 66-68.
10. Гайнанов Д. Н., Новокшенов Л. И., Тягунов Л. И. О графах, порождаемых несовместными системами линейных неравенств // Матем. заметки. 1983. № 33:2. С. 146-150.
11. Мазуров В. Д., Хачай М. Ю. Бустинг и полиномиальная аппроксимируемость задачи о минимальном аффинном разделяющем комитете // Тр. ИММ УрО РАН. 2013. Т. 19. №2. С. 231-236.

УДК 621.391.7 DOI 10.17223/2226308X/14/35

# О РАЗЛОЖИМОСТИ ПРОИЗВЕДЕНИЯ ШУРА — АДАМАРА СУММЫ ТЕНЗОРНЫХ ПРОИЗВЕДЕНИЙ КОДОВ РИДА — МАЛЛЕРА

Ю. В. Косолапов, Е. А. Лелюк

В рамках оценки стойкости кодовых криптосистем типа Мак-Элиса рассматривается задача исследования разложимости квадрата кода $K$, являющегося суммой специального вида двух тензорных произведений кодов Рида — Маллера. В ряде случаев удалось найти условия на параметры кодов-множителей, при которых квадрат кода $K$ раскладывается в прямую сумму кодов Рида — Маллера; найдены также условия, при которых такое разложение невозможно.

**Ключевые слова:** криптосистема типа Мак-Элиса, сумма тензорных произведений, произведение Шура — Адамара, разложимость.

Кодовые криптосистемы типа Мак-Элиса рассматриваются в качестве альтернативы современным асимметричным криптосистемам, так как при выборе подходящего кода являются стойкими к атакам с помощью компьютера на основе квантовой модели вычисления [1]. Оригинальная система Мак-Элиса на кодах Гоппы в настоящее время считается стойкой, но высокая стойкость достигается за счёт ключа большого размера [2]. С целью уменьшения размера ключа предложены криптосистемы типа Мак-Элиса на других кодах. Но для некоторых широко известных кодов, таких, как обобщённые коды Рида — Соломона, двоичные коды Рида — Маллера, системы типа Мак-Элиса оказываются нестойкими и для компьютеров на основе классической модели Тьюринга [3 — 5]. Для усиления стойкости криптосистем в [6] предлагается использовать тензорное произведение кодов Рида — Маллера. В [7] исследуется класс кодов, обобщающий конструкцию тензорного произведения. Коды из этого класса представляют собой сумму нескольких тензорных произведений специального вида. Эти коды эффективно декодируются, поэтому на их основе можно построить криптосистему типа Мак-Элиса. Но для применения криптосистемы необходимо проанализировать её стойкость. При анализе стойкости кодовых криптосистем к атакам на ключ часто исследуются свойства произведения Шура — Адамара кодов,

которые лежат в основе этих криптосистем [8].

В настоящей работе ставится задача исследования разложимости квадрата суммы специального вида двух тензорных произведений кодов Рида — Маллера.

Напомним, что линейным $[n, k]_q$-кодом $C$ называется подпространство размерности $k$ пространства $\underline{F}_{q^n}$ над полем Галуа $F_q$. Для кода $C$ ортогональный к нему код будем обозначать $C = \{\mathbf{x} \in F_n : \forall \mathbf{c} \in C ((\mathbf{x}, \mathbf{c}i = 0\}$, где $h\mathbf{x}, \mathbf{c}i$ – скалярное произведение векторов. Для двух кодов $C_1, C_2 \subset F_n$ произведение Шура – Адамара $C_1 * C_2$ определяется как линейная оболочка, натянутая на множество векторов $\{\mathbf{x} * \mathbf{y} : \mathbf{x} \in C_1, \mathbf{y} \in C_2\}$, где $\mathbf{x} * \mathbf{y} = (x_1y_1, \ldots, x_ny_n)$. При этом под квадратом кода $C$ понимается код $C^2 = C * C$ [8]. Под внутренней суммой кодов $C_1$ и $C_2$ будем понимать код $C_1 + C_2 = \{\mathbf{x} + \mathbf{y} : \mathbf{x} \in C_1, \mathbf{y} \in C_2\}$, а под внешней (прямой) суммой кодов $C \subset F_{q^{n_1}}$ и $D \subset F_{n^2}$ – код $C \oplus D = \{(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in C, \mathbf{y} \in D\}$, где $(\mathbf{x}, \mathbf{y})$ – конкатенация векторов $\mathbf{x}$ и $\mathbf{y}$. Тензорное произведение кодов $C$ и $D$ обозначим $C \otimes D$ [9]. В случае $C = F_{n'}$ получаем следующее равенство:

$$F_{n'} \otimes D = \underbrace{D \oplus \ldots \oplus D}_{n_1},$$

а в случае $D = F_{q^{n_2}}$ код $C \otimes F_{q^{n_2}}$ перестановочно эквивалентен коду

$$F_{n^2} \otimes C = \underbrace{C \oplus \ldots \oplus C}_{n_2}.$$

Код называется разложимым, если он перестановочно эквивалентен прямой сумме двух или более кодов ненулевой размерности [10].

Пусть $RM(r, m)$ – двоичный код Рида – Маллера порядка $r$ и длины $2^m$. Рассмотрим коды $C_1 = RM(r_1^1, m_1)$, $C_2 = RM(r_2^1, m_1)$, $D_1 = RM(r_1^2, m_2)$, $D_2 = RM(r_2^2, m_2)$, такие, что $C_2 \subset C_1$, $D_1 \subset D_2$. Код

$$\kappa = C_1 \otimes D_i + C_2 \otimes D_2 \qquad (1)$$

является мажоритарно-декодируемым кодом [7]. Отметим, что $C_1 \subset C_2$, $D_2 \subset D_1$. В [11] доказано, что для произвольных кодов $V_1, V_2 \subset F_{q^{n_1}}$, $W_1, W_2 \subset F_{q^{n_2}}$ выполняется равенство

$$(V_1 \oplus W_1) * (V_2 \oplus W_2) = (V_1 * V_2) \oplus (W_1 * W_2).$$

Отсюда получаем, что квадрат кода $K$ имеет следующий вид:

$$\kappa^2 = C_1 \otimes D\} + (C_1 * C_2) \oplus (D_i * в_2) + C_2 \oplus D_2. \qquad (2)$$

**Теорема 1.** Пусть $K$ – код вида (1).

1) Если $m_1 - r_1^1 - 1 > m_1/2$ и $m_2 - r_1^2 - 1 < m_2/2$, то

$$\kappa^2 = F_{2^{2^{m_1}}} \oplus RM(2(m_2 - r_1^2 - 1), m_2).$$

2) Если $m_1 - r_2^1 - 1 < m_1/2$ и $m_2 - r_2^2 - 1 > m_2/2$, то

$$\kappa^2 = RM(2(m_1 - r_2^1 - 1), m_1) \oplus F_{2^{2^{m_2}}}.$$

**Теорема 2.** Пусть $\kappa$ – код вида (1). Если выполняется хотя бы одно из условий:

1) $m_1 - r_1^1 - 1 > m_1/2$ и $m_2 - r_1^2 - 1$
2) $2m_1 - (r_1^1 + r_2^1) - 2 > m_1$ и $2m_2 - (r_1^2 + r_2^2) - 2 > m_2$,
3) $m_1 - r_2^1 - 1 > m_1/2$ и $m_2 - r_2^2 - 1 > m_2/2$,

то

$$\kappa^2 \quad {}_{2^{m_1+m_2}}$$

**Теорема 3.** Пусть $K$ – код вида (1), $m_1 - r_2^1 - 1 > m_1/2$, $m_2 - r_1^2 - 1 > m_2/2$, $m_1 - r_1^1 - 1 <$

$m_1/2$, $m_2 - r_2^2 - 1 < m_2/2$.

1) Если $2m_1 - (r_1^1 + r_2^1) - 2 > m_1$ и $2m_2 - (r_1^2 + r_2^2) - 2 < m_2$, то

$$K^2 = \mathrm{RM}(2r_1 - m_1 + 1, m_1) \circledast \mathrm{RM}(r_2 + r_2 - m_2 + 1, m_2).$$

2) Если $2m_1 - (r_1^1 + r_2^1) - 2 < m_1$ и $2m_2 - (r_1^2 + r_2^2) - 2 > m_2$, то

$$K^2 = \mathrm{RM}(r_1 + r_2 - m_1 + 1, m_1) \circledast \mathrm{RM}(2r_2 - m_2 + 1, m_2).$$

В случаях, не рассмотренных в теоремах 1-3, то есть при

$$m_i - r_x - 1 < m_1, m_2 - r_2 - 1 < m_2, 2m_i - (r_x + r_2) - 2 < m_i, 2m_2 - (r_x + r_2) - 2 < m_2, \quad (3)$$

представление (2) не удаётся упростить и сделать выводы о разложимости квадрата кода вида (1) в прямую сумму кодов Рида — Маллера. Но в этом случае можно оценить размерность кода (2) и проверить, возможно ли разложение этого кода в прямую сумму каких-либо кодов Рида — Маллера длины $2^{m_1}$ или $2^{m_2}$. А именно, если размерность кода (2) не делится на $2^{m_1}$ или $2^{m_2}$, то этот код не разлагается в прямую сумму и не является перестановочно эквивалентным такому коду. Согласно результатам вычислений, для $m_i = 2, \ldots, 10$ и $m_2 = 2, \ldots, 10$ общее количество кодов вида (1), удовлетворяющих условиям (3), равно $9025$. При этом количество кодов, размерность которых делится на $2^{m_1}$ или $2^{m_2}$, равно $204$. Это значит, что для случайно выбранного кода вида (1), удовлетворяющего условиям (3), с вероятностью более $0{,}97$ его квадрат не разлагается в прямую сумму кодов Рида — Маллера длины $2^{m_1}$ или $2^{m_2}$.

ЛИТЕРАТУРА


1. Sendrier N. and Tillich J.-P. Code-Based Cryptography: New Security Solutions Against a Quantum Adversary. ERCIM News, ERCIM, 2016.
2. https://classic.mceliece.org/nist/mceliece-20201010.pdf — Supporting Documentation describing the round-3 submission. 2020.
3. Сидельников В. М., Шестаков С. О. О системе шифрования, основанной на обобщенных кодах Рида — Соломона // Дискретная математика. 1992. Т. 3. №3. С. 57-63.
4. Minder L. and Shokrollahi A. Cryptanalysis of the Sidelnikov cryptosystem // LNCS. 2007. V. 4515. P. 347-360.
5. Чижов И. И., Бородин М. А. Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида — Маллера // Дискретная математика. 2014. Т. 26. № 1. С. 10-20.
6. Деундяк В. М., Косолапов Ю. В., Лелюк Е. А. Декодирование тензорного произведения MLD-кодов и приложения к кодовым криптосистемам // Модел. и анализ информ. систем. 2017. Т. 24. №2. С. 137-152.
7. Деундяк В. М., Лелюк Е. А. Теоретико-графовый метод декодирования некоторых групповых MLD-кодов // Дискретн. анализ и исслед. опер. 2020. Т. 27. №2. С. 17-42.
8. Randriambololona H. On products and powers of linear codes under componentwise multiplication. arXiv:1312.0022. 2014.
9. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
10. Деундяк В. М., Косолапов Ю. В. Анализ стойкости некоторых кодовых криптосистем, основанный на разложении кодов в прямую сумму // Вестн. ЮУрГУ. Сер. Матем. моделирование и программирование. 2019. Т. 12. № 3. С. 89-101.
11. Деундяк В. М., Косолапов Ю. В. О некоторых свойствах произведения Шура — Адамара для линейных кодов и их приложениях // Прикладная дискретная математика. 2020. № 50. С. 72-86.


УДК 519.17 DOI 10.17223/2226308X/14/36

# РЕГУЛЯРНОЕ ВЕРШИННОЕ 1-РАСШИРЕНИЕ ДВУХМЕРНЫХ РЕШЁТОК[XVIII]

А. А. Лобов, М. Б. Абросимов

Предлагается схема построения вершинного 1-расширения для двухмерной решётки n x m при $n > 2$ и $m > 2$, которое является регулярным графом степени 4.
Показано, что с помощью данной схемы для некоторых решёток можно построить минимальное вершинное 1-расширение. Приведён пример графа, для которого построенное по схеме расширение не является минимальным.

**Ключевые слова:** граф, решётка, отказоустойчивость, вершинное расширение.

Безопасность вычислительных систем имеет большое значение. Отказ элементов может привести к её полной неработоспособности. Для обеспечения отказоустойчивости таких систем может применяться графовая модель. Каждому вычислительному узлу системы сопоставляется вершина графа, а связь между двумя узлами представляется ребром между соответствующими вершинами. Далее граф дополняется вершинами и рёбрами до вершинного $k$-расширения, которое является представлением устойчивой к отказу $k$ узлов вычислительной системы. Будем рассматривать случай с $k = 1$.

Граф $G^*$ является вершинным 1-расширением (В-1-Р) графа $G$, если $G$ вкладывается в каждый граф, полученный из $G^*$ удалением одной вершины. Если количество вершин в $G^*$ на 1 больше, чем в $G$, и среди всех В-1-Р графа $G$ с таким числом вершин количество рёбер в $G^*$ минимально, то $G^*$ называется минимальным вершинным 1-расширением (МВ-1-Р) графа $G$ [1].

Задача построения расширений графа связана с построением отказоустойчивой вычислительной системы [2, 3]. В этих работах для некоторых классов графов, таких, как цепи и циклы, предложены способы построения МВ-1-Р, однако в целом задача нахождения МВ-1-Р заданного графа является вычислительно сложной [4].

Дадим определение рассматриваемым в работе графам.

**Определение 1.** *Двухмерной решёткой, или просто решёткой* $nxm$, называется граф, множество вершин которого состоит из пар $(i, j)$, $i,j \in \{0,\dots, n-1\}$, и множество рёбер состоит из всех возможных пар вершин $(u_1, v_1)$ и $(u_2, v_2)$, для которых $|u_1-u_2| = 1$ и $v_1 = v_2$ или $|v_1 - v_2| = 1$ и $u_1 = u_2$.

Пример такого графа представлен на рис. 1.

Двухмерная решётка является интересной топологией с практической точки зрения.

**Теорема 1.** При $n, m > 2$ для каждой решётки $n \times m$ существует регулярный граф степени 4, который является её вершинным 1-расширением. Количество дополнительных рёбер в данном расширении равно $n + m + 2$.

[XVIII]Работа выполнена при поддержке Минобрнауки России в рамках выполнения госзадания (проект № FSRR-2020-0006).

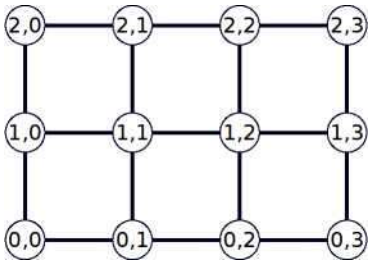



Рис. 1. Решётка 3 x 4

Для построения данного расширения необходимо выполнить следующие шаги:

1) Добавить рёбра между вершинами с метками $(0, i)$ и $(n-1, i-1)$, где $i \in \{1, \ldots, m-1\}$.

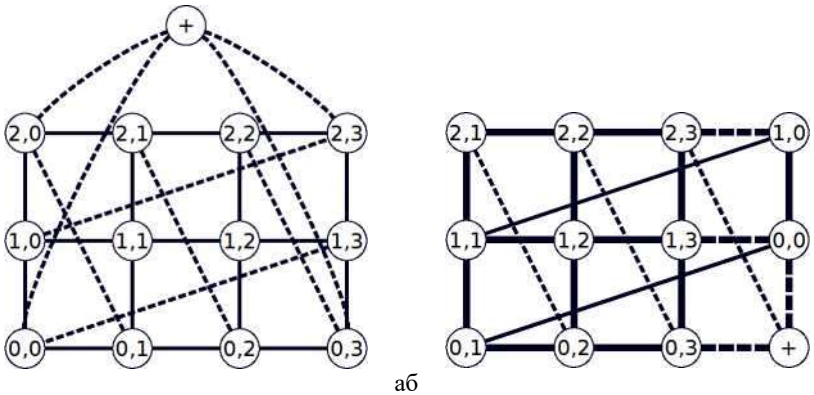
2) Добавить рёбра между вершинами с метками $(i, m-1)$ и $(i-1, 0)$, где $i \in \{1, \ldots, n-1\}$.

3) Добавить вершину и соединить её с $(0, m-1)$, $(n-1, m-1)$, $(n-1, 0)$, $(0, 0)$.

Расширение, построенное по этой схеме, является вершинно-симметричным регулярным графом степени 4. Напомним, что регулярным называется граф, степени вершин которого равны, а вершинно-симметричным – граф, для каждой пары вершин $u, v$ которого существует автоморфизм $\wedge$, такой, что $\wedge(u) = v$.

Расширения, получаемые по предложенной схеме, могут быть построены с помощью алгоритма А2 [5]. На примере решёток $3 \times 3$ и $4 \times 5$ это показано в [6]. Поэтому для реконфигурации таких 1-расширений графов можно использовать описанный в [5] способ. Под реконфигурацией понимается поиск вложения исходной решётки в полученный после удаления из расширения одной вершины граф.

Построенное по схеме расширение решётки $3 \times 4$ представлено на рис. 2, а. Граф, полученный удалением любой вершины, изоморфен графу рис. 2, б. На рисунке выделена изоморфная исходной решётке часть.

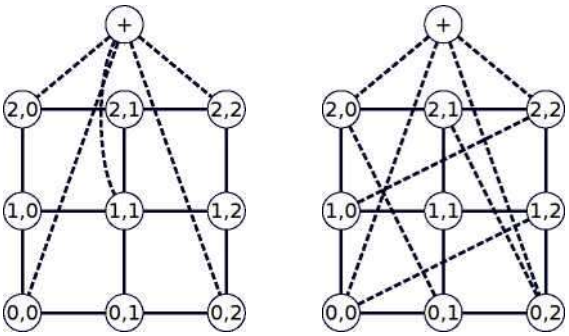



аб

Рис. 2. Расширение решётки 3 *x* 4 (а) и её реконфигурация после отказа (б)

Для решётки $3 \times 4$ построенное по предложенной схеме расширение является минимальным, что подтверждено вычислительным экспериментом [7]. Однако в общем

случае это неверно. Например, для решётки $3 \times 3$ минимальное расширение имеет пять дополнительных рёбер, а у расширения, построенного по схеме, их восемь. Данные расширения изображены на рис. 3.




аб

Рис. 3. МВ-1-Р (а) и построенное по предложенной схеме расширение решётки 3 х 3 (б)

Следует отметить, что для рассматриваемых в [7] решёток $2 \times m$ построенное по предложенной схеме расширение также не является минимальным.

ЛИТЕРАТУРА

1. Абросимов М. Б. Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012.
2. Hayes J. P. A graph model for fault-tolerant computing system // IEEE Trans. Comput. 1976. No. 9. P. 875-884.
3. *Harary F. and Hayes J. P.* Node fault tolerance in graphs // Networks. 1996. V. 27. P. 19-23.
4. *Абросимов М.Б.* О сложности некоторых задач, связанных с расширениями графов // Матем. заметки. 2010. № 5(88). С. 643-650.
5. *Каравай М. Ф.* Минимизированное вложение произвольных гамильтоновых графов в отказоустойчивый граф и реконфигурация при отказах. I // Автоматика и телемеханика. 2004. № 12. С. 159-178.
6. *Каравай М. Ф.* Минимизированное вложение произвольных гамильтоновых графов в отказоустойчивый граф и реконфигурация при отказах. II. Решетки и k-отказоустойчивость // Автоматика и телемеханика. 2005. № 2. С. 175-189.
7. *Камил И. А. К.* Вычислительный эксперимент по построению отказоустойчивых реализаций графов с числом вершин до 9 // Intern. J. Open Inform. Technol. 2020. V. 8. No. 9. P. 43-47.

УДК 519.1 DOI 10.17223/2226308X/14/37

# ОБ АТТРАКТОРАХ В ОДНОЙ ДИСКРЕТНОЙ ДВОИЧНОЙ ДИНАМИЧЕСКОЙ СИСТЕМЕ С ДВУДОЛЬНЫМ ГРАФОМ ЗАВИСИМОСТЕЙ

Р. И. Пантелеев, А. В. Жаркова

Рассматривается дискретная двоичная динамическая система $(S_n, f)$, $n > 1$, состояниями которой являются все возможные двоичные векторы длины n, с эволюционной функцией вида $f = (x_n, 0, \ldots, 0, x_1)$ и двудольным графом зависимостей.

Приводится теорема, определяющая аттракторы, их вид и количество, в рассматриваемых системах.

**Ключевые слова:** аттрактор, бассейн, граф, граф зависимостей, двудольный граф, дискретная двоичная динамическая система, эволюционная функция.

Система, использующая модель безопасности с полным перекрытием, должна

иметь, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути проникновения в систему. Множество отношений «объект-угроза» образует двудольный граф, в котором ребро $(u, v)$ существует тогда и только тогда, когда $u$ является средством получения доступа к объекту $v$. Графовые модели, в которых отказы процессоров интерпретируются как удаление соответствующих вершин, а отказы сетевых каналов — как удаление дуг, занимают важное место в задачах, связанных с отказоустойчивостью компьютерных сетей. При изучении модельных графов можно применять идеи и методы теории конечных динамических систем. В данной работе рассматривается дискретная двоичная динамическая система с двудольным графом зависимостей. Важная проблема в теории конечных динамических систем состоит в том, чтобы связать структуру системы с её динамикой.

Под *конечной динамической системой* понимается пара $(S, 5)$, где $S$ — конечное непустое множество, элементы которого называются *состояниями системы*, $5 : S \wedge S$ — отображение множества состояний в себя, называемое *эволюционной функцией системы*. Каждой конечной динамической системе сопоставляется карта, представляющая собой орграф с множеством вершин $S$ и дугами, проведёнными из каждой вершины $s \in S$ в вершину $5(s)$. Компоненты связности графа, задающего динамическую систему, называются её *бассейнами*. Каждый бассейн представляет собой контур с входящими в него деревьями. Контуры, в свою очередь, называются *предельными циклами*, или *аттракторами*.

Основными проблемами теории конечных динамических систем являются задачи отыскания эволюционных параметров без проведения динамики [1]. К их числу относятся аттракторы, их вид, количество. Например, в работе [2] подсчитано количество аттракторов в конечных динамических системах ориентаций полных графов. В данной работе определяется вид и количество аттракторов в одной дискретной двоичной динамической системе с двудольным графом зависимостей.

Рассмотрим, согласно [3], дискретную двоичную динамическую систему $(S_n, f)$, $n > 1$, состояниями которой являются все возможные двоичные векторы длины $n$, с эволюционной функцией $f = (f_1, \ldots, f_n)$, где двоичные функции имеют вид

$$f_i = c1 \wedge r^{Eli}_{a_i} x_i \ldots x_n^{Ei''},$$

где $a_i \in \{0,1\}$ и $E_{ji} \in \{0,1\}$. Если $a_i = 0$, то все $E_{ji} = 0$.

С $f$ ассоциируется ориентированный *граф зависимостей* $X$ с множеством вершин $\{a_1, \ldots, a_n, E\}$, в котором существует дуга из $a_i$ в $a_j$, если $a_i = 1$ и $x_j$ — множитель $f_i$ (то есть $E_{ji} = 1$), а также существует дуга из $a_i$ в $E$, если $a_i = 0$ (то есть $f_i = 0$).

В работе рассматриваются данные динамические системы с двудольными графами зависимостей и функциями вида $f = (x_n, 0, \ldots, 0, x_1)$, при $n = 2$ получаем $f = (x_n, x_1)$.

На рис. 1 изображена карта дискретной двоичной динамической системы $(S_3, f)$ с эволюционной функцией $f = (x_3, 0, x_1)$ и её двудольный граф зависимостей.

В результате исследований сформулирована следующая

**Теорема 1.** Дискретная двоичная динамическая система $(S_n, f)$, $n > 1$, с эволюционной функцией $f = (x_n, 0, \ldots, 0, x_1)$ имеет три бассейна и три аттрактора видов рис. 2, и только их.

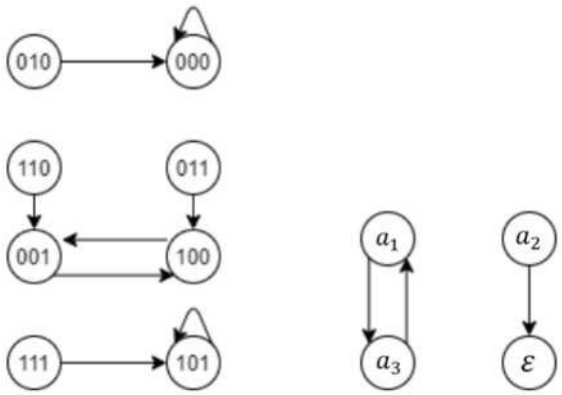



Рис. 1

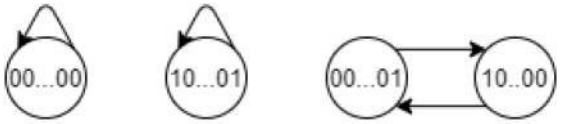



Рис. 2. Аттракторы

ЛИТЕРАТУРА

1. Жаркова А. В. Индексы состояний в динамической системе двоичных векторов, ассоциированных с ориентациями пальм // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2016. Т. 16. Вып. 4. С. 475-484.
2. Жаркова А. В. О количестве аттракторов в конечных динамических системах ориентаций полных графов // Прикладная дискретная математика. Приложение. 2018. № 11. С. 106-109.
3. Colon-Reyes O., Laubenbacher R., and Pareigis B. Boolean monomial dynamical systems // Ann. Combinatorics. 2004. V. 8. P. 425-439.

УДК 519.17 DOI 10.17223/2226308X/14/38

# СХЕМЫ ПОСТРОЕНИЯ МИНИМАЛЬНЫХ ВЕРШИННЫХ 1-РАСШИРЕНИЙ ПОЛНЫХ ДВУХЦВЕТНЫХ ГРАФОВ[XIX]

П. В. Разумовский, М. Б. Абросимов

Рассматриваются двухцветные графы, то есть графы, вершины которых раскрашены в два цвета. Пусть G = (V, *a, f*) —цветной граф с определённой на множестве его вершин функцией раскраски f. Цветной граф $G^*$ называется вершинным 1-расширением цветного графа G, если граф G можно вложить с учётом цветов в каждый граф, получающийся из графа $G^*$ удалением любой его вершины вместе с инцидентными рёбрами. Вершинное 1-расширение $G^*$ графа $G$ называется минимальным, если граф $G^*$ имеет на две вершины больше, чем граф G, а среди всех вершинных 1-расширений графа $G$ с тем же числом вершин граф $G^*$ имеет минимальное число рёбер. Предлагается полное описание минимальных вершинных 1-расширений полных двухцветных графов. Пусть $K_{n_1,n_2}$ —полный n-вершинный граф с $n_1$ вершинами одного цвета и $n_2$ вершинами другого цвета. Если в полном двуцветном графе $n_1 = n_2 = 1$, то в минимальном вершинном 1-расширении такого графа будет одно дополнительное ребро. Если в полном двуцветном графе либо $n_1 = 1$, либо $n_2 = 1$, то в минимальном вершинном 1-расширении такого графа будет 2n - 1 дополнительных рёбер. Во всех остальных случаях в минимальном вершинном 1-расширении полного двухцветного графа будет 2n дополнительных рёбер.

[XIX]Работа выполнена при поддержке Минобрнауки России в рамках госзадания (проект № FSRR- 2020-0006).

Предлагаются схемы построения соответствующих минимальных вершинных 1-расширений.

**Ключевые слова:** разметка графа, цветной граф, полный граф, расширение графа, минимальное вершинное расширение графа, отказоустойчивость.

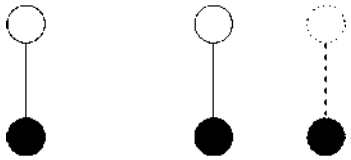
С точки зрения безопасности вычислительных систем большое значение имеет их надёжность, одним из аспектов которой является отказоустойчивость. Существуют разные математические модели отказоустойчивости. В данной работе рассматривается модель, предложенная Джоном Хейзом [1]. Техническая система моделируется графом. Элементам системы соответствуют вершины графа, а связям между элементами — рёбра (или дуги, если связи не являются симметричными). Если элементы имеют разный тип, то соответствующим им вершинам графа приписываются метки типа или цвета. Таким образом, моделью технической системы является граф с вершинами разного цвета, или цветной граф. Основные определения теории графов используются в соответствии с [2]. Будем рассматривать неориентированные графы. Понятия минимальных расширений для графов даются в соответствии с [1, 3].

**Определение 1.** Граф $G^* = (V^*, a^*, f^*)$ называется минимальным вершинным $k$-расширением $n$-вершинного $i$-цветного графа $G = (V, a, f)$, если выполняются следующие условия:

1) граф $G^*$ является вершинным $k$-расширением цветного графа $G$, то есть граф $G$ можно вложить с учётом цветов в каждый граф, получающийся из графа $G^*$ удалением любой его вершины вместе с инцидентными рёбрами;
2) граф $G^*$ содержит $n + ik$ вершин, то есть $|V^*| = |V| + ik$;
3) $a^*$ имеет минимальную мощность среди всех графов, удовлетворяющих условиям 1 и 2.

В работе [1] рассматривается задача построения минимального вершинного 1-расширения для цветного дерева особого вида. В [4] решается задача о генерации цветных графов без проверки на изоморфизм. В данной работе мы рассмотрим полные графы $K_{n_1,n_2}$ с вершинами двух цветов, то есть $i = 2$. Для удобства будем считать, что $n_1 \leq n_2$. Как следует из определения, минимальное вершинное 1-расширение графа $K_{n_1,n_2}$ содержит две дополнительные вершины. Далее представлено полное решение задачи построения всех минимальных вершинных 1-расширений для графов $K_{n_1,n_2}$. Заметим, что в работе [5] введена модель для изучения отказов связей, которой соответствует минимальное рёберное $k$-расширение. Если рассматриваются графы без кратных рёбер, то полные графы не имеют минимальных рёберных $k$-расширений ни при каких натуральных значениях $k$. Аналогичная ситуация имеет место и для цветных полных графов. Напомним, что объединением двух графов $G_1 = (V_1, a_1)$ и $G_2 = (V_2, a_2)$ называется граф $G_1 \cup G_2 = (V_1 \cup V_2, a_1 \cup a_2)$. Если $V_1 \cap V_2 = 0$, то естественным образом операция переносится и на случай цветных графов.

**Теорема 1.** Полный двухцветный граф $K_{1,1}$ имеет единственное с точностью до изоморфизма минимальное вершинное 1-расширение — граф $K_{1,1} \cup K_{1,1}$ (рис. 1).

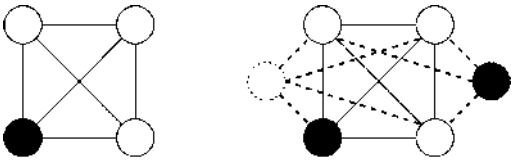


аб

Рис. 1. Полный двухцветный граф $K_{1,1}$ (а) и его минимальное вершинное 1-расширение (б)

**Теорема 2.** Полные n-вершинные двухцветные графы вида $K_{1,n_2}$, где $n_2 > 1$, имеют единственное с точностью до изоморфизма минимальное вершинное 1-расширение, которое содержит $2n_2+1$ дополнительных рёбер и строится следующим образом: добавляются вершина $v_1$ первого цвета и вершина $v_2$ второго цвета. Вершина $v_1$ соединяется со всеми вершинами второго цвета, вершина $v_2$ соединяется также со всеми вершинами второго цвета и с одной из вершин первого цвета.

На рис. 2 приведены полный двухцветный граф $K_{1,3}$ и его минимальное вершинное 1-расширение.

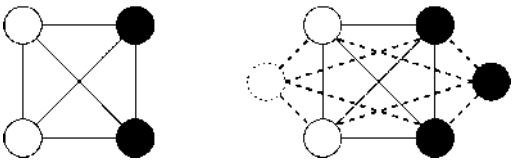


аб

Рис. 2. Граф $K_{1,3}$ (а) и его минимальное вершинное 1-расширение (б)

**Теорема 3.** Полные n-вершинные двухцветные графы вида $K_{n_1,n_2}$, $1 < n_1 \leq n_2$, имеют единственное с точностью до изоморфизма минимальное вершинное 1-расширение, которое содержит $2n$ дополнительных ребра и строится следующим образом: добавляются вершина $v_1$ первого цвета и вершина $v_2$ второго цвета. Вершины $v_1$ и $v_2$ соединяются рёбрами со всеми вершинами исходного графа.

На рис. 3 приведены полный двухцветный граф $K_{2,2}$ и его минимальное вершинное 1-расширение.



аб

Рис. 3. Граф $K_{2,2}$ (а) и его минимальное вершинное 1-расширение (б)

Таким образом, схемы построения минимальных вершинных 1-расширений найдены для всех возможных полных двухцветных графов.

ЛИТЕРАТУРА

1. Hayes J. P. A graph model for fault-tolerant computing system // IEEE Trans. Comput. 1976. V.C.-25. No. 9. P. 875-884.
2. Богомолов А. М., Салий В. Н. Алгебраические основы теории дискретных систем. М.: Наука, 1997. 368 с.
3. Абросимов М. Б. Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012. 192

с.
4. Разумовский П. В., Абросимов М. Б. Построение цветных графов без проверки на изоморфизм // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2021. Т. 21. Вып. 2. С. 267-277.
5. Harary F. and Hayes J. P. Edge fault tolerance in graphs // Networks. 1993. V. 23. P. 135-142.

UDC 004.453.2 DOI 10.17223/2226308X/14/39

# TOWARDS THE SECURITY OF McEliece's CRYPTOSYSTEM BASED ON HERMITIAN SUBFIELD SUBCODES[xx]

G. P. Nagy, S. El Khalfaoui

The purpose of this paper is to provide a comprehensive security analysis for the parameter selection process, which involves the computational cost of the information set decoding algorithm using the parameters of subfield subcodes of 1-point Hermitian codes.

**Keywords:** code-based cryptography, McEliece Cryptosystem, Hermitian subfield subcodes, Schur square dimension.

## 1. Introduction

Recently, there has been a big amount of research addressed to quantum computers that use quantum mechanical techniques to solve hard computational problems in mathematics [1]. The existence of these powerful machines threaten many of the publickey cryptosystem that are widely in use [2]. McEliece [3] introduced the first code-based public-key cryptosystem in 1978. The crucial issues in cryptography today is to reduce the key size and improve the security level of the McEliece cryptosystem, which is a promising cryptographic scheme for the post-quantum era [4]. Error correcting codes, used in codebased cryptographic protocols, must have efficient decoding algorithms. A rich class of such codes is the family algebraic-geometric (AG) codes, their subcodes and subfield subcodes. This includes the generalized Reed — Solomon codes, the alternant codes, the binary Goppa codes and BCH codes. See [5] for a survey on the decoding of AG codes.

The authors of [6 — 8] provided polynomial-time attacks against the McEliece cryptosystem that relies either on AG codes or on their subcodes. In general, evaluation codes do not behave like random codes which demonstrate the quite range of attacks proposed against the McEliece cryptosystem based on AG codes. The approach given in [6, 8] is inspired by the so-called filtration attacks that rely on computing the Schur product that make AG codes distinguishable form random ones. Wieschebrink [9] used this observation to provide an attack against McEliece scheme based on subcodes of GRS codes [10]. Many attacks have been founded on this argument, and have employed a

[xx]Project no. 2018-1.2.1-NKP-2018-00004 has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme.

combination of powerful techniques such as the filtration method, an error-correcting pair (ECP) or an error-correcting array (ECA), that lead to a key recovery attack or a blind reconstruction of a decoding algorithm [6, 8, 11]. These vulnerabilities are based on two operations: Schur product and s-closure. In some cases, the Schur filtration method can expand the latter to develop an efficient decoding algorithm.

The purpose of this paper is to provide a comprehensive security analysis for the parameter selection process, which involves the computational cost of the information set decoding (ISD) algorithm using Hermitian subfield subcode parameters. Our approach focuses on the optimal parameters that improve the key size for a given security level. Furthermore, due to practical considerations, the key size of several parameter selections is compared to that of the classical McEliece cryptosystem submitted to NIST [4] for the same security level. Besides, we identify the Hermitian subfield subcodes parameters that achieve a Schur square dimension roughly equal to that of random codes. This technique is employed in the so-called distinguisher attack, that allows the attacker to determine the Schur square dimension of the code used as a public key.

## 2. Preliminaries

Let $q$ be a prime power. A $q$-ary linear code of length $n$ is a linear subspace $C \subseteq \mathbb{F}_{q^n}$. The dimension of $C$ is denoted by $k$, $C$ is usually given by its $n \times k$ *generator matrix* $G$, or its $n \times (n-k)$ *parity check matrix* $H$:

$$C = \{Gx : x \in \mathbb{F}_k\} = \{y \in \mathbb{F}_n : Hy = 0\}.$$

The *minimal distance* of $C$ is $d(C) = \min\{wt(x) : x \in C \setminus \{0\}\}$, where $wt(x)$ denotes the *Hamming weight* of the vector $x$. If $2t < d(C)$, then for each $y \in \mathbb{F}_{q^n}$, there is at most one pair $x, e \in \mathbb{F}_{q^n}$ of vectors such that $x \in C$, $wt(e) \leq t$ and $y = x + e$. Define the map $D_{C,t} : \mathbb{F}_n \to C \cup \{*\}$ by $y \to x$ if the decomposition $y = x + e$ exists, and $y \to *$ otherwise. We call $D_{C,t}$ a *nearest neighbor decoding* of $C$, correcting up to $t$ errors. In general, known nearest neighbor decoding algorithms have exponential time complexity in the size of the input $G, t, y$. The seminal result by Berlekamp, McEliece and van Tilborg [12] shows that the decoding problem is NP-complete even for the binary case $q = 2$. The simplest general decoding technique is called *information set decoding* (ISD), with goes back to an old algorithm of Prange [13]. This algorithm has time complexity

$$C_{Prange}(n, k, t) = \qquad C_{Gauss}(n, k, q),$$

where $C_{Gauss}(n, k, q)$ is the time complexity of the Gauss – Jordan elimination of a $k \times n$ matrix over $\mathbb{F}_q$. There are many improvements of Prange's algorithms, but all known variants have the same asymptotic behavior, see [14] and the references therein.

Let us fix the parameters $n, k, t$ and $q$. The McEliece cryptographic scheme [3], or in general code-based cryptosystems has a $[n, k, t]_q$ linear code $C$ as public key, and an efficient decoding algorithm $D_{C,t}$ as private key. Usually, $C$ is given by a generator matrix in systematic form, that is, the key size is

$$G= \begin{matrix} I_k \\ G_0 \end{matrix}$$
$$k(n— k)\text{dlog}_2(q)\text{e}.$$

The plain text message $m$ G $F_q^k$ is encrypted to $c = Gm + e$ G $F_q^n$, where $e$ is a random element of weight $t$ in $F_q^n$. The security of the scheme relies on two facts:

1) To prevent a message recovery attack, the parameters n, k, t and q must be chosen such that the time complexity of ISD exceeds a given level L of security. This level is usually measured in bits, and corresponds to the time complexity of breaking an L-bits symmetric-key block cipher, like AES. Since it is not the purpose of this paper to give a detailed cryptanalysis of symmetric-key block ciphers, we interpret this condition as
$$\text{n . n-k} > 2^L.$$
tt
2) To prevent a key recovery attack, it should not be possible to give an efficient decoding algorithm for C. At this point, we not only assume the knowledge of G, but also the technique that was used to construct C from a given family of codes. In the classic McEliece proposal, $G = PG_1S$, where $G_1$ is the generator matrix of the binary Goppa code r(L,g). Here, $g = g(X)$ is a polynomial over $F_q$ with no repeated roots, L is an ordered n-tuple of distinct elements of $F_q$ that are no roots of g, $P$ is a random $n$ x $n$ permutation matrix, and $S$ is a random $k$ x $k$ invertible matrix; L, $g$, $P$, $S$ are parts of the private key; they are supposed to be kept secret for a long period of time.

The second requirement implies that the public key C must be indistinguishable from a random subspace of $F_q^n$. In general, distinguishing attacks do not necessarily lead to message or key recovery attacks. However, often they do, and cryptosystems must resist to distinguishing attacks.

## 3. The Schur product distinguisher

We briefly introduce some notions on attack techniques that allow us to describe some important results stated in [6].

**Definition 1.** Given two elements $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in $F_q^n$, the Schur product is the component-wise

$$a * b = (a_1b_1, \ldots, a_nb_n)$$

product on $F_n$. For two linear subspaces $A, B$ C $F_n$, their Schur product is the linear subspace

$$A * B = \text{Span}_{F_q}\{a * b : a \in A \text{ and } b \in B\}.$$

If $B = A$, then $A * A$ is denoted as $A^{*2}$, and we define $A^{*t}$ by induction for any positive integer $t$.

One of the main results in [15] is that when the length $n$ is such that $n > k(k+1)/2$, the dimension of the square of the random code $C$ is exactly $k(k+1)/2$, with probability tending to 1 as $n - k(k+1)/2$ approaches infinity. More precisely, we define $F(n, k)$ as the family of linear codes of length $n$ and dimension k. Let $n : N \longrightarrow N$ be such that $n(k) > k(k+1)/2$. Then there exits a constant $\gamma \in R$ such

that, for all large enough k,

$$\Pr_{\kappa}\left[\dim C * C = k(k+1)/2\right] > 1 - 2^{\gamma(n(k)-k(k+1)/2)}$$

where $C$ is chosen uniformly at random from $\mathsf{F}(n(k), k)$. This observation serves as a useful distinguisher between random linear subspaces and those with a rich algebraic structure.

**Definition 2.** Let C be an $[n, k]_q$ linear code. We say that C is s-good, if

$$\dim(C * C) = \dim(C^{\perp} * C^{\perp}) = n.$$

## 4. Algebraic-geometric codes: constructions and parameters

Algebraic-geometric codes are linear error-correcting codes constructed from algebraic curves over finite fields. They are defined by evaluating functions or by using residues of differentials. Their parameters can be derived from well-known theorems of algebraic geometry. Our notation and terminology on algebraic plane curves over finite fields, their function fields, divisors and Riemann – Roch spaces are standard, see for instance [16].

Let X be an algebraic curve, i.e., an affine or projective variety of dimension one, which is absolutely irreducible and nonsingular, and whose defining equations are (homogeneous) polynomials with coefficients in $F_q$. Let $g = g(X)$ be the genus of X, $F_q(X)$ denotes the function field of X. A divisor D of X is a formal sum $D = n_1P_1 + \ldots + n_kP_k$, where $n_1,\ldots,n_k \in Z$ and $P_1,\ldots, P_k$ are places of $F_q(X)$. If $n_1\ldots,n_k > 0$, then $D \geq 0$. If $D,E$ are two divisors and $D - E \geq 0$, then $D \geq E$. For a non-zero function f in the function field $F_q(x)$ and a place $P$, $v_P(f)$ stands for the order of $f$ at $P$. If $v_P(f) > 0$, then $P$ is a zero of $f$, while if $v_P(f) < 0$, then $P$ is a pole of $f$ with multiplicity $-v_P(f)$. The principal divisor of a non-zero function $f$ is $\mathrm{Div}(f) = \sum_P v_P(f)P$.

For a divisor $D$, the associated Riemann – Roch space $L(D)$ is the vector space

$$L(D) = \{f \in F_q(X) \setminus \{0\} : \mathrm{Div}(f) \geq -D\} \cup \{0\}.$$

The dimension $\ell(D)$ of $L(D)$ is given by the Riemann-Roch Theorem [16, Theorem 1.1.15]:

$$\ell(D) = \ell(W - D) + \deg D - g + 1,$$

where $W$ is a canonical divisor. We denote the set of *differentials* on X by $\Omega(D)$. The *differential space* of the dividor $D$ is

$$\Omega(D) = \{dh \in \Omega : \mathrm{Div}(dh) \geq A\} \cup \{0\}.$$

In the following, $P_1, P_2, \ldots, P_n$ are pairwise distinct places on X, and $D$ is the divisor $D = P_1 + \ldots + P_n$. Let $G$ be another divisor with support disjoint from $D$. We define two types of AG codes, the *functional* and the *differential codes*, respectively:

$$C_L(D,G) = \{(f(P_1),\ldots,f(P_n)) : f \in L(G)\},$$

$$C_\Omega(D, G) = \{(\mathrm{res}_{P_1}(\eta),\ldots, \mathrm{res}_{P_n}(\eta)) : \eta \in \Omega(G - D)\}.$$

These codes are dual to each other, and $C_Q(D, G) = C_L(D, K + D - G)$ for an well-chosen canonical divisor $K$. The Riemann – Roch theorem enables us to estimate the dimension and the minimum distance of AG codes:

$$|> \deg^{(G)} \overline{\quad} \; g + 1, \; 0 \; 6 \; \deg^{(G)} \; 6 \; 2g \overline{\quad} \; 2, \; \dim(C_L(D, G)) =$$
$$\deg(G) - g + 1, \; 2g - 2 \; 6 \; \deg(G) \; 6 \; n,$$
$$I \; 6 \; \deg(G) - g + 1, \; n \; 6 \; \deg(G) \; 6 \; n + 2g - 2.$$

The minimum distance of a functional code is at least its *designed minimum distance*

$$6_{L} = n - \deg(G).$$

AG codes have polynomial time decoding algorithms, that can correct up to $t = (J_L - g)/2$ errors [5]. However, they are vulnerable to Schur filtration attacks. In particular, AG codes are far from being s-good. The following proposition is derived from [17, Theorem 6].

**Proposition 1.** Let $G$ and $G^0$ be two divisors on the curve $X$ both with disjoint support with the divisor $D$ and such that $\deg G > 2g + 1$ and $\deg G^0 > 2g$. Then

$$C_L(D, G) * C_L(D, G_0) = C_L(D, G + G_0).$$

In particular, $\dim(C_L(D, G)^{*2}) \; 6 \; 2 \dim(C_L(D, G)) + g - 1.$

Let $C$ be a linear subspace of the functional code $C_L(D, G)$. The Schur filtration attack constructs an effective decoding algorithm using a system of linear subspaces

$$W_{i,j} = \{z \; G \; F_n : z * C^{*i} \; 6 \; C^{*j}\}.$$

Here, $i, j > 1$ may be arbitrary. Clearly, if $i < j$, then $C^{*(j-i)} \; 6 \; W_{ij}$.

## 5. Subfield subcodes of 1-point Hermitian codes

Reed – Solomon codes form a well-known subclass of AG codes. In this section, we present the construction of Hermitian codes, another subclass of interest. Let $H_q$ be a Hermitian curve over a finite field $F_{q^2}$. In affine coordinates, $H_q$ is given by the equation

$$H_q : Y^q + Y = X^{q+1}.$$

It is a non-singular curve, and its genus is $g = q(q - 1)/2$ by the genus formula. $H_q$ has one point $P_\infty = (0:1:0)$ at infinity, and $q^3$ affine rational points $P_1, \ldots, P_{q^3}$. This makes the class of Hermitian curves interesting since they attain the maximal number of rational points for Hasse – Weil bound [18]. Such curves are called $F_{q^2}$-maximal. Xing and Stichtenoth [19] showed that for fixed $q$, the genus of a $F_{q^2}$-maximal curve is $6 \; q(q - 1)/2$, and equality holds if and only if $X$ is isomorphic to $H_q$.

**Definition 3.** Let $s$ be a positive integer. The $F_{q^2}$-linear code $C_L(D, sP_\infty)$ of length $n = q^3$ is called a Hermitian 1-point code.

In general, it is a hard computational problem to determine a bases of the Riemann – Roch space $L(D)$. For 1-point divisors $D = sP_\infty$ of the Hermitian curve,

such a basis is given in [18, Theorem 10.4]. The dual of $C_L(D, sP_\infty)$ is a 1-point Hermitian code too, with parameter

$$s^{\perp} = n + 2g - 2 - s = q(q^2 - q - 1) - s.$$

Clearly, 1-point Hermitian codes form an increasing series of linear subspaces of $F_{q^2}$.

Let $m$ be a positive integer and $r = q^m$. Let $C$ be a linear $[n, k, t]$ code over $F_r$. The $F_r/F_q$ subfield subcode of $C$ is defined as

$$C|_{F_q} = C \cap F_n.$$

The true dimension $k^*$ of $C|_{F_q}$ is hard to determine, but the bound

$$k^* > n - m(n - k)$$

is straightforward. Any algorithm that can decode up to $t$ errors of $C$ can be used to correct up to $t$ errors of the subfield sub code $C|_{F_q}$.

In this paper, we examine the class

$$C_q(s) = C(D, sP).$$

of Hermitian subfield subcodes, and propose their usage in code-based cryptosystems. In [20], we determined the true dimension of $C_q(s)$ for some specific values of $s$. In [21], we conducted an experimental study to analyze the true dimension of $C_q(s)$ for $q \le 16$, and concluded that the datasets can be best approximated by the extreme value distribution.

Here, our focus is on the resistance of $C_q(s)$ to the Schur distinguishing attack. We determine the parameters such that the key size is significantly smaller than in the classic McEliece scheme. Notice that the Schur filtration technique may be used for key recovery attacks on subfield subcodes of AG codes, as well, provided the degree $m$ of the field extension, and the genus of the underlying algebraic curve are small. In our case, $m = 2$ is small, but the genus is the largest possible with fixed field $F_{q^2}$ and maximal length $n$.

**Proposition 2.** Let $q$ be a prime power and let $C_q(s) = C_L(D, sP_\infty)_q$ be a 1-point Hermitian subfield subcode. There are positive integers $a_q, b_q$ such that $C_q(s)$ is s-good if and only if $a_q \le s \le b_q$.

We conducted numerical experiments to determine the values $a_q, b_q$ for $q \le 16$, see Table 1. The results motivate the following conjecture.

**Open problem 1.** Let $q$ be a prime power and let $C_q(s) = C_L(D, sP_\infty)|_{F_q}$ be a 1-point Hermitian subfield subcode. Then $\dim(C_q(s)^{\perp} * C_q(s)^{\perp}) = q^3$ if and only if $s \le q^3 - q - 1$.

Table 1

Interval bounds for s-goodness

| $q$ | 4 | 5 | 7 | 8 | 9 | 11 | 13 | 16 |
|---|---|---|---|---|---|---|---|---|
| $a_q$ | 45 | 72 | 192 | 315 | 400 | 720 | 1176 | 2 295 |
| $b_q$ | 59 | 119 | 335 | 503 | 719 | 1319 | 2183 | 4 079 |

## 6. Comparative of Hermitian subfield subcodes to McEliece cryptosystem: key size and security level

The National Institute of Standards and Technology (NIST) has recently begun a selection process to standardize asymmetric cryptosystems resistant to quantum computer attacks [4]. Code-based cryptosystems are promising candidates for NIST selection.

In this section, we analyse the computational cost of solving the ISD problem for various sets of parameters relevant to post-quantum cryptography. To do so, we consider classical McEliece cryptosystem variants built on Goppa codes. The parameters for cryptosystems reported in [22] are designed to be comparable to the computational cost required to break AES-128 (Category 1), AES-192 (Category 3), and AES-256 (Category 5). The Tables 2 and 3 summarize the code parameters of Classical McEliece cryptosystem submitted to NIST round 2-code-based cryptosystems, and those of 1-point Hermitian subfield subcodes $C_q(s)$ (code length $n$, dimension $k$, and error-capability $t$), as well as the computational cost of Prange's ISD algorithm, expressed as $\log_2$ (bit operations) with the public key size.

Table 2

Classic McEliece cryptosystem

| Classic McEliece | $n$ | $k$ | $t$ | Prange complexity | Key size (bit) |
|---|---|---|---|---|---|
| Category 1 | 3 488 | 2 720 | 64 | 142.78 | 2088 960 |
| Category 3 | 4 608 | 3 360 | 96 | 184.89 | 4193 280 |
| Category 5 | 6 688 | 5 024 | 128 | 262.35 | 8 359 936 |
| | 6 960 | 5413 | 119 | 263.44 | 8373911 |
| | 8192 | 6 528 | 128 | 300.14 | 10 862 592 |

Table 3

McEliece cryptosystem based on s-good 1-point Hermitian subfield subcodes

| | Code Type | $n$ | k | $t$ | Prange complexity | Key size (bit) |
|---|---|---|---|---|---|---|
| Category 1 | $C_{11}$(1174) | 1331 | 927 | 78 | 142.33 | 1 123 524 |
| Category 3 | $C_{13}$(2039) | 2197 | 1 735 | 79 | 185.89 | 3 206 280 |
| | $C_{16}$(3 980) | 4 096 | 3 634 | 58 | 187.40 | 6 715 632 |
| Category 5 | $C_{13}$(1861) | 2197 | 1 398 | 168 | 263.01 | 4 468 008 |
| | $C_{16}$(3 874) | 4 096 | 3 422 | 111 | 300.65 | 9 225 712 |

REFERENCES


1. Arute F., Arya K., Babbush R, et al. Quantum supremacy using a programmable superconducting processor . Nature, 2019, vol .574(7779), pp .505-510.
2. Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 1997, vol. 26, pp. 1484-1509.
3. McEliece R. J. A Public-Key Cryptosystem Based on Algebraic Coding Theory. Jet Propulsion Lab, 1978. DSN Progress Report 44. pp. 114-116.
4. Post-Quantum Cryptography. http://csrc.nist.gov/projects/post-quantum-crypto graphy. Updated: March 25, 2020.
5. *H0holdtT., and PellikaanR.* On the decoding of algebraic-geometric codes. Special Issue on Algebraic Geometry Codes. IEEE Trans. Inform. Theory, 1995, vol. 41, no. 6, part 1, pp. 1589-1614.
6. *Couvreur A., Marquez-Corbella I., and Pellikaan R.* Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes. IEEE Trans. Inform. Theory, 2017, vol. 63(8), pp. 5404-5418.
7. *Couvreur A., Maarquez-Corbella I., and Pellikaan R.* Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes. Coding Theory and Applications. Cham, Springer, 2015, pp. 133-140.

8. *Couvreur A., Otmani A., and Tillich J.-P.* Polynomial time attack on wild mceliece over quadratic extensions. IEEE Trans. Inform. Theory, 2016, vol. 63(1), pp. 404-427.
9. *Wieschebrink C.* Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. Intern. Workshop Post-Quantum Cryptogr., Berlin, Springer, 2010, pp. 61-72.
10. *Berger T. P. and Loidreau P.* How to mask the structure of codes for a cryptographic use. Des. Codes Cryptogr., 2005, vol. 35(1), pp. 63-79.
11. *Couvreur A., GaboritP., Gauthier-Umana V., et al.* Distinguisher-based attacks on publickey cryptosystems using Reed —- Solomon codes. Des. Codes Cryptogr., 2014, vol. 73(2), pp. 641-666.
12. *Berlekamp E. R., McEliece R. J., and van Tilborg H. C. A.* On the inherent intractability of certain coding problems. IEEE Trans. Inform. Theory, 1978, vol. IT-24(3), pp. 384-386.
13. *Prange E.* The use of information sets in decoding cyclic codes. IRE Trans. Inform. Theory, 1962, vol. 8(5), pp. 5-9.
14. *Canto Torres R. and Sendrier N.* Analysis of information set decoding for a sub-linear error weight. LNCS, 2016, vol. 9606,pp. 144-161.
15. *Cascudo I., Cramer R., Mirandola D., and Zaemor G.* Squares of random linear codes. IEEE Trans. Inform. Theory, 2015, vol. 61(3), pp. 1159-1173.
16. *Stichtenoth H.* Algebraic Function Fields and Codes. Graduate Texts in Math., Berlin, Springer Verlag, 2009, vol. 254, 355 p.
17. *Mumford D.* Varieties defined by quadratic equations. Questions on Algebraic Varieties. C.I.M.E. Summer Schools, vol. 51. Berlin; Heidelberg, Springer, 2010, pp. 29-100.
18. Menezes A. J., Blake I. F., Gao X., et al. Applications of Finite Fields. Kluwer Intern. Series Engin. Computer Sci., Boston, MA, Kluwer Academic Publishers, 1993, vol. 199. 218 p.
19. Xing C. P. and Stichtenoth H. The genus of maximal function fields over finite fields. Manuscripta Math., 1995, vol. 86(2), pp. 217-224.
20. El Khalfaoui S. and Nagy G. P. On the dimension of the subfield subcodes of 1-point Hermitian codes. Adv. Math. Commun., 2021, vol. 15(2), pp. 219-226.
21. Nagy G. P. and Khalfaoui S. E. Estimating the dimension of the subfield subcodes of Hermitian codes. Acta Cybernetica, 2020, vol. 24(4), pp. 625-641.
22. Baldi M., Barenghi A., Chiaraluce F., et al. A finite regime analysis of information set decoding algorithms. Algorithms, 2019, vol. 12(10), p. 209.

Секция 6

# МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 519.682 DOI 10.17223/2226308X/14/40

## О РЕШЕНИИ ПОЛИНОМИАЛЬНЫХ ГРАММАТИК И ОБЩЕГО АЛГЕБРАИЧЕСКОГО УРАВНЕНИЯ

О. И. Егорушкин, И. В. Колбасина, К. В. Сафонов

Исследуется разрешимость формальных грамматик, под которыми подразумеваются системы некоммутативных полиномиальных уравнений, в случае одного уравнения. Формальные грамматики решаются в виде формальных степенных рядов (ФСР), которые выражают нетерминальные символы языка через терминальные символы; первая компонента решения и есть формальный язык. Авторы развивают метод, основанный на изучении коммутативного образа грамматики и языка, который получается, если во всяком ФСР символы алфавита считать коммутативными переменными. Получена теорема, которая даёт разложение в степенной ряд решения общего алгебраического уравнения, а также позволяет исследовать разрешимость в виде ФСР полиномиальной грамматики, состоящей из одного уравнения.

**Ключевые слова:** общее алгебраическое уравнение, полиномиальная грамматика, формальный степенной ряд, некоммутативные символы, коммутативный образ.

Как известно, теория формальных языков имеет фундаментальное значение не только для лингвистики, но и программирования. Наиболее важные для приложений классы формальных грамматик можно записать в виде системы полиномиальных уравнений с некоммутативными переменными [1, 2].

Следуя [3, 4], понимаем под полиномиальной грамматикой систему полиномиальных уравнений

$$P_j(z,x)=0,\ P_j(0,0)=0,\ j=1,...,k,$$

которая решается относительно символов $z=(z_1,\ldots,z_n)$ в виде формальных степенных рядов, зависящих от символов $x=(x_1,\ldots,x_m)$.

Символы $x_1,\ldots,x_m$ называются терминальными и образуют словарь языка, а символы $z_1,\ldots,z_n$ — нетерминальными, они необходимы для задания грамматических правил. Над всеми символами определена некоммутативная операция конкатенации и коммутативные операции формального сложения и умножения на числа, а значит, можно рассматривать ФСР с числовыми коэффициентами. Мономы от терминальных символов интерпретируются как предложения языка, а каждый ФСР — сумма всех «правильных» мономов, который является решением полиномиальной системы, понимается как порождённый грамматикой язык [1, 2].

Исследовать системы с некоммутативными символами очень трудно, и потому в работах [3 - 5] предложено рассмотреть коммутативный образ полиномиальной грамматики: для ФСР $s$ коммутативный образ $ci(s)$ получается в предположении, что все переменные коммутативны.

Трудность исследования полиномиальных грамматик имеет место даже в случае одного уравнения:

$$P_1(z, x) = 0.$$

Так, известно [3, 4], что одно уравнение с некоммутативными неизвестными может: не иметь решений; иметь любое конечное число решений; иметь бесконечно много решений. Поэтому случай некоммутативных переменных принципиально отличается от уравнения над полем комплексных чисел, которое всегда разрешимо.

Понятно, что достаточно рассмотреть общее алгебраическое уравнение

$$P_l(z, x) = X_n Z^n + X_{n-i} Z_{n-1} + \text{-----} + X_1 z + X_0 = 0 \qquad (1)$$

относительно символа $z$ (здесь $z = z_1$) и исследовать разложение неявной функции $z = z(x)$, определяемой коммутативным образом уравнения (1) в степенной ряд либо ряд Лорана относительно переменных $x_0, x_1, \ldots, x_n$.

С одной стороны, решение уравнения (1) представляет интерес для теории формальных языков и грамматик, с другой — конструктивное решение общего алгебраического уравнения в виде функции от коэффициентов является фундаментальной математической задачей, имеющей многовековую историю.

Как известно, после открытия формул Кардано и Феррари для решения уравнений третьей и четвертой степени появилась некоторая надежда решать произвольное алгебраическое уравнение в радикалах, однако почти через триста лет, в 1826 г., Абель доказал невозможность этого для уравнений пятой и более высоких степеней. Точнее, Абель доказал, что если существует формула, выражающая в радикалах корни уравнения пятой степени через его коэффициенты, то в случае действительных коэффициентов уравнение имеет либо один действительный корень, либо пять (очевидно, такое уравнение может иметь лишь три действительных корня, а значит, формулы в радикалах не существует). С этого времени конструктивное представление решений вызывает особый интерес.

Конструктивное представление решения как функции от коэффициентов возможно в виде интегралов и рядов, что часто оказывается более удобным для приближённых вычислений. Так, в 1921 г. Меллин предложил решать общее уравнение с помощью гипергеометрических функций, причём разложение в ряд получено на основе интегрального представления Меллина — Барнса. В 1984 г. Умемура доказал разрешимость уравнения произвольной степени с помощью тэта-функций.

В принципе, получить разложение в ряд неявной функции $z = z(x_1, \ldots, x_n)$, определяемой функциональным уравнением

$$F(z, x_1, \ldots, x_n) = 0,$$

не очень сложно. Как правило, такие разложения содержат оператор дифференцирования возрастающего порядка, либо коэффициенты степенного разложения даются формулой с возрастающим числом слагаемых.

Теперь наша цель — найти конструктивный способ разложить в ряд неявную функцию $z(x)$, заданную коммутативным образом уравнением (1), если возможно, в «замкнутом виде». Идея состоит в том, что функция $z(x)$ — алгебраическая, и потому её ряд является диагональю ряда некоторой рациональной функции от переменных, число которых на 1 больше числа коэффициентов уравнения [6].

Рассмотрим произвольную ветвь $z = z(x)$ решения уравнения (1), проходящую через точку $(0, 0)$ (достаточно считать, что такая ветвь единственная).

**Теорема 1.** Для функции, заданной коммутативным образом уравнения (1), имеет

место разложение в ряд Лорана

$$z(x) = P(-1)^{k} \sum_{k_2+\ldots+k_n>1} \frac{(2k_2+\ldots+nk_n)!}{((n-1)k_n+\ldots+k_2+1)!\,k_2!\ldots k_n!} x_0^{(n-1)k_n+\ldots+k_2+1} x_1^{-nk_n-\ldots-2k_2-k_2} x_2^{k_2} \ldots x_n^{k_n}.$$

Поскольку в формуле решения степени переменной $x_1$ отрицательные, то решение исходного некоммутативного уравнения (1) в виде ФСР невозможно, таким образом, имеет место следующее

**Следствие 1.** Полиномиальная грамматика, порождённая уравнением (1), не имеет решения (не порождает полиномиального языка).

ЛИТЕРАТУРА


1. Глушков В. М., Цейтлин Г. Е., Ющенко Е. Л. Алгебра. Языки. Программирование. Киев: Наукова думка, 1973.
2. Salomaa A. and Soitolla M. Automata-Theoretic Aspects of Formal Power Series. N.Y.: Springer Verlag, 1978.
3. Егорушкин О. И., Колбасина И. В., Сафонов К. В. О совместности систем символьных полиномиальных уравнений и их приложении // Прикладная дискретная математика. Приложение. 2016. №9. С. 119-121.
4. Egorushkin O. I., Kolbasina I. V., and Safonov K. V. On solvability of systems of symbolic polynomial equations // Журн. СФУ. Сер. Матем. и физ. 2016. Т. 9. Вып. 2. С. 166-172.
5. Семёнов А. Л. Алгоритмические проблемы для степенных рядов и контекстно-свободных грамматик // Докл. АН СССР. 1973. № 212. С. 50-52.
6. Safonov K. V. On power series of algebraic and rational functions in $C^n$ // J. Math. Analysis Appl. 2000. V. 243. P. 261-277.


УДК 510.52 DOI 10.17223/2226308X/14/41

# О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ ИЗОМОРФИЗМА КОНЕЧНЫХ ПОЛУГРУПП

А. Н. Рыбалов

Изучается генерическая сложность проблемы изоморфизма конечных полугрупп: по любым двум полугруппам одинакового порядка, заданным таблицами умножения, требуется определить, являются ли они изоморфными. К этой проблеме полиномиально сводится проблема изоморфизма конечных графов. Таким образом, проблема изоморфизма конечных полугрупп с вычислительной точки зрения не проще проблемы изоморфизма графов. Предлагается генерический полиномиальный алгоритм для проблемы изоморфизма конечных полугрупп. В его основе лежит характеризация почти всех конечных полугрупп как 3-нильпотентных полугрупп специального вида, а также полиномиальный алгоритм Боллобаша, решающий проблему изоморфизма для почти всех сильно разреженных графов.

**Ключевые слова:** генерическая сложность, конечные полугруппы, изоморфизм.

## Введение

Понятие изоморфизма является одним из важнейших понятий в современной математике. Изоморфные объекты имеют одинаковые математические свойства, одинаковую математическую структуру. Это позволяет абстрагироваться от конкретных представителей этих объектов, однако это также порождает проблему изоморфизма: по двум конкретным представлениям определить, являются ли они изоморфными. Наиболее известной алгоритмической проблемой такого рода является проблема

изоморфизма конечных графов. Несмотря на то, что эта проблема находится в центре внимания специалистов с 1970-х гг., до сих пор не найдено полиномиальных алгоритмов её решения. В то же время не доказана её NP-полнота. Таким образом, она может занимать промежуточное положение между проблемами из класса P и NP-полными проблемами. Проблема изоморфизма возникает для многих других конечных алгебраических объектов: групп, полугрупп, колец, полей, алгебр и т. д. Например, для конечных полей эта проблема решается тривиально: известно, что любые два конечных поля одинакового порядка изоморфны. Для конечных полугрупп ситуация гораздо сложнее. Простой алгоритм, который перебирает всевозможные биекции между полугруппами и проверяет, являются ли эти биекции изоморфизмами, работает за экспоненциальное время. Существуют ли полиномиальные алгоритмы для решения этой проблемы, неизвестно. В [1] доказано, что к этой проблеме полиномиально сводится проблема изоморфизма конечных графов. Таким образом, проблема изоморфизма конечных полугрупп с вычислительной точки зрения не проще проблемы изоморфизма конечных графов.

В рамках генерического подхода [2] алгоритмическая проблема рассматривается не на всём множестве входов, а на некотором подмножестве «почти всех» входов. Такие входы образуют генерическое множество. Понятие «почти все» формализуется введением естественной меры на множестве входных данных. С точки зрения практики алгоритмы, решающие быстро проблему на генерическом множестве, так же хороши, как и быстрые алгоритмы для всех входов.

В данной работе предлагается генерический полиномиальный алгоритм для проблемы изоморфизма конечных полугрупп. В его основе лежит характеризация почти всех конечных полугрупп как 3-нильпотентных полугрупп специального вида, установленная в [3], а также полиномиальный алгоритм Боллобаша, решающий проблему изоморфизма для почти всех сильно разреженных графов [4].

## 1. Генерические алгоритмы

Пусть $I$ – некоторое множество входов. Для подмножества $S \subseteq I$ определим *последовательность относительных плотностей*

$$P_n(S) = \frac{|S_n|}{|I_n|}, \quad n = 1, 2, 3, \ldots,$$

где $I_n$ – множество входов размера $n$; $S_n = S \cap I_n$. Заметим, что $p_n(S)$ – это вероятность попасть в $S$ при случайной и равновероятной генерации входов из $I_n$.

*Асимптотической плотностью* множества $S$ назовём верхний предел

$$p(S) = \lim_{n \to \infty} p_n(S).$$

Множество $S$ называется *генерическим*, если $p(S) = 1$, и *пренебрежимым*, если $p(S) = 0$. Очевидно, что $S$ генерическое тогда и только тогда, когда его дополнение $I \setminus S$ пренебрежимо.

Алгоритм $A$ с множеством входов $I$ и множеством выходов $J \cup \{?\}$ $(? \notin J)$ называется *генерическим*, если

1) $A$ останавливается на всех входах из $I$;
2) множество $\{x \in I : A(x) = ?\}$ является генерическим.

Генерический алгоритм $A$ вычисляет функцию $f : I \to J$, если

$$\forall_x \in I\,(A(x) = y \in J) \wedge (f(x) = y).$$

Ситуация $A(x) = ?$ означает, что $A$ не может вычислить функцию $f$ на аргументе $x$. Но условие 2 гарантирует, что $A$ корректно вычисляет $f$ на почти всех входах (входах из генерического множества). Множество $S \subset I$ называется *генерически разрешимым за полиномиальное время*, если существует генерический полиномиальный алгоритм, вычисляющий его характеристическую функцию.

## 2. Проблема изоморфизма конечных полугрупп

Для определённости будем рассматривать конечные полугруппы с элементами из множеств $\{1, 2, \ldots, n\}$, $n \in N$. *Таблицей умножения* конечной полугруппы $S$ порядка $n$ называется таблица $n \times n$, в которой на месте $(i,j)$ стоит результат произведения элементов $i$ и $j$.

Полугруппы $S_1$ и $S_2$ *изоморфны*, если существует биекция $\varphi : S_1 \to S_2$, такая, что для любых элементов $a,b \in S_1$ имеет место $\varphi(ab) = \varphi(a)\varphi(b)$. Биекция $\varphi$ называется *изоморфизмом*. *Проблема изоморфизма конечных полугрупп* состоит в следующем: даны две конечные полугруппы $S_1$ и $S_2$ одинакового порядка, заданные таблицами умножения; определить, являются ли они изоморфными.

**Теорема 1.** Проблема изоморфизма конечных полугрупп генерически разрешима за полиномиальное время.

ЛИТЕРАТУРА

1. Земляченко В. Н., Корнеенко Н. М., Тышкевич Р. И. Проблема изоморфизма графов // Записки научных семинаров ЛОМИ. 1982. Т. 118. С. 83-158.
2. Kapovich I., Miasnikov A., Schupp P., and Shpilrain V. Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665-694.
3. Kleitman D. J., Rothschild B. R., and Spencer J. H. The number of semigroups of order n // Proc. Amer. Math. Soc. 1976. V. 55. No. 1. P. 227-232.
4. Bollobas B. Distinguishing of vertices of random graphs // Ann. Discr. Math. 1982. V. 13. P. 33-50.

Секция 7

# ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.719.2 DOI 10.17223/2226308X/14/42

## ОБ ЭВРИСТИЧЕСКОМ ПОДХОДЕ К ПОСТРОЕНИЮ БИЕКТИВНЫХ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ С ЗАДАННЫМИ КРИПТОГРАФИЧЕСКИМИ ХАРАКТЕРИСТИКАМИ

М. А. Коврижных, Д. Б. Фомин

Предложен эвристический алгоритм построения биективных булевых функций с заданными криптографическими свойствами — нелинейностью и дифференциальной 5-равномерностью — на основе обобщённой конструкции. Производится поиск вспомогательных подстановок меньшей размерности в обобщённой конструкции с использованием идей спектрально-линейного и спектрально-разностного методов. Исследована возможность оптимизации вычисления криптографических характеристик на каждой итерации алгоритма. Экспериментально получены 8-битовые 6-равномерные подстановки с нелинейностью 108.

**Ключевые слова:** булева функция, подстановка, нелинейность, дифференциальная 5-равномерность.

Биективные векторные булевы функции (подстановки) используются в качестве нелинейных примитивов многих симметричных шифров. Построение подстановок размерности $n > 8$ бит с криптографическими характеристиками, гарантирующими стойкость шифров к разностному и линейному методам криптоанализа, является сложной задачей.

В [1] представлены спектрально-линейный и спектрально-разностный методы генерации подстановок, основанные на итеративном улучшении их криптографических характеристик путём умножения на транспозиции.

В [2, 3] описана обобщённая конструкция векторных булевых $(2m, 2т)$-функций, использующая мономиальные и произвольные подстановки размерности $m$. В случае $m = 4$ экспериментально найдены 768 наборов показателей степеней мономов, перспективных для построения 8-битовых 6-равномерных подстановок, имеющих нелинейность 108 и алгебраическую степень 7 при правильном выборе вспомогательных 4-битовых подстановок.

В настоящей работе предложен эвристический алгоритм поиска таких 4-битовых подстановок в обобщённой конструкции, при этом используются идеи спектрально-линейного и спектрально-разностного методов.

Обозначим: $V_n$ — n-мерное векторное пространство над полем из двух элементов $F_2$; $V_n = V_n \setminus \{0\}$; $S(V_n)$ — симметрическую группу всех подстановок пространства $V_n$; $F_{2^n}$ — конечное поле из $2^n$ элементов. Пусть $a \in V_n$, $b \in V_m$. *Конкатенацию* двух векторов будем обозначать как $a \| b \in V_{n+m}$. *Скалярным произведением* двух векторов $a, b \in V_n$ называется элемент поля $F_2$, вычисляемый по формуле $(a, b) = a_{n-1}b_{n-1} + \ldots + a_0b_0$. *Транспозиция* — это цикл длины 2. Умножение подстановки $G$ на транспозицию справа $G \circ (i_1, i_2)$ приводит к транспозиции элементов $i_1$ и $i_2$ в верхней строке

подстановки G [4, с. 51], другими словами, в нижней строке подстановки G меняются местами образы элементов $i_1$ и $i_2$.

Приведём определения некоторых криптографических характеристик подстановок.

Подстановка $F\ G\ S(V_n)$ называется *Дифференциально $J_F$-равномерной*, если

$$J_F = \max_{a \in V_n', b \in V_n} J_F(a,b),$$

где $J_F(a, b) = |\{x \in V_n : F(x + a) + F(x) = b\}|$. Значение $J_F$ называется *показателем дифференциальной равномерности* подстановки $F$.

*Таблицей распределения разностей* (Difference Distribution Table — DDT) подстановки $F$ называется такая $2^n \times 2^n$ таблица DDTF, что $DDT_F[a, b] = J_F(a, b)$. Для всех элементов $J \in \{0, 2, ..., 2^n\}$ определим множества $D_F(J) = \{(a, b) \in V_n \times V_n : J_F(a, b) = J\}$. *Разностным спектром* подстановки F называется множество пар $D_F = \{(J, |D_F(J)|)\}$.

*Преобразованием Уолша — Адамара* $W_F(a, b)$ подстановки $F \in S(V_n)$ называется отображение $W_F : V_n \times V_n \to Z$, заданное равенством

$$W_F(a, b) = \sum_{x \in V_n} (-1)^{\langle a,x\rangle + \langle b,F(x)\rangle} \text{ для любых } a, b \in V_n.$$

*Линейность* $\Delta_F$ подстановки $F$ определяется как $\Delta_F = \max_{a \in V_n, b \in V_n} |W_F(a, b)|$. *Нелинейность* $N_F$ подстановки $F$ вычисляется по формуле $N_F = 2^{n-1} - \Delta_F$.

*Таблицей линейных приближений* (Linear Approximation Table — LAT) [5] подстановки F называется такая $2^n \times 2^n$ таблица LATF, что $LAT_F[a, b] = \Delta_F(a, b)$, где

$$\Delta_F(a,b) = |\{x \in V_n : \langle a,x\rangle = \langle b,F(x)\rangle\}| - 2^{n-1} = 2W_F(a,b).$$

Для всех элементов $\Delta \in \{0, 2, \ldots, 2^{n-1}\}$ определим множества $L_F(\Delta) = \{(a, b) \in V_n \times V_\phi : |\Delta_F(a, b)| = \Delta\}$. *Линейным спектром* подстановки $F$ называется множество пар $L_F = \{(\Delta, |L_F(\Delta)|)\}$.

*Алгебраической степенью* $\deg(F)$ подстановки $F$ называется минимальная степень многочленов Жегалкина для всевозможных линейных комбинаций её координатных функций $\langle a, F(x)\rangle$ по всем $a \in V_n'$: $\deg(F) = \min_{a \in V_n} \deg(\langle a, F(x)\rangle)$.

Рассмотрим $(2m, 2т)$-функцию $F(x_1, x_2) = y_1 \| y_2$, где $x_1, x_2, y_1, y_2 \in V_m$, задаваемую следующей *обобщённой* конструкцией [2]:

$$\begin{aligned} y_1 &= G_1(x_1 + x_2) + b_1(x_2), & G_1(x_1 + x_2) &= 0, \\ y_2 &= G_2(x_1 + x_2) + b_2(x_2), & G_2(x_1 + x_2) &= 0 \end{aligned} \qquad (1)$$

В силу существования взаимно-однозначного отображения $V_m \to F_{2^m}$ в (1) и далее операции возведения в степень и умножения производятся в поле $F_{2^m}$.

Параметрами функции (1) являются набор показателей степеней $(a, в, \gamma, \delta)$ мономиальных подстановок и значения подстановок $b_1, b_2 \in S(V_m)$. Без ограничения общности будем предполагать, что

$$b_1(0) = 0, \quad b_2(0) = 0. \qquad (2)$$

Отметим, что конструкция (1) основана на структуре типа «бабочка», предложенной в [6] и полученной при изучении декомпозиции APN-подстановки Диллона [7], и

допускает T U -представление [8].

Далее исследуем обобщённую конструкцию (1) в случае $m = 4$ с одним из 768 наборов параметров $(a, в, Y, ^)$, приведённых в [3]. Поскольку подстановки $b_1$, $b_2$ в (1) выбираются независимо от параметров (a,в, Y,^), предложим эвристический алгоритм поиска таких 4-битовых подстановок $b_1$, $b_2$, чтобы итоговая 8-битовая подстановка (1) обладала заданными криптографическими характеристиками $N_F = 108$, $6_F = 6$. Вопрос о возможности получения с использованием конструкции (1) подстановок с $N_F > 108$, $8_F$ 6 6 требует дополнительного исследования.

Идея алгоритма 1 заключается в итеративном умножении начальных случайно сгенерированных 4-битовых подстановок на транспозиции и отбора среди полученных по формулам (1) 8-битовых подстановок, лучших по нелинейности, показателю дифференциальной равномерности и соответствующим значениям в линейном и разностном спектрах.

**Алгоритм 1.**

**Вход:** Подстановка $F E S (V_8)$, построенная по формулам (1) с использованием одного из 768 наборов параметров (a, в, Y, ^) [3] и произвольных 4-битовых подстановок $b_1$, $Ь_2$ (2), с криптографическими характеристиками $'_F > 40$ или $8_F > 6$.

**Параметры:** $Num\_T rans$ – количество умножений на транспозиции, $N um\_B est$ – количество отбираемых пар $(b_1,b_2)$ на каждой итерации алгоритма.

1: Сформировать список $Best$ из одной пары подстановок $(b_1,b_2)$.

2: **Для всех** пар подстановок $(Ь_1, П_2)$ из списка $Best$:

3: запомнить пару $(b_1,b_2)$ как просмотренную;

4: псевдослучайно выбрать номер $t \in \{1, 2\}$.

5: **Для** $i = 1, \ldots, Num\_T rans$

6: псевдослучайно выбрать $x,y \in Ц^x$, $x = y$, получить подстановку $b_t = b_{t^\circ}(x, y)$.

7: **Если** пара $(b_1,b_2)$ ещё не просмотрена, **то**

8: встроить $b_t$ в $F$;

9: вычислить набор характеристик подстановки $('F, 8_F, |L_F(('F/2)|, |D_F(\$_F)|)$;

10: добавить пару $(b_1,b_2)$ в список Best.

11: Отобрать (по принципу многоуровневой сортировки по возрастанию) N um_B est лучших (т. е. с меньшими значениями с учётом приоритетов) из всех наборов характеристик подстановок $F$, порождённых парами $(b_1,b_2)$ из текущего списка $Best$, считая, что в наборе приоритет убывает от $'_F$ к $|DF(6_F)|$.

12: **Если** в наилучшем наборе значения $'_F = 40$ и $6_F = 6$, **то**

13: **Вывести** подстановки $b_1, b_2$, порождающие подстановку $F$,

14: **иначе**

15: Сформировать новый список $Best$ из $Num\_Best$ пар подстановок $(b_1,b_2)$, соответствующих лучшим наборам, отобранным на шаге 11.

16: **Перейти** к шагу 2.

**Выход:** Подстановка $F \in S(V_8)$, отличающаяся от исходной только значениями подстановок $b_1$, $b_2$, такая, что

$$'_F = 40 \ (\mathrm{NF} = 108), \qquad \delta_F = 6. \tag{3}$$

Значения Num_Trans, N um_B est являются параметрами алгоритма. Вычислительные эксперименты показали, что при N um_B est = 10, Num_Trans = 500 на первой итерации и N um_T rans = 100 на последующих за приемлемое число итераций можно получить 8-битовые подстановки с характеристиками (3) и алгебраической степенью 7.

Наиболее трудоёмким этапом алгоритма является вычисление $'_F$, $\delta_F$, линейного и разностного спектров. С целью оптимизации этих вычислений теория из работы [9] применена для определения ячеек в DDT и LAT, в которых возникают изменения значений при умножении на транспозицию только 4-битовой подстановки $b_1$ или $b_2$. Асимптотические оценки трудоёмкости нахождения разностного спектра, дифференциальной равномерности, линейного спектра и линейности совпадают с приведёнными в [9]. Так, алгоритм вычисления разностного спектра и показателя дифференциальной равномерности примерно в $2^{2m}$ раз быстрее по сравнению с алгоритмом их вычисления для произвольной подстановки, а трудоёмкость алгоритма пересчёта линейного спектра и линейности примерно в $2m$ раз меньше трудоёмкости их нахождения для произвольной подстановки. По сравнению с [9] при вычислении криптографических характеристик можно получить выигрыш по памяти за счёт уменьшения числа хранимых ячеек в DDT и LAT в силу особенностей обобщённой конструкции.

ЛИТЕРАТУРА

1. Menyachikhin A. V. Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters // Матем. вопр. криптогр. 2017. Т. 8. Вып. 2. С.97-116.
2. Фомин Д. Б. О подходах к построению низкоресурсных нелинейных преобразований // Обозрение прикладной и промышленной математики. 2018. Т. 25. Вып. 4. С. 379-381.
3. Фомин Д. Б. Об алгебраической степени и дифференциальной равномерности подстановок пространства $V_{2m}$, построенных с использованием (2m, т)-функций // Матем. вопр. криптогр. 2020. Т. 11. №4. С. 133-149.
4. Кострикин А. И. Введение в алгебру. Ч. I. Основы алгебры: учебник для вузов. 3-е изд. М.: Физматлит, 2004. 272 с.
5. O'Connor L. Properties of linear approximation tables // LNCS. 1995. V. 1008. P. 131-136.
6. Biryukov A., Perrin L., and Udovenko A. Reverse-engineering the s-box of Streebog, Kuznyechik and STRIBOBr1 // LNCS. 2016. V. 9665. P. 372-402.
7. Browning K. A., Dillon J. F., McQuistan M. T., and Wolfe A. J. An APN permutation in dimension six // 9th Int. Conf. Finite Fields Appl. 2009. Contemp. Math. 2010. V. 518. P. 33-42.
8. Canteaut A. and Perrin L. On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting. Cryptology ePrint Archive, Report 2018/713. https://eprint.iacr.org/2018/713.
9. Menyachikhin A. V. The change in linear and differential characteristics of substitution after the multiplication by transposition // Матем. вопр. криптогр. 2020. Т. 11. № 2. С. 111-123.

УДК 519.688 DOI 10.17223/2226308X/14/43

## О НЕКОТОРЫХ ПОДГРУППАХ БЕРНСАЙДОВОЙ ГРУППЫ $B_0(2, 5)$

А. А. Кузнецов, А. С. Кузнецова

Пусть $B_0(2, 5) = \langle x, y \rangle$ — наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен $5^{34}$. В работе изучена серия подгрупп $H_i = \langle a_i, b_i \rangle$ группы $B_0(2, 5)$, где $a_0 = x$, $b_0 = y$, $a_i = a_{i-1}b_{i-1}$ и $b_i = b_{i-1}a_{i-1}$ для $i \in N$. Получено, что группа H является абелевой, поэтому $H_5$ — циклическая группа, и серия подгрупп прерывается. Показано, что элементы $a_4 = = xy^2xyx^2y^2x^2yxy^2x$ и $b_4 = yx^2yxy^2x^2y^2xyx^2y$ длины 16 порождают в $B_0(2, 5)$ абелеву подгруппу порядка 25, и никакие другие два групповых слова, длины которых меньше 16, не порождают нециклическую абелеву подгруппу в $B_0(2, 5)$.

**Ключевые слова:** некоммутативная криптография, группа Бернсайда.

Наиболее распространённые в настоящее время криптографические алгоритмы, такие, как RSA, Диффи — Хеллмана, на эллиптических кривых и др., зависят от структуры коммутативных групп и связаны со сложностью решения задачи факторизации целых чисел и дискретного логарифмирования. Однако в 1994 г. П. Шор представил квантовый алгоритм полиномиальной сложности, решающий эти проблемы [1]. Данный факт побудил исследователей к поиску альтернативных методов построения криптосистем. В последние два десятилетия были разработаны новые криптосистемы и протоколы обмена ключами, основанные на различных некоммутативных алгебраических системах (группы кос, полициклические группы, линейные группы и др.).

Пусть $B(m, n) = \langle x_1, \ldots, x_m \rangle$ – свободная бернсайдова группа периода $n$, в которой для любого элемента группы $g$ выполняется тождество $g^n = 1$. В работах [2-4] в качестве криптографических примитивов предложено использовать бернсайдовы группы периода $n = 3$. Для $n > 3$ вопрос пока не рассматривался. Заметим, что, помимо прикладного интереса, изучение бернсайдовых групп имеет большое значение и для алгебры, поскольку там до сих пор остаётся ряд нерешённых проблем. Например, неизвестно, конечна ли группа $B(2, 5)$.

Пусть $B_0(2, 5) = \langle x, y \rangle$ – наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен $5^{34}$ [5]. Если группа $B(2, 5)$ конечна, то $B_0(2, 5) = B(2, 5)$.

Рассмотрим подгруппы $H_i$ группы $B_0(2, 5)$ следующего вида:

$$H_i = \langle a_i, b_i \rangle,$$

где $a_0 = x$, $b_0 = y$, $a_i = a_{i-1}b_{i-1}$ и $b_i = b_{i-1}a_{i-1}$ для $i \in N$.

Обозначим $N_i$ и $E_i$ – класс нильпотентности и энгелев индекс подгруппы $H_i$ соответственно. В таблице представлены свойства групп $H_i$, полученные при помощи компьютерных вычислений.

| i | $a_i$, $b_i$ | $\lvert H_i \rvert$ | $N_i$ | $E_i$ | $H_i$ абелева? |
|---|---|---|---|---|---|
| 1 | $xy$, $yx$ | $5^{14}$ | 6 | 5 | Нет |
| 2 | $xyzx$, $yxzy$ | $5^6$ | 4 | 4 | Нет |
| 3 | $xyzxyxzy$, $yxzyxyzx$ | $5^3$ | 2 | 2 | Нет |
| 4 | $xy^2xyx^2y^2x^2yxy^2x$, $yx^2\ yxy^2\ x^2\ y^2xyx^2y$ | $5^2$ | 1 | 1 | Да |

Заметим, что группа $H_1$ уже изучена ранее [6].

Поскольку группа $H_4$ является абелевой, то $H_5$ – циклическая группа порядка 5, и серия подгрупп прерывается.

В качестве примера далее представлено коммутаторное представление (power commutator presentation) подгруппы $H_2 = \langle a_2, b_2 \rangle = \langle xy^2x, yx^2y \rangle$.

Для каждого элемента данной группы $H_2$ существует уникальное коммутаторное

представление вида $c^{*}_{1} \ldots c^{\wedge}$, где $a_i \in Z_5$, $i = 1, 2, \ldots, 6$. Здесь $c_1 = a_2$ и $c_2 = b_2$ — порождающие элементы $H_2$; $c_3, c_4, c_5, c_6$ — коммутаторы, которые вычисляются рекурсивно через $c_1$ и $c_2$:

$c_5^5 = 1$ (1 6 i 6 6), $[c_2, c_1] = c_3$, $[c_3, c_1] = c_4$, $[c_3, c_2] = c_5$, $[c_4, c_1] = c_6$,
$[c_4, c_2] = 1$, $[c_4, c_3] = 1$, $[c_5, c_1] = 1$, $[c_5, c_2] = c_6^4$, $[c_5, c_3] = 1$, $[c_5, c_4] = 1$,
$[c_6, c_1] = 1$, $[c_6, c_2] = 1$, $[c_6, c_3] = 1$, $[c_6, c_4] = 1$, $[c_6, c_5] = 1$.

Для быстрого умножения элементов на основе алгоритма из [7] вычислены полиномы Холла группы $H_2$.

Пусть $d_? \ldots c^{\wedge}$ и $c^{e_1} \ldots c^{e_6}$ — два произвольных элемента из $H_2$. Тогда

$$C_T \ldots \quad c_a \cdot c_в \ldots \quad c_в = c_{Y_1} \ldots \quad c_Y, \quad a_i, e_i, \quad Y_i \in Z_5,$$

где

$Y_1 = a_1 + A$, $Y_2 = a_2 + B_2$,
$Y_3 = a_3 + B_3 + a_2 B_1$,
$Y_4 = a_4 + B_4 + 2\ 2\ j\ a_2 + a_3 B_1$,

$Y_5 = a_5 + B_5 + (2)\ B_1 + a_3 B_2 + a_2 e_1 e_2$,

$Y_e = a_6 + B_6 + \wedge 2\ \wedge a_3 + \wedge 3\ j a_2 + 4\wedge 3\ j\ B_1 + 4\ f\ 2)a_3 + a_4 B_1 + 4a_5 B_2 + 4 + 4\wedge 2\ a_2 B_1$. $\binom{\alpha_2}{2} B_1 B_2 +$

Заслуживает внимания также тот факт, что элементы

$$a_4 = xy^2xyx^2y^2x^2yxy^2x,\ b_4 = yx^2yxy^2x^2y^2xyx^2y$$

порождают в $B_0(2, 5)$ абелеву подгруппу порядка 25. Длина каждого из этих элементов равна 16. При помощи компьютерных вычислений проведена проверка, которая показала, что никакие другие два групповых слова, длины которых меньше 16, не порождают нециклическую абелеву подгруппу в $B_0(2, 5)$.

ЛИТЕРАТУРА

1. Shor P. Algorithms for quantum computation: Discrete logarithms and factoring // Proc. 35th Ann. Symp. Foundations Comput. Sci. 1994. P. 124-134.
2. Baumslag G., Fazio N., Nicolosi A. R., et al. Generalized learning problems and applications to non-commutative cryptography // LNCS. 2011. V. 6980. P. 324—339.
3. Fazio N., Iga K., Nicolosi A. R., et al. Hardness of learning problems over Burnside groups of exponent 3 // Designs, Codes Cryptogr. 2015. V. 75(1). P. 59—70.
4. Kahrobaei D. and Noce M. Algorithmic problems in Engel groups and cryptographic applications // Intern. J. Group Theory. 2020. V. 9(4). P. 231—250.
5. Havas G., Wall G., and Wamsley J. The two generator restricted Burnside group of exponent five // Bull. Austral. Math. Soc. 1974. No. 10. P. 459—470.
6. Кузнецов А. А. Об одной подгруппе бернсайдовой групы $B_0(2, 5)$ // Тр. Института математики и механики УрО РАН. 2011. Т. 17. № 4. С. 176-180.
7. Кузнецов А. А., Кузнецова А. С. Быстрое умножение элементов в конечных двупорож- дённых группах периода пять // Прикладная дискретная математика. 2013. № 1(19). С. 110-116.

УДК 004.4 DOI 10.17223/2226308X/14/44

## DPLL-ПОДОБНЫЙ РЕШАТЕЛЬ ЗАДАЧИ ВЫПОЛНИМОСТИ НАД СИСТЕМОЙ УРАВНЕНИЙ В АНФ[XXI]

А. В. Ткачев, К. В. Калгин

[XXI]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) и лаборатории

Описаны SAT-решатель, использующий системы булевых уравнений в алгебраической нормальной форме (АНФ) для внутреннего представления задачи, и особенности реализации типичных для SAT-решателей методик для работы с таким представлением. Приводится сравнение данного решателя с рядом классических SAT-решателей при решении некоторых задач криптоанализа (как, например, атака «guess-and-determine» на потоковый шифр Grain).

**Ключевые слова:** *SAT-решатель, АНФ, криптоанализ, потоковые шифры.*

Сложные задачи из совершенно различных областей, таких, как проектирование электронных схем или криптоанализ, могут быть представлены в виде задач выполнимости булевых формул (SAT) в конъюнктивной нормальной форме (КНФ). Для эффективного решения SAT существуют и активно развиваются специализированные инструменты — SAT-решатели.

SAT в своей изначальной формулировке подразумевает представление в КНФ, и ещё в 1971г. было доказано, что данная задача является NP-полной [1]. Современные SAT-решатели обрабатывают задачи, представленные в КНФ (чаще всего записанные в текстовом формате DIMACS).

Однако для некоторых задач — например криптоанализа шифров — «естественным» представлением является АНФ. А потому не менее естественным кажется желание использовать инструмент, напрямую работающий с АНФ. Авторам не удалось обнаружить такого инструмента, равно как и обоснования, что он был бы неэффективным, и потому было решено разработать его самостоятельно. Ближайшим аналогом можно назвать проект Bosphorus [2], использующий представление в АНФ в дополнение к решению задачи в КНФ.

Для удобства решатель работает не с одной большой формулой в АНФ, а с системой уравнений в АНФ, то есть конъюнкцией множества отдельных АНФ с общим набором неизвестных.

## 1. Конструкция решателя

Постановка задачи: для данной системы уравнений в АНФ выяснить, имеет ли она решение, и если да, то найти одно из них.

Разработанная программа разделена на модули, которые можно отключать независимо друг от друга, чтобы можно было исследовать, какие алгоритмы, методики и эвристики дают наибольший вклад в ускорение решения и насколько эффективно они работают вместе (подобное исследование для классических SAT-решателей проводилось в [3]). По структуре решатель напоминает классический SAT-решатель, основанный на алгоритме DPLL, а реализованные модули — адаптированные под АНФ модификации этого алгоритма.

**Распространение констант.** Как и в классическом DPLL, одним из базовых этапов работы решателя является вывод значений переменных после означивания очередной переменной. В ходе этого этапа находятся уравнения, которые после подстановки означенных переменных становятся тривиальными, и вычисляются значения новых переменных. Просмотр уравнений продолжается до тех пор, пока удаётся делать выводы значений переменных. Если в ходе этого этапа выявляется конфликт, это означает, что текущие значения переменных неверны, и происходит откат всех выводов и предшествующего им означивания переменной в DPLL, а затем DPLL продолжает работу, пытаясь означить переменные по-другому. Ввиду представления ограничений в АНФ многие уравнения могут быстро становиться

криптографии JetBrains Research.

тривиальными — если хотя бы одна переменная в мономе равна нулю, то и весь моном равен нулю, и нужно рассматривать только ненулевые мономы, часть переменных в которых уже может быть означена.

**Распространение синонимов.** Помимо простого вывода значений отдельных переменных, из ограничений в АНФ при определённых обстоятельствах можно сделать вывод, что две переменные должны иметь одинаковые или противоположные значения. Это может сокращать количество неизвестных в обрабатываемых уравнениях, что позволяет быстрее обнаружить конфликт. Такие выводы не требуют каких-либо сложных структур или вычислений. Рассмотрим такое ограничение: $abx + bcx + acx + y = 1$. Если $a = b = c = 1$, то после упрощения ограничение будет иметь вид $x + x + x + y = 1$, что эквивалентно $x + y = 1$, и несложно сделать вывод, что значения $x$ и $y$ должны быть противоположными. Тогда можно объявить $y$ «антонимом» $x$ и при просмотре других ограничений подставлять вместо $y$ отрицание $x$, снижая таким образом число неизвестных в этом ограничении и ещё больше упрощая его.

**Отслеживаемые мономы (2WM).** По аналогии с Watched Literals (2WL) при работе с КНФ, при обработке ограничений в АНФ можно поддерживать структуру «отслеживаемых» частей уравнений. Если в КНФ это отдельные литералы, изменение значений которых может приводить к изменению значения всего дизъюнкта, то в АНФ такой частью является отдельный моном, от значения которого зависит значение всего полинома. Данная эвристика ограничивает число полиномов, которые нужно просмотреть при изменении значения переменной, что позволяет сократить общее время работы решателя, но при этом гарантирует, что «важные» полиномы (которые действительно могут измениться при изменении значения переменной) не будут пропущены.

**Упрощение уравнений перед обработкой.** Прежде чем запустить DPLL, решатель подставляет известные значения переменных (если таковые имеются, то есть заданы с помощью уравнений вида $x = \mathrm{const}$) во все уравнения и выводит значения других переменных, а также находит синонимы, если это возможно. Эта процедура повторяется до тех пор, пока не останется переменных, значения которых можно вывести и подставить. Упрощенные таким способом уравнения становятся короче и потому обрабатываются немного быстрее. В некоторых случаях возможно доказать невыполнимость или даже вывести значения всех переменных исключительно в ходе этой процедуры, без запуска DPLL.

**Порядок выбора переменной.** Порядок, в котором выбирается следующая переменная для означивания в алгоритме DPLL, может иметь значительное влияние на время работы решателя. Хотя в разработанном решателе пока можно задать только один из нескольких простых порядков выбора — например, отсутствует выбор переменной на основе «активности», которая подсчитывается в ходе работы решателя на основе частоты встречаемости переменной, возможность смены порядка в него заложена. По умолчанию решатель выбирает неозначенную переменную с наименьшим порядковым номером.

## 2. Результаты сравнения

Приведём результаты тестирования современных решателей lingeling, cryptominisat5 и представленного в работе решателя на задаче восстановления части ключа (атака «guess-and-determine» [4]) потокового шифра Grain [5]. Атака заключается в том, что часть неизвестных бит фиксируется и эти биты означиваются тем или иным образом («угадываются»), а затем с помощью SAT-решателя вычисляются

значения оставшихся неизвестных бит или выявляется, что при таких значениях зафиксированных бит шифр не мог сгенерировать известную гамму, и тогда выбираются другие значения зафиксированных бит. В общем случае при фиксации $k$ бит из $n$ неизвестных потребуется рассмотреть $2^k$ задач, а время такой атаки можно оценить как $2^k T$, где $T$ – среднее время работы SAT-решателя на одной задаче, в которой $\kappa$ из $n$ бит означены.

Обычно рассматриваются два варианта восстановления начального состояния – задача восстановления ключа, когда известна вся гамма, и задача восстановления состояния регистров, когда гамма известна с какого-то произвольного момента времени. Первую задачу будем обозначать «init=yes», а вторую – «init=no». В шифре Grain из- за фазы инициализации в случае «init=yes» получаются более сложные уравнения, описывающие зависимости значений генерируемых бит ключевого потока от исходных бит ключа, но неизвестными считаются только 80 бит ключа. В случае «init=no» биты гаммы генерируются сразу из некоторого состояния и уравнения получаются более простыми, но неизвестными считаются все 160 бит состояния регистров. Атаки на подобные шифры в различных режимах проводились в [6, 7].

Эксперименты показали, что в случае «init=no» классические и разработанный решатель ведут себя схожим образом, и разработанный решатель лишь незначительно проигрывает классическим по времени решения задач. Однако в случае «init=yes» классические решатели серьёзно уступают разработанному. Некоторые решатели не справляются с задачами такого типа, даже если неизвестно всего 1-2 бита – вероятно, решатель «запутывается» среди множества промежуточных переменных и начинает выбирать их вместо «важных» переменных, соответствующих битам ключа.

На рис. 1 показаны оценки времени атаки для разных решателей. Видно, что при использовании разработанного решателя время остаётся более-менее стабильным при увеличении числа неизвестных бит, в то время как для классических решателей время атаки поначалу снижается, но после некоторого значения начинает возрастать, при этом оценка времени выше. В случае «init=no» общее число неизвестных больше и время полной атаки гораздо выше ($10^{30}$ ч против $10^{17}$ в случае «init=yes»), поэтому проводить атаку с применением SAT-решателей в этом режиме нецелесообразно.

В дальнейшем планируется провести исследование на большем числе шифров и SAT-решателей. Однако уже из проведённого сравнения понятно, что разработка решателя, использующего представление уравнений в АНФ, перспективна.

Планируется выяснить, с чем связано то, что современные решатели уступают по времени представленному в работе на порядок и больше. Вероятно, замедление классических решателей может быть связано с неудачными эвристиками выбора порядка, в котором означиваются биты. Это означает, что перспективной является разработка новых эвристик как для решателей, использующих представление уравнений в КНФ, так и для представленного в работе. Другая версия – неэффективность работы эвристики clause learning (обучение и пополнение базы конъюнкций) современных решателей на рассматриваемой задаче.

Помимо этого, необходимо изучить применимость других алгоритмов и методик, использующихся в классических решателях, к решателю, основанному на АНФ. На-

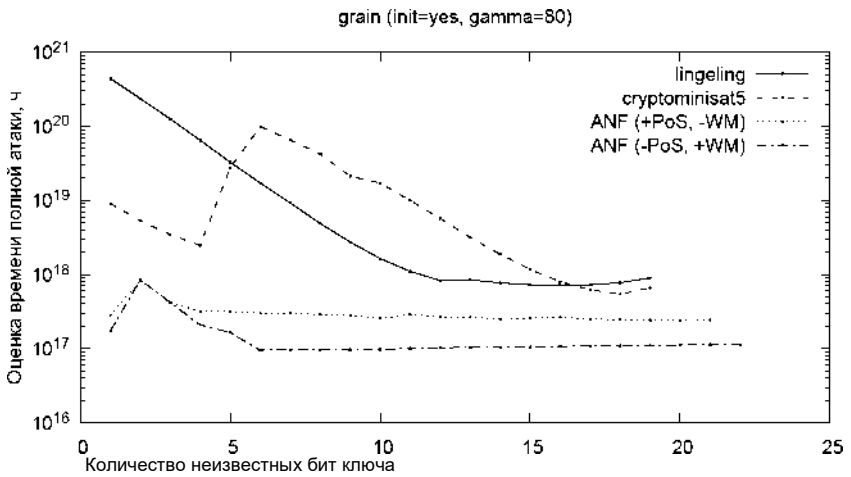



Рис. 1. Оценка времени полной атаки в зависимости от количества неизвестных бит

пример, насколько эффективен clause learning при работе с КНФ и можно ли его адаптировать к АНФ. Возможно, следует использовать другие методы — например, добавление новых уравнений, подобно тому, как это делается в алгебраических атаках.

ЛИТЕРАТУРА

1. Cook S. The complexity of theorem-proving procedures // 3rd Ann. ACM Symp. Theory Comput. 1971. P. 151-158.
2. Choo D., Soos M., Chai K. M. A., and Meel K. S. BOSPHORUS: Bridging ANF and CNF solvers // Proc. DATE Conf. Exhibition. 2019. P. 468-473.
3. Katebi H., Sakallah K., and Silva J. Empirical study of the anatomy of modern SAT Solvers // LNCS. 2011. V. 6695. P. 343-356.
4. Bard G. V. Algebraic Cryptanalysis. Springer, 2009.
5. Hell M., Johansson T., and Meier W. Grain: A stream cipher for constrained environments // Intern. J. Wireless Mobile Comput. 2007. No. 2. P. 86-93.
6. Yeo S., Le D. P., and Khoo K. Improved algebraic attacks on lightweight block ciphers // J. Cryptogr. Eng. 2011. No. 11. P. 1-19.
7. Semenov A. A. and Zaikin O. S. Algorithm for finding partitionings of hard variants of Boolean satisfiability problem with application to inversion of some cryptographic functions // SpringerPlus. 2016. Art. No. 554. P. 1-16.

# СВЕДЕНИЯ ОБ АВТОРАХ

АБРОСИМОВ Михаил Борисович — доктор физико-математических наук, доцент, заведующий кафедрой теоретических основ компьютерной безопасности и криптографии Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов. E-mail: mic@rambler.ru

АГИЕВИЧ Сергей Валерьевич — кандидат физико-математических наук, заведующий НИЛ проблем безопасности информационных технологий НИИ прикладных проблем математики и информатики Белорусского государственного университета, г. Минск. E-mail: agievich@bsu.by АНТОНОВ Кирилл Валентинович — магистрант ИИКС МИФИ, г. Москва.

E-mail: aknitr@mail.ru

АТУТОВА Наталья Дмитриевна — студентка механико-математического факультета Новосибирского государственного университета, исследователь лаборатории криптографии JetBrains Research, г. Новосибирск. E-mail: atutova.n@yandex.ru

АХМЕТЗЯНОВА Лилия Руслановна — заместитель начальника отдела криптографических исследований ООО «КРИПТО-ПРО», г. Москва. E-mail: lah@cryptopro.ru

АХТЯМОВ Данил Айдарович — студент Еврейского университета, г. Иерусалим.

E-mail: akhtyamoff1997@gmail.com

БАБУЕВА Александра Алексеевна — инженер-аналитик 1 категории ООО «КРИПТО-ПРО», г. Москва. E-mail: babueva@cryptopro.ru

БАХАРЕВ Александр Олегович — студент Новосибирского государственного университета, исследователь лаборатории криптографии JetBrains Research, г. Новосибирск.

E-mail: sana.bakharev@gmail.com

БЕРДНИКОВА Наталья Юрьевна — студентка Национального исследовательского Томского государственного университета, г. Томск. E-mail: nickiskit@gmail.com

БОБРОВСКИЙ Дмитрий Александрович — старший системный аналитик ООО «Код Безопасности», г. Москва.

E-mail: d.bobrovskiy@securitycode.ru

БОЛТНЕВ Юрий Федорович — старший преподаватель Института физико-математических наук и информационных технологий Балтийского федерального университета им. И. Канта, г. Калининград. E-mail: yuri.boltnev@gmail.com

БОНИЧ Татьяна Андреевна — студентка Новосибирского государственного университета, г. Новосибирск. E-mail: t.bonich@g.nsu.ru

ГЕУТ Кристина Леонидовна — старший преподаватель Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: geutkrl@yandex.ru

ГРИБАНОВА Ирина Александровна — младший научный сотрудник ИДСТУ СО РАН, г. Иркутск. E-mail: the42dimension@gmail.com

ДЕВЯНИН Петр Николаевич — доктор технических наук, профессор, член-корреспондент Академии криптографии Российской Федерации, научный руководитель ООО «РусБИТех-Астра», г. Москва. E-mail: pdevyanin@astralinux.ru

ЕГОРУШКИН Олег Игоревич — кандидат физико-математических наук, доцент Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск. E-mail: olegegoruschkin@yandex.ru

ЕЛ КАЛФАУИ Сабира — постдокторант Института Бойяи Сегедского университета, г. Сегед, Венгрия. E-mail: sabiraelkhalfaoui@gmail.com

ЖАНТУЛИКОВ Булат Фаритович — студент Новосибирского государственного университета, г. Новосибирск. E-mail: b.zhantulikov@g.nsu.ru

ЖАРКОВА Анастасия Владимировна — кандидат физико-математических наук, доцент кафедры теоретических основ компьютерной безопасности и криптографии Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов.
E-mail: ZharkovaAV3@gmail.com

ЗАДОРОЖНЫЙ Дмитрий Игоревич — руководитель службы сертификации, ИБ и криптографии ООО «Код Безопасности», г. Москва. E-mail: d.zadorozhny@securitycode.ru

ЗЮБИНА Дарья Александровна — студентка факультета информационных технологий НГУ, исследователь лаборатории криптографии JetBrains Research, г. Новосибирск.
E-mail: zyubinadarya@gmail.com

ИЩУКОВА Евгения Александровна — кандидат технических наук, доцент кафедры безопасности информационных технологий, Южный федеральный университет, г. Таганрог.
E-mail: uaishukova@sfedu.ru

КАЛГИН Константин Викторович — кандидат физико-математических наук, старший преподаватель Новосибирского государственного университета, младший научный сотрудник Института вычислительной математики и математической геофизики СО РАН, г. Новосибирск.
E-mail: kalginkv@gmail.com

КОВРИЖНЫХ Мария Антоновна — выпускница Национального исследовательского университета «Высшая школа экономики», г. Москва. E-mail: makovrizhnykh@gmail.com

КОЛБАСИНА Ирина Валерьевна — старший преподаватель Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск.
E-mail: kabaskina@yandex.ru

КОЛЕГОВ Денис Николаевич — кандидат технических наук, доцент, доцент кафедры компьютерной безопасности Томского государственного университета, г. Томск.
E-mail: dnkolegov@gmail.com

КОЛОМЕЕЦ Николай Александрович — кандидат физико-математических наук, научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск.
E-mail: kolomeec@math.nsc.ru

КОНДЫРЕВ Дмитрий Олегович — аспирант факультета информационных технологий Новосибирского государственного университета, исследователь лаборатории крипторафии JetBrains Research, младший научный сотрудник Института математики им. С. Л. Соболева, г. Новосибирск. E-mail: dkondyrev@gmail.com

КОРЕНЕВА Алиса Михайловна — кандидат физико-математических наук, начальник отдела ООО «Код Безопасности», г. Москва. E-mail: a.koreneva@securitycode.ru

КОРЯКИН Илья Алексеевич — аспирант Новосибирского государственного университета, г. Новосибирск. E-mail: ed4140@gmail.com

КОСОЛАПОВ Юрий Владимирович — кандидат технических наук, доцент Южного федерального университета, г. Ростов-на-Дону. E-mail: itaim@mail.ru

КУЗНЕЦОВ Александр Алексеевич — доктор физико-математических наук, профессор, директор Института космических исследований и высоких технологий Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнева, г. Красноярск.
E-mail: alex_kuznetsov80@mail.ru

КУЗНЕЦОВА Александра Сергеевна — кандидат физико-математических наук, доцент кафедры информационных технологий и математического обеспечения информационных систем Красноярского государственного аграрного университета, г. Красноярск.
E-mail: alexakuznetsova85@gmail.com

КУЦЕНКО Александр Владимирович — аспирант механико-математического факультета Новосибирского

государственного университета, м.н.с. Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: alexandrkutsenko@bk.ru

КЯЖИН Сергей Николаевич — кандидат физико-математических наук, руководитель проектов Лаборатории блокчейн, Сбербанк России, г. Москва. E-mail: blockchain-research@sberbank.ru ЛЕБЕДЕВ Владимир Витальевич — студент Национального исследовательского Томского государственного университета, г. Томск. E-mail: d3fl4t3@gmail.com

ЛЕБЕДЕВ Роман Константинович — аспирант Новосибирского государственного университета, г. Новосибирск. E-mail: n0n3m4@gmail.com

ЛЕЛЮК Евгений Андреевич — аспирант Южного федерального университета, г. Ростов-на-Дону. E-mail: lelukevgeniy@mail.ru

ЛЕОНОВА Мария Александровна — старший научный сотрудник ООО «РусБИТех-Астра», г. Москва. E-mail: mleonova@astralinux.ru

ЛОБОВ Александр Андреевич — аспирант Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов. E-mail: aisanekai@mail.ru МАРО Екатерина Александровна — кандидат технических наук, доцент кафедры безопасности информационных технологий Южного федерального университета, г. Таганрог.
E-mail: marokat@gmail.com

МЕДВЕДЕВА Наталья Валерьевна — кандидат физико-математических наук, доцент, доцент Уральского государственного университета путей сообщения, г. Екатеринбург.
E-mail: medvedeva_n_v@mail.ru

МЕЖЕННАЯ Наталья Михайловна — кандидат физико-математических наук, доцент, доцент кафедры прикладной математики Московского государственного технического университета им. Н. Э. Баумана, г. Москва. E-mail: natalia.mezhennaya@gmail.com

МИХАЙЛОВ Владимир Гаврилович — доктор физико-математических наук, ведущий научный сотрудник отдела дискретной математики Математического института им. В. А. Стеклова Российской Академии Наук, г. Москва. E-mail: mikhail@mi-ras.ru

МУХА Ники — Ph.D., сотрудник компании Strativia, г. Ларго, Мэриленд. E-mail: nicky@mouha.be НАБИЕВ Тимур Русланович — программист ООО «Код Безопасности», г. Москва.
E-mail: t.nabiev@securitycode.ru

НАБОКОВ Денис Алексеевич — научный сотрудник компании QApp, Сколково, г. Москва.
E-mail: nabokov.da@yandex.ru

НАДЬ Габор Петер — профессор, доктор математических наук, заведующий кафедрой алгебры Будапештского университета технических и экономических наук, г. Будапешт, Венгрия.
E-mail: nagygp@math.bme.hu

НЕДЯК Мария Сергеевна — разработчик системных модулей ООО «БИЗОН», г. Томск.
E-mail: mashanedyak@gmail.com

НИКОЛАЕВ Антоний Анатольевич — аспирант Национального исследовательского Томского государственного университета, г. Томск. E-mail: antoniynikolaev@gmail.com

НИКУЛИН Владимир Сергеевич — аспирант Новосибирского государственного университета экономики и управления «НИНХ», г. Новосибирск. E-mail: nikulin-94@inbox.ru

НОВОСЕЛОВ Семен Александрович — старший преподаватель Института физико-математических наук и информационных технологий Балтийского федерального университета им. И. Канта, г. Калининград. E-mail: snovoselov@kantiana.ru

ОСИПОВ Вадим Александрович — выпускник Балтийского федерального университета им. И. Канта, г. Калининград. E-mail: vadimosipov24@gmail.com

ПАНКОВ Константин Николаевич — кандидат физико-математических наук, старший научный сотрудник отдела НИО-48, и.о. заведующего кафедрой Московского технического университета связи и информатики, эксперт ТК-159 и ISO 307, г. Москва. E-mail: k.n.pankov@gmail.com

ПАНКРАТОВА Ирина Анатольевна — кандидат физико-математических наук, доцент, заведующая

лабораторией компьютерной криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: pank@mail.tsu.ru

ПАНТЕЛЕЕВ Роман Игоревич — аспирант кафедры теоретических основ компьютерной безопасности и криптографии Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов. E-mail: PanteleevRmn95@gmail.com ПАНФЕРОВ Матвей Андреевич — студент Новосибирского государственного университета, г. Новосибирск. E-mail: m.panferov@g.nsu.ru

ПОГОРЕЛОВ Борис Александрович — доктор физико-математических наук, профессор, действительный член Академии криптографии Российской Федерации, г. Москва.

ПОПОВ Владимир Александрович — технический директор Лаборатории блокчейн, Сбербанк России, г. Москва. E-mail: blockchain-research@sberbank.ru

ПУДОВКИНА Марина Александровна — доктор физико-математических наук, профессор кафедры информационной безопасности Московского государственного технического университета им. Н. Э. Баумана, г. Москва. E-mail: maricap@rambler.ru

РАЗУМОВСКИЙ Петр Владимирович — аспирант Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов.

E-mail: shprotby@gmail.com

РОМАНЬКОВ Виталий Анатольевич — доктор физико-математических наук, профессор, профессор Омского государственного университета им. Ф. М. Достоевского, г. Омск; главный научный сотрудник Сибирского федерального университета, г. Красноярск. E-mail: romankov48@mail.ru РЫБАЛОВ Александр Николаевич — кандидат физико-математических наук, старший научный сотрудник лаборатории комбинаторных и вычислительных методов алгебры и логики Института математики им. С. Л. Соболева СО РАН, г. Омск. E-mail: alexander.rybalov@gmail.com САФОНОВ Константин Владимирович — доктор физико-математических наук, профессор, заведующий кафедрой Сибирского государственного университета науки и технологий имени академика М. Ф. Решетнёва, г. Красноярск. E-mail: safonovkv@rambler.ru

СЕМЁНОВ Александр Анатольевич — кандидат технических наук, доцент, ведущий научный сотрудник ИДСТУ СО РАН, г. Иркутск. E-mail: biclop.rambler@yandex.ru

СУТОРМИН Иван Александрович — младший научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: ivan.sutormin@gmail.com

ТИТОВ Сергей Сергеевич — доктор физико-математических наук, профессор Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: stitov@usaaa.ru

ТИТОВА Ксения Максимовна — студентка Новосибирского государственного университета, г. Новосибирск. E-mail: sitnich@gmail.com

ТКАЧЕВ Александр Витальевич — аспирант Новосибирского государственного университета, г. Новосибирск. E-mail: alexander@tkachov.ru

ТОКАРЕВА Наталья Николаевна — кандидат физико-математических наук, старший научный сотрудник Института математики им. С. Л. Соболева СО РАН, доцент НГУ, заведующая лабораторией криптографии JetBrains Research, г. Новосибирск. E-mail: tokareva@math.nsc.ru ТУРЧЕНКО Олег Юрьевич — аспирант Южного федерального университета, г. Ростов-на-Дону. E-mail: olegmmcs@gmail.com

ФИЛИППОВ Степан Дмитриевич — студент Санкт-Петербургского государственного университета, г. Санкт-Петербург. E-mail: filippowstepan@yandex.ru

ФОМИН Денис Бонославович — старший преподаватель Национального исследовательского университета «Высшая школа экономики», г. Москва. E-mail: dfomin@hse.ru

ФОМИЧЁВ Владимир Михайлович — доктор физико-математических наук, профессор, научный консультант службы сертификации, ИБ и криптографии ООО «Код Безопасности», профессор Финансового университета при Правительстве РФ, ведущий научный сотрудник ФИЦ ИУ РАН, г. Москва. E-mail: fomichev.2016@yandex.ru

ХАЛНИЯЗОВА Юлия Ринатовна — разработчик-исследователь криптографических сервисов, компания BI.ZONE, г. Томск. E-mail: yulia.khalniyazova@gmail.com

ЧЕРЕМУШКИН Александр Васильевич — доктор физико-математических наук, член- корреспондент Академии криптографии РФ, г. Москва. E-mail: avc238@mail.ru

ШАПОРЕНКО Александр Сергеевич — м.н.с. Института математики им. С. Л. Соболева СО РАН, аспирант Новосибирского государственного университета, исследователь лаборатории криптографии JetBrains Research, г. Новосибирск. E-mail: a.shaporenko@g.nsu.ru

# АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ

## SECTION 1

Boltnev Y. F., Novoselov S. A., Osipov V. A. **ON CONSTRUCTION OF MAXIMAL GENUS 3 HYPERELLIPTIC CURVES.** We describe two methods of contructing genus 3 maximal hyperelliptic curves of type $y^2 = x^7 + ax^4 + bx$ over a finite field. We consider the case when b is a cubic residue in this field. In this case the Jacobian of the curve decomposes into three elliptic curves. The first method is based on finding a pair of supersingular elliptic curves over a prime field. One of the curves in the pair is chosen to have j-invariant equal to 0 or 1728. The j-invariant of the second elliptic curve can be computed from the j-invariant of the first curve using an explicit formula. After finding the pair, the maximal genus 3 curve is constructed over a suitable extension of the finite field. This method does not allow us to enumerate all maximal curves, but gives a very efficient algorithm for the family of maximal curves. The second method is based on factorization of the Legendre polynomials, which are Hasse invariants of the elliptic curves in the Jacobian decomposition. Using this method, we construct all possible maximal hyperelliptic curves over $F_{p^2}$ for a 6= 0, b = 1 and p 6 7151.

**Keywords:** maximal hyperelliptic curve, supersingular elliptic curve, characteristic polynomial.

Mezhennaya N. M., Mikhailov V. G. **CENTRAL LIMIT THEOREM FOR U- STATISTICS OF TUPLES OF VERTEX LABELS ON A COMPLETE GRAPH.** In a complete graph with vertices 1, 2, . . . , n, the vertices 2, 3, . . . , n are provided with independent random labels taking values in the finite set $A_N$. Consider the set of all chains of s adjacent edges, each of which leaves vertex 1 and does not pass through the same vertex twice. Each chain corresponds to an s-tuple of random labels of the passed vertices. In this paper, we consider the U -statistics $U_k(s)$ with a kernel depending on the k of such s-tuples. The number k > 2 is considered to be fixed, but s > 1 can change. It has been proved that a sufficient condition for the asymptotic normality of $U_k(s)$ (under ordinary standardization) is a condition of the form $\mathbf{D}U_k(s) > Cn^{2(ks\ 1)+\kappa}$, where $C, \kappa > 0$. **Keywords:** U -statistic, central limit theorem, complete graph, tuple, random labels

Fomichev V. M. **ON THE LARGEST ORDER OF SUBSTITUTIONS OF A GIVEN DEGREE.** A necessary requirement for an encryption system is a sufficiently large order of the group associated with the cipher (i.e., generated by the cipher substitution). In this regard, the value of ^(n) that estimates the orders of cyclic substitution groups of degree n, including cyclic groups generated by cipher substitutions, is of interest. It is known that the order of a substitution is equal to the lowest common multiple of its cycle lengths. However, function ^(n), defined as the dependence of the largest order value among all permutations of degree n, is poorly studied. The monotonicity of function ^(n) is shown, and a two-sided estimate of its values is obtained: $П_{Ц_n)}$ 6 ^(n) 6 I"^2(n — 1) 1!, where $П_{Ц_n}$ is the greatest value of the product of prime numbers, the sum of which is not greater than n. An asymptotic estimate of the lower bound for large n is obtained: ^(n) > 224k!(1,665)$_k$(lnk)$^{(k-15)/2}$ for any n > 1000 and $k$ = ^p2n/lnnj.

**Keywords:** order of a substitution, cycle structure, prime number.

## SECTION 2

Atutova N. D. **HYBRID APPROACH TO THE SEARCH FOR BOOLEAN FUNCTIONS**

**WITH HIGH ALGEBRAIC IMMUNITY BASED ON HEURISTICS.** Currently, one of the most promising and developing methods for analyzing ciphers is algebraic cryptanalysis. In order to provide resilience to such type of attack, it is necessary to use Boolean functions with high algebraic immunity in constructing components of block and stream ciphers. The paper proposes a combined approach to the search for Boolean functions with high algebraic immunity based on heuristic methods, in particular, the genetic algorithm and the Hill Climbing algorithm. Computational experiments for Boolean functions in n 6 8 variables demonstrate the effectiveness of the proposed approach.

**Keywords:** genetic algorithm, Hill Climbing algorithm, algebraic immunity, nonlinearity, heuristics.

Zyubina D. A., Tokareva N. N. **S-BLOCKS WITH MAXIMUM COMPONENT ALGEBRAIC IMMUNITY ON A SMALL NUMBER OF VARIABLES.** Let n be a permutation on n elements, f be a Boolean function in n variables. Define a vector Boolean function $F_n : F_n \wedge F_n$ as $F_n(x) = (f(x), f(n(x)), \bullet\bullet\bullet, f(n^{n-1}(x)))$. In this paper, we study the component algebraic immunity of the vector Boolean function $F_n$ as a function of the Boolean function $f$ and the permutation n for n = 3, 4,5. We obtain complete sets of Boolean and, partly, vector Boolean functions with maximum algebraic immunity in 3, 4 and 5 variables. If the function $F_n$ has maximum algebraic immunity, then the permutation n is full cycle.

**Keywords:** Boolean function, vector Boolean function, algebraic immunity, component algebraic immunity.

Kutsenko A. V. **ON SOME PROPERTIES OF SELF-DUAL GENERALIZED BENT FUNCTIONS.** Bent functions of the form $F_n \wedge Z_q$, where $q > 2$ is a positive integer, are known as generalized bent (gbent) functions. A gbent function for which it is possible to define a dual gbent function is called regular. A regular gbent function is said to be self-dual if it coincides with its dual. We obtain the necessary and sufficient conditions for the self-duality of gbent functions from Eliseev — Maiorana — McFarland class. We find the complete Lee distance spectrum between all self-dual functions in this class and obtain that the minimal Lee distance between them is equal to $q \bullet 2^{n-3}$. For Boolean case, there are no affine bent functions and self-dual bent functions, while it is known that for generalized case affine bent functions exist, in particular, when q is divisible by 4. We prove the non-existence of affine self-dual gbent functions for any natural even q. A new class of isometries preserving self-duality of a gbent function is presented. Based on this, a refined classification of self-dual gbent functions of the form $F_2 \wedge Z_4$ is given.

**Keywords:** self-dual bent function, generalized bent function, Eliseev — Maiorana — McFarland bent function, Lee distance.

Mouha N., Kolomeec N. A., Ahtyamov D. A., Sutormin I. A., Panferov M. A., Titova K. M., Bonich T. A., Ishchukova E. A., Tokareva N. N., Zhantulikov B. F **ON PROPERTIES OF ADDITIVE DIFFERENTIAL PROBABILITIES OF XOR.** The additive differential probability of exclusive-or $adp_{\oplus}(a, в, Y)$, where a,e,$Y \wedge Z_n$, is studied. It is used in the analysis of symmetric-key primitives that combine XOR and modular addition, such as Addition-Rotation-XOR (ARX) constructions. We focus on the maximal differentials which are helpful when constructing differential trails. It is proven that

maxadp⊕(a,e, Y) = adp⊕(0,Y,Y). In addition, there exist either 2 or 8 distinct pairs (a, a,в в) such that adp⊕(a,e,Y) = adp⊕(0,Y,Y)• Also, we obtain a simplified representation of adp⊕(0, Y, Y) and formula for minadp⊕(0, Y, Y).
Y

**Keywords:** ARX, XOR, modular addition, differential cryptanalysis.

Pankov K. N. **IMPROVED ESTIMATES FOR THE NUMBER OF** (n, m, k)**- RESILIENT AND CORRELATION-IMMUNE BOOLEAN MAPPINGS.** Improved lower and upper bounds for |K (n, m, k)| (the number of correlation-immune of order k binary mappings) and |R (m, n, k)| (the number of (n, m, k)-resilient binary map- kn
pings) are obtained. By M (n, k) we denote , and by T (n, m, k) — the expres-
s=0 \s /

sion (2m If m > 5 and k (5 + 2log2n) + 6m 6
6 n (1/3 — Y) for fixed 0 < Y < 1/3, then there is n0 such that, for any £1 ,£2 and n > n0,

$$\frac{m^2}{m^2} \quad \underline{m—}\ ^{12}_{+17} \quad M(n,k) — £_1\, 6\, \log_2 |R(n,m,k)| — m2^n + T(n,m,k)\ 6$$

$$6\,(16m — 47)\,2^{m-4} — m + 3\ M(n,k) + £_2.$$

If m > 5 and k (5 + 2log2n) + 6m 6 n (5/18 — y) for fixed 0 < y < 5/18, then there is n0 such that, for any £1 , £2 and n > n0,

$$m^{™}\text{--}m\text{-}^{12} + 17^{\wedge}\ M\,(n,\ k) — £_1\, 6\, \log_2 |K\,(n,m,\ k)| — m2^n + m2^{m-1} + T\,(n,m,\ k) —$$

$$— n\ n + ^{1} + 1^{\log_2} \text{—}\ Л\ (2^m — 1)\ 6\ ^{\wedge}(16m — 47)\ 2^{m-4} — m + 3)\ M.\ (^{\wedge} + £_2.$$

**Keywords:** distributed ledger, blockchain, information security, resilient vectorial Boolean function, correlation-immune function.

*Fomin D.B.* **ON THE WAY OF CONSTRUCTING DIFFERENTIALLY** *26-* **UNIFORM PERMUTATIONS OVER** $F_{2^{2m}}$**.** The paper studies new ways of constructing differentially 26-uniform bijections over $F_{2^{2m}}$, m > 3, that are based on TU-con- struction. Some well known results on the constructing differentially 4-uniform permutations over $F_{2^{2m}}$ are generalized in this work. The core idea is to use TU-construction and differentially 6-uniform bijections to construct $2^t$ • 6-uniform permutations. A generalized method for constructing 2m-bit differentially 4-uniform permutations is proposed, and new constructions of differentialy 6 and 8-uniform permutations are introduced.

**Keywords:** *S-Box, permutation, differential uniformity, TU-construction.*

*Cheremushkin A. V.* **A CONDITIONS FOR UNIQUENESS RERESENTATION OF** p**-LOGIC FUNCTION INTO DISJUNCTIVE PRODUCT OF FUNCTIONS.** Let $f : V_n \wedge Z_p$ be p-logic function, $n > 2$, and $V_n = Z_n$ is considered as a vector space over $Z_p$ . A disjunctive decomposition of f into a product of p-logic functions under various linear transformations of arguments is considered. Function f *is linearly decomposable into disjunctive product* if there exists a linear transformation A of the vector space $V_n$ such that
f (xA) = f1 (x1 , . . . , xk)f2 (xk+1 , . . . , xn) for some k, 1 6 k < n, and functions f1 and f2 . We say that argument xn of functions f (x) is essential iff f (x) 6= f (x + en) for en = (0, . . . , 0, 1). The main result is: if all arguments of all functions f (xA) under linear substitutuions A of the vector space $V_n$ are essential, the set {a G $V_n$ : *f* (a) = 0} is not contained in hyperplane of $V_n$, and *f* is linearly decompsable into the disjunctive product *fl* *fm,* where m is maximal, then the direct sum of subspaces $V_n = V^{(1)} + \ldots + V^{(m)}$ is unique and invariant under the stabilizer group of

the function f in general linear group.

**Keywords:** p-logic functions, disjunctive product, linear transformation.

Shaporenko A. S. **ON DERIVATIVES OF BOOLEAN BENT FUNCTIONS.** Bent function can be defined as a Boolean function f(x) in n variables (n is even) such that for any nonzero vector $y$ its derivative $D_y f(x) = f(x) \oplus f(x \oplus y)$ is balanced, that is, it takes values 0 and 1 equally often. Whether every balanced function is a derivative of some bent function or not is an open problem. In this paper, special case of this problem is studied. It is proven that every non-constant affine function in n variables, $n > 4$, n is even, is a derivative of $(2^{n-1} - 1)|B_{n-2}|^2$ bent functions, where $|B_{n-2}|$ is the number of bent functions in n - 2 variables. New iterative lower bounds for the number of bent functions are presented.

**Keywords:** Boolean functions, bent functions, derivatives of bent function, lower bounds for the number of bent functions.

**SECTION 3**

Agievich S. V. **XS-CIRCUITS: HIDING ROUND ORACLES.** XS-circuits describe block ciphers that utilize 2 operations on binary words of fixed length: X — bitwise modulo 2 addition and S — substitution. In this paper, we develop a model of XS-circuits according to which several instances of a simple round circuit containing only one S operation are linked together and form a compound circuit called a cascade. S operations of a cascade are interpreted as independent round oracles. Determining some input/output pair of some round oracle from an input/output of the cascade is considered a security breach. We introduce the notion of hiding round oracles when such determining is hard. We show that a cascade based on a regular round circuit hides round oracles when the number of rounds is at least twice its dimension (the number of words in the processed data blocks).

**Keywords:** block cipher, XS-circuit, round oracle, linear recurrence sequence.

Bakharev A. O. **DEVELOPMENT AND ANALYSIS OF ORACLE FOR THE HIBRID ATTACK ON A CRYPTOGRAPHIC SYSTEM NTRU USING A QUANTUM SEARCH ALGORITHM.** Due to the development of quantum computing, there is a need for the development and analysis of cryptosystems resistant to attacks using a quantum computer (post-quantum cryptography algorithms). The security of many well-known post-quantum cryptosystems based on lattice theory depends on the complexity of solving the shortest vector problem (SVP). In the paper, a model of the quantum oracle which is required for the implementation of the hybrid quantum-classical algorithm for solving SVP is proposed and analyzed. For the public key post-quantum cryptosystem NTRU which is the finalist of the third round of the NIST competition, upper bounds for the number of qubits and the depth of the scheme are obtained. The bounds are based on the proposed model of the quantum oracle.

**Keywords:** cryptosystem NTRU, quantum search, public-key cryptography, post-quantum cryptography.

Berdnikova N. Yu., Pankratova I. A. **CRYPTANALYTIC INVERTIBILITY OF TWO-ARGUMENT FUNCTIONS.** Tests of cryptanalytic invertibility of all possible types for functions $g : D_1 \times D_2 \to D$ are proposed. Let $G_a = \{g(a,x_2) : x_2 \in D_2\}$ for any $a \in D_1$. Then: 1) function $g$ is invertible with respect to the variable $x_1$ of the type W iff $\forall a, b \in D_1$ $(a = b \to G_a \cap G_b = 0)$; 2) function $g$ is invertible with respect to the variable $x_1$ of the type V3 iff there exists a mapping $\hat{}$ such that the mapping $a \mapsto g(a, \hat{}(a))$ is injective; 3) function $g$ is invertible with respect to the variable $x_2$ of the type 3V iff $|G_a| = |D_2|$ for some value $a \in D_1$. Algorithms for constructing a recovering function and generating invertible functions are formulated; some estimates of the number of invertible functions are given.

**Keywords:** cryptanalytic invertibility, invertibility test, recovering function.

Bobrovskiy D. A., Zadorozhny D. I., Koreneva A. M., Nabiev T. R., Fomichev V. M. **EXPERIMENTAL STUDY OF THE CHARACTERISTICS OF ONE METHOD OF INTEGRITY CHECKING OF LARGE VOLUME DATA STORAGE.** A way of embedding the high-performance integrity check value algorithm in the hash function (GOST 34.11-2018) is described. The results previously presented at RusCrypto'2020 have been substantially improved. Experimental studies of performance and cryptographic properties of the new algorithm have been conducted. The proposed algorithm was found to be more productive than the known cryptographic hashing functions, similar in performance to the CRC32, and significantly superior to the CRC32 algorithm in cryptographic properties.

**Keywords:** additive generators, integrity check value, matrix-graph approach, mixing properties, shift registers, AG-S, AG-S-Stribog, SMHasher.

Bobrovskiy D. A., Nabiev T. R., Fomichev V. M. **ON THE PADDING ALGORITHM OF LARGE-SIZED BLOCKS IN INTEGRITY CONTROL SYSTEMS.** In integrity check value algorithms, calculating the checksum of a file requires that its length be a multiple of a given value ($l$ bits). When file size of any length is used to be checked, the file is usually padded to the required length. A computationally simple and efficient padding scheme, designed for integrity control systems processing large blocks (about 1 Kbyte), is presented. The scheme is based on the outputs of a linear congruent generator. The initial state of the generator is formed with the data of the block to be padded and the length of the file. The results of analysis of cryptographic properties of the integrity control algorithm and performance evaluation experiments showed the comparative advantages of the proposed scheme in comparison with the known standard padding schemes.

**Keywords:** padding, wide block, linear congruent generator, characteristics of padding procedures, checksum, integrity control, $AG$-$S$, SMHasher.

Kolegov D. N., Khalniyazova Y.R. **THRESHOLD DIFFIE — HELLMAN PROTOCOL.** We introduce a threshold elliptic curve Diffie — Hellman (ECDH) scheme which allows to generate and store private keys in a distributed way so that the private key doesn't have to be recomputed in order to perform a cryptographic operation. The main idea is to use a dealerless DKG scheme based on Feldman's VSS to generate shares of a private key without ever having the private key computed. To complete a cryptographic operation, a shareholder performs some computations on the share and sends the resulting piece to the other participating shareholders. Combined together, those values give the expected result of the cryptographic operation without ever giving a clue on the share values themselves.

**Keywords:** threshold cryptography, threshold Diffie — Hellman, ECDH.

Kolegov D. N., Khalniyazova Y.R. **WireGuard PROTOCOL WITH GOST CIPHER SUITES.** In the paper, we consider WireGuard VPN protocol instantiated with GOST cipher suites. The motivation for this work emerges from the rising use of WireGuard protocol in cloud and distributed solutions adopted in Russia. We retrospectively describe our project considering the choice of GOST primitives, alternative solutions, some aspects of implementation, the results of our work, and directions for future research. The resulting specification and reference implementation could be used as a starting point for the development of recommendations for WireGuard protocol implemented with GOST cipher suites.

**Keywords:** WireGuard, GOST, VPN.

Kutsenko A. V., Atutova N. D., Zyubina D. A., Maro E. A., Filippov S. D. **ALGEBRAIC CRYPTANALYSIS OF ROUND-REDUCED LIGHTWEIGHT CIPHERS SIMON AND**

**SPECK.** This paper presents algebraic attacks on Simon and Speck, two families of lightweight block ciphers having LRX- and ARX-structures respectively. They were presented by the U.S. National Security Agency in 2013 and later standardized by ISO as a part of the RFID air interface standard. The ciphers are algebraically encoded, and the resulting systems of Boolean equations are solved with different SAT solvers as well as methods based on the linearization. For the first time, the approaches that use the sparsity of systems of Boolean equations are applied to these ciphers. The linearization parameters in systems of equations for both of the ciphers are estimated. A comparison of the efficiency of the used methods is provided.The results of the algebraic analysis show that the inclusion of additional nonlinear operations significantly increases the attack time and the amount of memory used. Therefore, the methods considered are more effective for cryptanalysis of the Simon cipher than Speck.

**Keywords:** algebraic cryptanalysis, block cipher, lightweight cryptography, Simon, Speck.

Medvedeva N. V., Titov S. S. **TO THE TASK OF DESCRIPTION MINIMAL BY INCLUSION PERFECT CIPHERS.** This work is dealing with the problem of description Shannon perfect ciphers (which are absolutely immune against the attack on ciphertext, according to Shannon), minimal by inclusion. A graph approach to the description of perfect ciphers and their modern analogues and generalizations is proposed. The equivalence graph of the keys of the cipher is defined. Key equivalence refers to the following: two different keys are equivalent in cipher-value $x_i$, if the cipher-value $x_i$ on these keys is encrypted to the same code designation. In this case, pairwise different keys $k_1$, $k_2$, $k_3$, . . . , $k_{n-1}$, $k_n$ form a cycle of length n, if there is such a sequence of cipher-values that: 1) the neighboring cipher-values are different; 2) the keys $k_1$, $k_2$, $k_3$, . . . , $k_{n-1}$, $k_n$, $k_1$ are sequentially equivalent in the corresponding cipher-values. If n is an odd number, then the keys $k_1$, $k_2$, . . . , $k_n$ form an odd-length cycle. A sufficient minimum inclusion condition of the cipher has been proven: let some inhomogeneously connected component of the equivalence graph of the keys of the cipher have an odd-length cycle, then the cipher is minimal by inclusion. Examples are given to illustrate the effectiveness of the proposed approach. The results can be used to study almost-perfect ciphers.

**Keywords:** perfect ciphers, endomorphic ciphers, non-endomorphic ciphers.

Nabokov D. A. **POST-QUANTUM LATTICE-BASED E-VOTING FOR MULTIPLE CANDIDATES.** In recent years, many effective lattice-based cryptographic schemes have emerged, including (fully) homomorphic encryption and a multi-party computation. Such lattice-based schemes are interesting because they are resistant to attacks by a quantum computer. In this paper, an electronic voting scheme is implemented that can efficiently work for multiple voting candidates. Moreover, two voting options are possible: a vote for a single candidate or a vote for any subset of candidates. There are many authorities in the scheme, the vote privacy is preserved in the case when at least one authority remains honest. The scheme is aimed at maintaining the vote privacy and verifiability of the results, therefore, various assumptions are used to comply with other often considered security features of electronic voting, e.g. each authority has the public keys of all admitted voters. The scheme is based on zero-knowledge proofs and a commitment scheme with homomorphic properties. Due to the zero-knowledge proofs, any member of the scheme can verify the voting results.

**Keywords:** lattices, e-voting, commitment scheme, zero-nowledge proof, amortized zeroknowledge opening proof.

Pogorelov B. A., Pudovkina M. A. **ON ARX-LIKE CIPHERS BASED ON DIFFERENT CODINGS OF 2-GROUPS WITH A CYCLIC SUBGROUP OF INDEX 2.** A large number of block ciphers are based on easily and efficiently implemented group operations on 2-groups such as the additive group of the residue ring $Z_{2^m}$, the additive group of the vector space $V_m(2)$ over

GF(2) and their combination. ARX-like ciphers use the operations of cyclic shifts and additions in $Z_{2^m}$, $V_m(2)$. For developing techniques of building and analysing new symmetric-key block ciphers, we study group properties of m-bit ARX-like ciphers based on regular groups generated by $(0, 1, \ldots, 2^m - 1)$ and different codings of permutation representations of nonabelian 2-groups with a cyclic subgroup of index 2. There are exactly four isomorphism classes of the nonabelian 2-groups such as the dihedral group $D_{2^m}$, the generalized quaternion group $Q_{2^m}$, the quasidihedral group $SD_{2^m}$ and the modular maximal-cyclic group $M_{2^m}$. For such groups, we get imprimitivity criterions and give conditions on codings in order that the group of the ARX-like cipher should be equal to the symmetric group $S_{2^m}$. We also provide examples of three natural codings and their group properties.

**Keywords:** ARX-ciphers, primitive group, dihedral group, generalized quaternion group, modular maximal-cyclic group, quasidihedral group.

Semenov A. A., Antonov K. V., Gribanova I. A. **GENERATING ADDITIONAL CONSTRAINTS IN ALGEBRAIC CRYPTANALYSIS USING SAT ORACLES.** We describe a new technique aimed to generate new constraints which augment with the original set of constraints for a problem of algebraic cryptanalysis. In case the original problem is reduced to a system of Multivariate Quadratic equations over GF(2), the generated constraints can be in the form of linear equations over two-element field. If the considered problem is reduced to SAT, then new constraints are in the form of logic equivalences, anti-equivalences or unit resolvents. In both cases we demonstrate that new constraints generated by the proposed technique can decrease the complexity estimation of attacks on considered functions.

**Keywords:** algebraic cryptanalysis, Boolean satisfiability problem (SAT), MQ systems of equations over GF(2), SAT oracle.

Kosolapov Y. V., Turchenko O. Y. **CHOOSING PARAMETERS FOR ONE IND- CCA2 SECURE McEliece MODIFICATION IN THE STANDARD MODEL.** The paper is devoted to choosing parameters for one IND-CCA2-secure McEliece modification in the standard model. In particular, the underlying code, plaintext length and one-time strong signature scheme are suggested. The choice of parameters for the scheme was based on efficiency, on the one hand, and security, on the other. Also, experiments for the suggested parameters are provided using the NIST statistical test suite.

**Keywords:** post-quantum cryptography, McEliece-type cryptosystem, IND-CCA2-security, NIST statistical test suite.

Roman'kov V. A. **AN IMPROVEMENT OF CRYPTOGRAPHIC SCHEMES BASED ON THE CONJUGACY SEARCH PROBLEM.** The key exchange protocol is a method of securely sharing cryptographic keys over a public channel. It is considered as important part of cryptographic mechanism to protect secure communications between two parties. The Diffie — Hellman protocol, based on the discrete logarithm problem, which is generally difficult to solve, is the most well-known key exchange protocol. One of the possible generalizations of the discrete logarithm problem to arbitrary noncommutative groups is the so-called conjugacy search problem: given two elements g, h of a group G and the information that $g^x = h$ for some $x \in G$, find at least one particular element x like that. Here $g^x$ stands for $x^{-1}gx$. This problem is in the core of several known public key exchange protocols, most notably the one due to Anshel et al. and the other due to Ko et al. In recent years, effective algebraic cryptanalysis methods have been developed that have shown the vulnerability of protocols of this type. The main purpose of this short note is to describe a new tool to improve protocols based on the conjugacy search problem. This tool has been introduced by the author in some recent papers. It is based on a new mathematical concept

of a marginal set.

**Keywords:** cryptography, key exchange protocol, conjugacy searh problem, marginal set, algorithm.

**SECTION 4**

Akhmetzyanova L. R., Babueva A. A., Kyazhin S. N., Popov V. A. **ON PRIVACY IN DECENTRALIZED SYSTEMS WITH TOKENS.** A three-level model of a decentralized system is proposed, the level with protocols for the creation and validation of private transactions is highlighted. The main feature of ensuring the transaction privacy in decentralized systems with tokens is the need to validate the various conditions for the transaction content without access to it. Therefore, classes of non-classical (and non-standardized in the Russian Federation) cryptographic mechanisms, which are often used in decentralized systems with private transactions, are highlighted. The non-universality of the existing formal definitions of such systems is shown. Therefore, formalizing the transaction privacy property in the general case is an open problem.

**Keywords:** decentralized system, privacy, token, zero know ledge proof, homomorphic encryption, commitment, aggregate signature, ring signature.

Devyanin P. N., Leonova M. A. **ABOUT METHODS OF DEVELOPING CONSISTENT DESCRIPTION OF THE MROSL DP-MODEL FOR OS AND DBMS FOR ITS VERIFICATION WITH Rodin AND ProB TOOLS.** Access control mechanism performs one of the main functions to ensure the security of information security tools, such as OS or DBMS. Formal models of access control are developed to achieve confidence in correctness of this mechanism, to create conditions for the scientific justification of its compliance with the security requirements. The paper presents methods of consistent description of the MROSL DP-model in the language used in mathematics (mathematical notation) and in Event-B formal method (formalized notation). The first result of using these methods in refining the formalized notation was provision the possibility of its joint verification by deductive method and method of model checking using the Rodin and ProB tools. The second result was modeling using Event-B formal method of interacting systems with their own developed access control mechanisms, such as OS and DBMS, which is necessary to match the description of the model in mathematical notation. These methods are formed on expression of the properties of the original hierarchical description of the model in mathematical notation in a sequential refinement of the model levels based on the refinement technique of Rodin and on application of total functions instead of directly using axiom of mathematical induction.

**Keywords:** formal model of access control, verification, assurance requirements, Astra Linux Special Edition.

Kondyrev D. O. **zk-SNARK-BASED DATA PRIVACY METHOD.** The paper presents a method for ensuring data confidentiality with the possibility of validation based on the zk-SNARK zero-knowledge proof protocol. This method allows the creation of zk- SNARK-based algorithms in Ethereum smart contracts code using high-level basic cryptographic schemes that implement logical operations (AND, OR, NOT) and comparison operations. Cryptographic schemes are implemented on the basis of the libsnark library as a rank-1 constraint systems (R1CS). The Ethereum virtual machine has been modified to include functions for schema creation, proof generation and verification.

**Keywords:** distributed systems, blockchain, zero-knowledge proof, zk-SNARK, Ethereum platform.

Lebedev V. V. **CONTROL FLOW FLATTENING DEOBFUSCATION USING SYMBOLIC**

**EXECUTION.** Control Flow Flattening obfuscation method replaces jumps in program code (both conditional and unconditional) with a jump to a dispatcher block, which determines the real control flow. It complicates reverse engineering of the program, because researcher can't easily say which block of code will be executed after another one. In the paper, we propose the algorithm which recovers the original control flow for given obfuscated program. This algorithm is based on symbolic execution, which helps us to find all possible triples $(a_i, x_i, b_i)$, where $a_i$ is the address from which the dispatcher was reached, $x_i$ is the value of the control register at which the jump to address $b_i$ occurs. Then the set of triples is converted to the set of patches to the original program. In comparison with other algorithms, this algorithm doesn't imply any restrictions on the structure of obfuscated functions, but also doesn't affect anything except the control flow.
**Keywords:** reverse engineering, symbolic execution, obfuscation, control flow flattening.

Lebedev R. K., Koryakin I. A. **APPLICATION OF X86 EXTENSIONS FOR CODE PROTECTION.** A new approach is proposed to protect the program code against reverse engineering tools, such as decompilers and symbolic execution tools. The approach is based on the usage of uncommon x86 processor instructions that could be implemented incorrectly in the aforementioned tools. Existing approaches to this problem are also considered, and the relative performance advantage of the proposed approach is noted. A method for numeric constants obfuscation, following this approach, is developed with the usage of AES-NI extension for the x86 architecture and its AESENC instruction in particular. This method is implemented for Clang compiler with the help of LLVM Intermediate Representation and tested against reverse engineering tools, such as IDA and Ghidra decompilers and angr symbolic execution tool.
**Keywords:** code protection, reverse engineering, decompiler, symbolic execution, x86 processor architecture.

Nedyak M. S. **EXTENDED GRAMMAR-BASED FUZZING ALGORITHM FOR JAVASCRIPT ENGINES.** JavaScript engine security continues to be critical for user safety. Unfortunately, modern fuzzing algorithms cover only a small part of the entire engine. JavaScript engine requires highly structured input — JavaScript programs that are syntactically and semantically correct. The most of generated input struggle to pass syntax and semantic correctness checks. In this paper, we describe the extension of the grammarbased fuzzing algorithm. We propose a way of describing grammar for fuzzing using a set of JavaScript source codes. Grammars constructed with our method cover larger part of JavaScript language in comparison with grammars created by describing grammar rules. Another change of the basic algorithm is controlling the context in the mutation process. It allows filtering a lot of inputs that don't give new results. Our experiments show that the improved algorithm has increased speed of finding new paths in the target program. **Keywords:** fuzzing, JavaScript.

Nikolaev A. A. **EXTENSION AND ANALYSIS OF INFORMATION HIDING METHOD DEEP STEGANOGRAPHY.** Information hiding method Deep Stegano- graphy has been implemented. As a result, an extension of the method is proposed in the form of adding n additional hidden layers to the encoded image. This extension allows transmitting more messages in the image container per one transmission session. The properties and metrics of the method have been analyzed, and the results show that this method allows revealing secret messages with SSIM-index accuracy of 56 % on average for the deepest layer for optimal n = 3 and 82 % for the closest (third) layer with almost imperceptible hiding properties.
**Keywords:** information hiding, covert channels, neural networks.

Nikulin V. S. **ADAPTATION OF THE ROSENBLATT — PARZEN METHOD FOR THE**

**EXPERIMENTAL EVALUATION OF THE COMPUTING SYSTEM RELIABILITY.** The lack of initial information about the law of distribution of random variables and their realization at a time moment close to the beginning of the observation, as well as the presence of censored data, force us to adapt the nonparametric Rosenblatt — Parzen method. To compensate for the bias and eliminate the violation of the normalization condition, the method of mirroring the original data is considered. When constructing the distribution density of random variables, it is proposed to take into account censored data. The accuracy of the estimate shows a decrease in error when using the adapted Rosenblatt — Parzen method. The practical implementation of the adapted Rosenblatt — Parzen method is demonstrated by the example of an experimental assessment of the reliability indicators of a computing system. Plotting the density and the mean time between failures distribution function allows calculating the main indicators of the object's reliability: failure rate, probability of no-failure operation, mean time between failures. Calculated estimates of the reliability indicators of a computing system are necessary for making control decisions during operation and maintaining the facility's performance. **Keywords:** experimental reliability analysis, small samples, computing systems, Rosenblatt — Parzen method.

**SECTION 5**

Geut K. L., Titov S. S. **BASES OVER THE FIELD GF(2) GENERATED BY THE SCHUR — HADAMARD OPERATION.** The paper deals with the problem of constructing, describing and applying bases of vector spaces over the field GF(2) generated by the componentwise product operation up to degree d. This problem "Bases" was posed as unsolved in the Olympiad in cryptography NSUCRYPTO. In order to give a way to solve this problem with the Reed — Muller codes, we define the generating family F as a list of all string i in a true table under condition: the word $x_{i^1}, \ldots, x_{i^s}$ has Hamming weight not superior d. The values of coefficients of function f are determined recurrently, as in the proof of the theorem on ANF: the coefficient before composition for subset T (cardinality does not exceed d) in the set $\{t^1, \ldots, t^s\}$ of arguments is determined as the sum of the values of *f* and the values of the coefficients for the whole subset $R \subset T$. Hence, for all $s, d, s > d > 1$, there is a basis for which such a family exists, and the construction of the bases is described above. We propose to use general affine group on space $F^s$, $F$ = GF(2), for obtaining the class of such bases in the condition of the problem.
**Keywords:** NSUCRYPTO, orthomorphisms, vector space basis, Reed — Muller code.

Kosolapov Yu. V., Lelyuk E. A. **ON DECOMPOSABILITY OF SCHUR — HADAMARD PRODUCT OF THE TENSOR PRODUCTS SUM OF REED — MULLER CODES.** McEliece code-based cryptosystems are considered to be a perspective alternative to modern asymmetric cryptosystems, because by choosing a suitable errorcorrecting code they are assume to be resistant to attacks by computer based on a quantum computing model. The original McEliece cryptosystem based on Goppa codes is now considered to be resistant. It should be noted that high resistance is achieved by using a large key size. In order to reduce the key size, cryptosystems of the McEliece type based on another error-correcting codes have been proposed. But for some well-known codes, such as generalized Reed — Solomon codes and binary Reed — Muller codes, these cryptosystems turn out to be broken even by computers based on the classical Turing model. Earlier, to enhance the resistance, it was proposed to use the tensor product of Reed — Muller codes. The natural generalization of this approach is using the class of codes that are the sum of several tensor products of a special form. Such codes are effectively decoded, so a McEliece type cryptosystem can be built on their basis. In order to use a cryptosystem, its resistance should be analized. For analysis of the code-based cryptosystems resistance to a

structural attacks, the properties of the Schur — Hadamard product of codes that lie in the basis of these cryptosystems are often investigated. In the paper, we investigate the decomposability of codes that are a special sum of two tensor products of Reed — Muller codes. In a number of cases, we found conditions on the parameters of the multiplier codes that lead us to decomposition of the square of the code under consideration into a direct sum of Reed — Muller codes. Conditions were also found under which such a decomposition is impossible. **Keywords:** McEliece type cryptosystem, sum of tensor products, Schur — Hadamard product, decomposability.

Lobov A. A., Abrosimov M. B. **REGULAR VERTEX 1-EXTENSION FOR 2-DI- MENSION MESHES.** In the paper, a schema of vertex 1-extension for 2-dimensional mesh is proposed. The extension is 4-regular graph. The schema can be applied to meshes $n$ x m, $n > 2$ and m > 2. The extension is minimal for some meshes. Some extensions made by schema are not minimal. An example of such mesh is given.
**Keywords:** graph,mesh,fault tolerance, vertex extension.

Panteleev R. I., Zharkova A. V. **ON ATTRACTORS IN ONE DISCRETE BINARY DYNAMIC SYSTEM WITH BIPARTITE DEPENDENCY GRAPH.** One discrete binary dynamic system $(S_n, f)$, $n > 1$, with bipartite dependency graph is considered. The states of such a system are all possible binary vectors of length $n$, and evolutionary function is $f = (x_n, 0, \ldots, 0, x_1)$. In this case, $f$ is associated with a bipartite directed dependency graph with vertices set $\{a_1, \ldots, a_n, e\}$ and with arcs from $a_1$ to $a_n$, from $a_n$ to $a_1$ and from $a_i$ to £, $1 < i < n$. The map of the $(S_3, f)$ system with the evolutionary function $f = (x_3, 0, x_1)$ and its bipartite dependency graph are presented. A theorem is given on the type and number of attractors in these systems. Namely, the system has two attractors of length 1: $0^n$ and $10^{n-2}1$, and one attractor of length 2 formed by states $00^{n-2}1$ and $10^{n-2}0$.
**Keywords:** attractor, basin, graph, dependency graph, bipartite graph, discrete binary dynamic system, evolutionary function.

Razumovsky P. V., Abrosimov M. B. **SCHEMES FOR CONSTRUCTING MINIMAL VERTEX 1-EXTENSIONS OF COMPLETE BICOLORED GRAPHS.** Bicolored graphs are considered, i.e., graphs whose vertices are colored in two colors. Let $G = (V, a, f)$ be a colored graph with a coloring function $f$ defined on the set of its vertices. A colored graph $G^*$ is called a vertex 1-extension of a colored graph $G$ if the graph $G$ can be embedded preserving the colors into each graph obtained from the graph $G^*$ by removing any of its vertices together with incident edges. A vertex 1-extension $G^*$ of a graph $G$ is called minimal if the graph $G^*$ has two more vertices than the graph $G$, and among all vertex 1-extensions of the graph $G$ with the same number of vertices the graph $G^*$ has the minimum number of edges. In this paper, we propose a full description of minimal vertex 1-extensions of complete bicolored graphs. Let $K_{n_1,n_2}$ be a complete $n$-vertex graph with $n_1$ vertices of one color and $n_2$ vertices of a different color. If in a complete bicolored graph $n_1 = n_2 = 1$, then in the minimal vertex 1-extension of such a graph there is one additional edge. If in a complete bicolored graph either $n_1 = 1$ or $n_2 = 1$, then the minimal vertex 1-extension of such a graph has $2n - 1$ additional edges. In all other cases, the minimal vertex 1-extension of a complete bicolored graph has $2n$ additional edges. The schemes for constructing the corresponding minimal vertex 1-extensions are proposed.
**Keywords:** colored graph, complete graph, graph extension, minimal vertex graph extension, fault tolerance.

Nagy G. P., El Khalfaoui S. **TOWARDS THE SECURITY OF McEliece's CRYPTOSYSTEM BASED ON HERMITIAN SUBFIELD SUBCODES.** The purpose of this paper is to provide a comprehensive security analysis for the parameter selection process, which involves the computational cost of the information set decoding (ISD) algorithm using Hermitian subfield sub

code parameters.

**Keywords:** code-based cryptography, McEliece Cryptosystem, Hermitian subfield subcodes, Schur square dimension.

**SECTION 6**

Egorushkin O. I., Kolbasina I. V., Safonov K. V. **ON A SOLUTION OF POLYNOMIAL GRAMMARS AND THE GENERAL ALGEBRAIC EQUATION.** In this paper, we investigate the solvability of formal grammars, by which we mean systems of non-commutative polynomial equations, in the case of one equation. Formal grammars are solved in the form of formal power series (FPS), which express nonterminal symbols of the language through terminal symbols; the first component of the solution is the formal language. The authors develop a method based on the study of the commutative image of grammar and language, which is obtained if in any FPS the symbols of the alphabet are considered commutative variables. A theorem is obtained that gives a power series expansion of the solution to a general algebraic equation, and also allows us to investigate the solvability in the form of an FPS of a polynomial grammar consisting of one equation. **Keywords:** general algebraic equation, polynomial grammar, formal power series, non-commutative symbols, commutative image.

Rybalov A. N. **ON GENERIC COMPLEXITY OF THE ISOMORPHISM PROBLEM FOR FINITE SEMIGROUPS.** Generic-case approach to algorithmic problems was suggested by A. Miasnikov, V. Kapovich, P. Schupp, and V. Shpilrain in 2003. This approach studies behavior of an algorithm on typical (almost all) inputs and ignores the rest of inputs. In this paper, we study the generic complexity of the isomorphism problem for finite semigroups. In this problem, for any two semigroups of the same order, given by their multiplication tables, it is required to determine whether they are isomorphic. V. Zemlyachenko, N. Korneenko, and R. Tyshkevich in 1982 proved that the graph isomorphism problem polynomially reduces to this problem. The graph isomorphism problem is a well-known algorithmic problem that has been actively studied since the 1970s, and for which polynomial algorithms are still unknown. So from a computational point of view the studied problem is no simpler than the graph isomorphism problem. We present a generic polynomial algorithm for the isomorphism problem of finite semigroups. It is based on the characterization of almost all finite semigroups as 3-nilpotent semigroups of a special form, established by D. Kleitman, B. Rothschild, and J. Spencer, as well as the Bollobas polynomial algorithm, which solves the isomorphism problem for almost all strongly sparse graphs.

**Keywords:** generic complexity, isomorphism, finite semigroups.

**SECTION 7**

Kovrizhnykh M. A., Fomin D. B. **ON A HEURISTIC APPROACH TO CONSTRUCTING BIJECTIVE VECTOR BOOLEAN FUNCTIONS WITH GIVEN CRYPTOGRAPHIC PROPERTIES.** Bijective vector Boolean functions (permutations) are used as nonlinear primitives of many symmetric ciphers. In this paper, we study a generalized construction of (2m, 2m)-functions using monomial and arbitrary m-bit permutations as constituent elements. A heuristic algorithm for obtaining bijective Boolean functions with given nonlinearity and differential uniformity, based on this construction, is proposed. For this, a search is carried out for auxiliary permutations of a lower dimension using the ideas of spectral-linear and spectral-difference methods. The proposed algorithm consists of iterative multiplication of the initial randomly generated 4-bit permutations by transposition, selecting the best ones in nonlinearity, the differential uniformity, and the corresponding values in the linear and differential spectra

among the obtained 8-bit permutations. The possibility of optimizing the calculation of cryptographic properties at each iteration of the algorithm is investigated; 8-bit 6-uniform permutations with nonlinearity 108 are experimentally obtained.

**Keywords:** Boolean function, permutation, nonlinearity, differential uniformity.

Kuznetsov A. A., Kuznetsova A. S. **SOME SUBGROUPS OF THE BURNSIDE GROUP** $B_0(2, 5)$**.** Let $B_0(2, 5) = \langle x, y \rangle$ be the largest finite two generator Burnside group of exponent five and order $5^{34}$. We study a series of subgroups $H_i = \langle a_i, b_i \rangle$ of the group $B_0(2,5)$, where $a_0 = x$, $b_0 = y$, $a_i = a_{i-1}b_{i-1}$ and $b_i = b_{i-1}a_{i-1}$ for $i \in \mathbb{N}$. It has been found that $H_4$ is a commutative group. Therefore, $H_5$ is a cyclyc group and the series of subgroups is broken. The elements $a_4 = xy^2xyx^2y^2x^2yxy^2x$ and $b_4 = yx^2yxy^2x^2y^2xyx^2y$ of length 16 generate an abelian subgroup of order 25 in $B_0(2, 5)$. Using computer calculations, we have found that there is no other pair of group words of length less than 16 that generate a noncyclic abelian subgroup in $B_0(2, 5)$.

**Keywords:** non-commutative cryptography, Burnside group.

Tkachev A. V., Kalgin K. V. **DPLL-LIKE SATISFIABILITY PROBLEM SOLVER OVER THE SYSTEM OF ANF EQUATIONS.** In the paper, we describe SAT solver for problems in ANF and show how typical SAT techniques can be implemented to work with ANF. This solver is compared to a number of classic SAT solvers on cryptanalysis problems (such as “guess-and-determine” attack on Grain stream cipher). The solver uses such techniques as Propagation of Constants, Propagation of Synonyms, Watched Monomials (2WM), equations simplification and variable selection order. Our experiments show that for “init=no” case this ANF solver works similarly to typical CNF SAT solvers, but in the “init=yes” case the latter fail where the ANF solver finds a solution. Based on the data we’ve gathered we make a conclusion that it is impractical to use SAT solvers to attack Grain in “init=no” case. For the future research, we want to make experiments with more ciphers and solvers, explore why modern CNF SAT solvers work slower than the ANF solver and adapt more SAT techniques into our implementation.

**Keywords:** SAT solver, ANF, cryptanalysis, stream ciphers.