ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

№3 2025 (67)

Спецвыпуск, посвященный 10-летию образовательного центра «Сириус»

DOI: 10.21681/2311-3456

Университет Сириус

Университет «Сириус»: Инновационная модель высшего образования

Университет «Сириус», открытый в 2019 году на базе одноимённого образовательного центра в Сочи, представляет собой уникальное учебное заведение, созданное для подготовки специалистов мирового уровня. Его деятельность ориентирована на развитие талантов и формирование нового поколения лидеров в области науки, технологий, искусства и спорта.

Образовательная модель университета «Сириус» кардинально отличается от традиционных подходов. Программы обучения разрабатываются с учётом индивидуальных интересов и целей каждого студента, что позволяет им углублённо изучать профильные дисциплины и осваивать смежные области знаний. Обучение строится вокруг реальных проектов, которые студенты выполняют под руководством опытных наставников. Такой подход помогает развивать навыки решения практических задач и готовит выпускников к работе в условиях современной экономики.

Научно-исследовательская работа является неотъемлемой частью учебного процесса. Студенты с первых курсов вовлечены в исследования, проводимые совместно с ведущими российскими и международными лабораториями, институтами и компаниями. Университет активно взаимодействует с зарубежными партнёрами, такими как MIT (США) и ETH Zurich (Швейцария), что обеспечивает доступ к глобальным образовательным и научным ресурсам. Интеграция с образовательным центром «Сириус» создаёт уникальные возможности для обмена знаниями и опытом с участниками программ центра.

Университет предлагает программы бакалавриата, магистратуры и аспирантуры по ключевым направлениям: естественные и точные науки — математика, физика, химия, биология; инженерные и технологические науки — искусственный интеллект, робототехника, биомедицинские технологии, квантовые технологии; гуманитарные и социальные науки — история и культурология, психология, экономика и управление; искусство и дизайн — современное искусство, дизайн и медиа; спорт и здоровье — физическая культура и биомеханика.

Преподавательский состав университета включает ведущих учёных, практиков и педагогов как из России, так и из-за рубежа. Среди них — лауреаты Нобелевской премии, члены академий наук, руководители крупных компаний и международных проектов. Такой состав обеспечивает высокий уровень подготовки студентов и их интеграцию в мировое научное сообщество.

В перспективе университет планирует усилить международное сотрудничество и стать одним из ключевых центров инновационного развития в России. Его выпускники готовы к решению сложных задач в науке, бизнесе и культуре, что делает их ключевыми фигурами в процессе модернизации страны.

Синтез науки, спорта и искусства стимулирует творческое развитие личности

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ

№3 (67) 2025 г.

Выходит 6 раз в год

Журнал выходит с 2013 г. (Свидетельство о регистрации ПИ № ФС77-75239). Перерегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 07.03.2019.

Журнал входит в рейтинг научных изданий ВАК в категории К1, индексируется в RSCI, публикует статьи по специальностям 1.2.4 и 2.3.6 – физ-мат. науки; 2.2.15, 2.3.1, 2.3.5, 2.3.6 – техн. науки

Учредитель и издатель

АО «Научно-производственное объединение «Эшелон»

Над номером работали:

Г. И. Макаренко – *шеф-редактор*, И. Ю. Шахалов – *отв. секретарь*, С. С. Игнатов – *верстка*, Ю. С. Логинова – *зам. главного редактора*

Подписано к печати 20.06.2025 г.
Общий тираж 120 экз. Цена свободная

Адрес: 107023, Москва, ул. Электрозаводская, д. 24, стр. 1.
E-mail: editor@cyberrus.info, тел.: +7 (985) 939-75-01.
Требования, предъявляемые к рукописям, размещены на сайте: **https://cyberrus.info/**

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс 40707

ОБРАЗОВАТЕЛЬНОМУ ЦЕНТРУ «СИРИУС» – 10 ЛЕТ

Гусев А. С.[1]

Уважаемый профессорско-преподавательский состав, сотрудники, аспиранты, студенты и выпускники Университета «Сириус»! Дорогие друзья! Примите самые искренние и сердечные поздравления со знаменательной датой – десятилетием Образовательного центра «Сириус»!

В 2025 году Образовательный центр «Сириус» отмечает знаменательную дату – 10 лет со дня создания. Образовательный центр «Сириус» создан Образовательным Фондом «Талант и успех» на базе олимпийской инфраструктуры по инициативе Президента Российской Федерации В. В. Путина. Фонд учрежден 24 декабря 2014 г.

Оглядываясь на пройденный путь, вспомним, что зимняя Олимпиада в Сочи 2014 заложила мощный фундамент для стремительного развития всего региона, но не менее важным было правильно распорядиться ее наследием. У Образовательного центра «Сириус» это получилось. Определяющую роль в этом сыграло беспрецедентное решение Президента России передать олимпийскую инфраструктуру детям и дальнейшее постоянное внимание *Владимира Владимировича Путина* к проектам и планам «Сириуса». Нам удалось выстроить системный подход к использованию всех объектов, сформировать на их базе собственные уникальные компетенции по подготовке талантливой молодежи, внедрить экспериментальные методы управления, которые позволяют реализовывать проекты в образовании, науке, искусстве и спорте, не имеющие аналогов в стране. Вся эта работа сегодня определяет будущее «Сириуса» и его олимпийского наследия, и, главное, будущее России.

Сегодня модель «Сириуса» включает все уровни образования от дошкольного до университетского, а также программы повышения квалификации педагогов и тренеров. Сам «Сириус» стал городом, где воспитывается будущая интеллектуальная элита России. Так, в 2019 году по поручению Президента России *Владимира Путина* был создан Научно-технологический университет «Сириус», который продолжает логику Образовательного центра «Сириус» и объединяет студентов и молодых исследователей с выдающимися, известными во всем мире, учеными, педагогами и практиками. Продвижением и поддержкой перспективных научно-технических проектов занимается Инновационный научно-технологический центр «Сириус», созданный в 2019 году.

Задача Университета «Сириуса» – готовить молодых ученых и технологических предпринимателей, которые смогут работать над передовыми исследованиями как в области фундаментальных открытий, так и прикладных исследований. Поэтому в подготовке первых магистров принимали участие несколько десятков ведущих ученых и экспертов страны. Нам удалось собрать команду из выдающихся ученых России, которые выступают наставниками для студентов. Кроме того, была запущена первая очередь крупнейшего в стране лабораторного комплекса наук о жизни, создается научно-технологический кампус мирового уровня. И мы рады, что все состоялось. Сегодня перед нашими молодыми исследователями и технологическими предпринимателями открыто настоящее море возможностей как в науке, так и в индустрии.

В 2023 году Университет «Сириус» выпустил первых магистров. Свои дипломы получили 37 магистров, окончивших программы подготовки: «Математическая робототехника и искусственный интеллект», «Биоинформатика и математическая биология», «Финансовая математика и финансовые технологии», «Генетика и генетические технологии». Половина из получивших дипломы магистров продолжили обучение в аспирантуре Университета «Сириус». Все программы подготовки реализовывались в тесном сотрудничестве с ведущими компаниями-партнерами. В их числе ГК «Росатом», «Газпром нефть», «Р-Фарм», «Генериум», Банк России, «Тинькофф» и многие другие.

Проект «Сириус» продолжает развиваться!

2025-й год стал особенным для Научно-технологического университета «Сириус». В начале этого года ООН провозгласила 2025 год Международным годом квантовой науки и технологий (International Year of Quantum

1 Гусев Антон Сергеевич, директор Научно-технологического университета «Сириус». Федеральная территория «Сириус», Россия. E-mail: gusev.as@talantiuspeh.ru

Science and Technology – IYQ), признав квантовые технологии исключительно важными для технологического развития стран мира[2]. В нашей стране по поручению Президента России Владимира Путина отечественные ученые и инженеры активно проводят научные исследования и инженерные разработки по направлениям: *квантовые вычисления* (ГК «Росатом»), *квантовые коммуникации* (ОАО «РЖД») и *квантовая сенсорика* (ГК «Ростех»). Разработана соответствующая Дорожная карта «Квантовые технологии» (2019), которая была обновлена в конце 2024 года[3].

В 2025 году Россия вышла в число лидеров в области квантовых технологий, создав работающие квантовые вычислители на всех четырех приоритетных платформах: ионах, атомах, фотонах и сверхпроводниках. Стране удалось это сделать. Такие достижения есть только у трех стран – США, Китая и России. Кроме того, Россия вошла в число шести стран, которые обладают квантовыми компьютерами в 50 кубитов и выше. Квантовая тематика стала частью повестки страны. Это стало возможным благодаря, прежде всего, президенту России и усилиям выдающихся отечественных ученых и инженеров-исследователей. Поставлены новые задачи. В их числе – квантовые компьютеры уже не в десятках, а в сотнях кубит, количество квантовых сервисных решений, добавляется тематика, связанная с квантовыми сенсорами и др. В атомной отрасли уже запущена первая программа внедрения квантовых вычислений, в том числе квантовых алгоритмов. В настоящее время определяется спектр конкретных промышленных запросов, которые приоритетно будут решаться с помощью квантовых процессоров; планируется их апробация на модельных задачах. С 2026 года планируется постепенный переход от решения модельных задач – к практическим. Ожидается, что после 2030 года будут представлены эффекты от применения квантовых вычислений в решении производственных задач в атомной отрасли.

Полученные результаты в области квантовых вычислений наглядно показывают высокий технологический потенциал квантовых технологий. Вместе с тем, становится понятно, что квантовые компьютеры скоро достигнут достаточной зрелости и окажутся способны к взлому большей части криптографических алгоритмов, что может радикально изменить весь экономический и социальный ландшафт. В первую очередь, уязвимыми окажутся системы шифрования и протоколы с открытым ключом. В том числе, схемы электронной подписи, а также прикладные протоколы защищенной передачи данных в интернете, например, протокол HTTPS, который сейчас используется повсеместно. Под угрозой окажутся цифровые финансовые активы (ЦФА) – финансовые инструменты, зафиксированные в блокчейн-системах и предоставляющие владельцам права на цифровые объекты или данные. В том числе, токены и криптовалюты, а также более сложные финансовые инструменты, такие как смарт-контракты и цифровые валюты, в том числе, цифровой рубль. Насколько эта угроза реальна? Для ответа на этот вопрос в Университете «Сириус» был поставлен и успешно выполняется Проект ФТС-2024-2.3-VY-1160-5744 «*Технологии противодействия ранее неизвестным квантовым киберугрозам*» (2024–2027 гг.) под руководством ведущего ученого – д.т.н., профессора *Петренко Сергея Анатольевича*. Получены первые весомые научные результаты, о которых подробнее будет рассказано далее на страницах настоящего тематического или специального выпуска научного журнала «Вопросы кибербезопасности», посвященного актуальной «квантовой повестке безопасности» России.

Квантовые технологии (квантовые вычисления, квантовые коммуникации, квантовая сенсорика) развиваются очень стремительно. В будущем они способны решить проблемы, над которыми человечество бьётся десятилетиями, обещая революцию в компьютерных науках, машинных вычислениях, информационной безопасности, искусственном интеллекте, экологии, медицине, урбанистики, решении климатических кризисов и многих других областях. Разбираться в них важно не только учёным и инженерам, но и абсолютно каждому думающему человеку, чтобы понимать, какую именно пользу та или иная разработка принесет в вашу работу и область знания. Это процессы, которые происходят прямо сейчас, и упускать такой шанс попасть в квантовое будущее точно не стоит.

Учитывая современные тенденции и перспективы развития квантовых технологий, Университет «Сириус» разработал новые программы дополнительного профессионального образования «Практическое применение квантовых алгоритмов» и «Квантовая информатика и информационная безопасность». Кроме того, создаётся новая образовательная программа для подготовки специалистов по разработке универсальных библиотек квантовых алгоритмов независимо от используемых квантовых платформ и чипов. Разработчики, владеющие навыками создания программ для квантовых компьютеров, получат конкурентное преимущество по мере развития квантового «железа». Также по новой программе будут готовить специалистов, способных переводить классические математические модели большой размерности и сложности в квантово-механические для последующего применения в различных предметных областях «Экономики данных» Российской Федерации.

В завершении своего обращения позвольте пожелать Всем счастья, удачи, благополучия и новых свершений! Пусть этот юбилейный год – 10 лет со дня создания Образовательного центра «Сириус» – всем нам запомнится яркими интересными событиями и высокими достижениями в науке и образовании!

С уважением,
Гусев Антон Сергеевич

2 https://quantum2025.org/
3 https://digital.gov.ru/uploaded/files/07102019kvantyi.pdf

ПРЕДСТАВЛЕНИЕ ТЕМАТИЧЕСКОГО ВЫПУСКА ЖУРНАЛА

Ширяев М. В.[1]

Дорогие коллеги!

Представляю Вашему вниманию тематический выпуск научного журнала «Вопросы кибербезопасности», который посвящен актуальной «квантовой повестке безопасности» России!

Сегодня квантовые технологии находятся в центре внимания научного и делового сообщества. При этом обеспечение квантовой устойчивости (англ. Quantum Resilience) ключевых цифровых экосистем и платформ Экономики данных является одной из злободневных научно-технических проблем современности. Здесь под квантовой устойчивостью понимается способность упомянутых систем достигать целей функционирования в условиях атак злоумышленников с применением квантового компьютера. Актуальность этой проблемы объясняется появлением новой квантовой угрозы безопасности информации, ростом требований безопасности к критической информационной инфраструктуре РФ, ростом структуры и поведения упомянутых систем, и уже недостаточностью (неспособностью) известных технологий (моделей, методов и средств) обеспечения информационной безопасности и киберустойчивости для решения задач обнаружения, нейтрализации и упреждения квантовых атак злоумышленников. Достижения IBM, а также ряда других высокотехнологичных производителей квантовых компьютеров убедительно подтверждают реалистичность новой «квантовой угрозы». Так, в США уже начали подготовку к противодействию будущим квантовым кибератакам. Администрация Президента США подготовила ряд первых директив о подготовке государства и бизнеса к будущим квантовым кибератакам (https://www.quantum.gov/; https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/).

Анализ состояния научной проблемы обеспечения квантовой устойчивости ключевых цифровых экосистем и платформ экономики данных Российской Федерации в условиях появления новой квантовой угрозы безопасности позволил выделить три возможных направления ее разрешения.

Во-первых, создание и переход на постквантовые криптопримитивы (англ. Public-Key Encryption) и электронной подписи (англ. Digital Signatures)» на основе разделов математики, потенциально содержащих сложные вычислительные задачи, для которых в настоящее время не известны эффективные алгоритмы решения на классических и квантовых вычислителях. В том числе, на основе решеток, многочленов от многих переменных, изогений на эллиптических кривых, октонионов, многочленов Чебышева, конечных некоммутативных ассоциативных алгебрах (КНАА) и др.

Во-вторых, создание и переход на единичные квантово-устойчивые компоненты и связи упомянутых систем с математически доказуемой стойкостью. В том числе, квантовые протоколы передачи данных, которые невозможно незаметно перехватить и дешифровать, системы квантового распределения ключей (англ. Quantum key distribution, QKD), квантовые генераторы действительно случайных чисел (англ. Quantum Random Number Generator, QRNG) и др.

В-третьих (менее изученное и достаточно перспективное), создание и программно-техническая

1 Ширяев Михаил Виссарионович, Исполнительный директор Научного центра информационных технологий и искусственного интеллекта Научно-технологического университета «Сириус». Федеральная территория «Сириус», Россия. E-mail: shiryaev.mv@talatiuspeh.ru

реализация принципиально новых квантово-механических моделей ключевых цифровых экосистем и платформ Экономики данных Российской Федерации на физических принципах и законах квантовой механики. Так, Питер Шор, автор известного квантового алгоритма факторизации, совместно с коллегами из MIT и Harvard University в 2022 году ввел в обиход новое понятие «квантовые деньги», т.е., по сути, новый способ организации децентрализованных квантовых денег[2]. При такой организации проверка права собственности на валюту может осуществляться локально в автономном режиме, не требуя глобальной синхронизации с помощью таких механизмов, как блокчейн. Однако понятно, что оборот квантовых денег потребует создания соответствующей квантовой инфраструктуры[3]. Экосистема квантовых технологий только формируется, поэтому переход на квантово-механические модели цифровых экосистем и платформ Экономики данных Российской Федерации представляет собой достаточно дальнюю перспективу. По всей видимости, сейчас будут востребованы гибридные вычислители сверхвысокой производительности, сочетающие достоинства как известных архитектур, главным образом фон Неймана, так и квантовой архитектуры.

В предлагаемом Вашему вниманию тематическом выпуске научного журнала «Вопросы кибербезопасности» с разной степенью подробности обсуждаются все три перечисленные направления. В номере представлены лучшие авторские статьи научной группы «Квантовая информатика и информационная безопасность» Университета «Сириус», выполняющей Проект ФТС-2024-2.3-VY-1160-5744 «Технологии противодействия ранее неизвестным квантовым киберугрозам» в рамках реализации мероприятия 2.3 государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус». Также в тематическом выпуске представлены избранные статьи ведущих отечественных ученых и инженеров-практиков в области квантовых технологий (квантовых вычислений, квантовых коммуникаций и квантовой сенсорики). Существенно, что все обсуждаемые вопросы и полученные отечественными учеными и практиками научно-технические результаты соответствуют направлениям стратегии научно-технологического развития Российской Федерации и Федеральной территории «Сириус», а также сквозным информационным технологиям в рамках Национальной технологической инициативы (НТИ) и экономики данных Российской Федерации.

В работах ученых Университета «Сириус» (С.А. Петренко, К.О. Гнидко, П.В. Сундеева, Н.А. Молдовян, Я.А. Холодова, А.С. Петренко, Е.А. Ищуковой и А.А. Балябина) представлены первые весомые научно-технические результаты, полученные в ходе выполнения Проекта ФТС-2024-2.3-VY-1160-5744 «Технологии противодействия ранее неизвестным квантовым киберугрозам» под руководством ведущего ученого С.А. Петренко. В том числе, предложено и обосновано применение двух скрытых коммутативных групп для повышения производительности постквантовых алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения больших систем степенных уравнений (Н.А. Молдовян, А.С. Петренко). Это позволило разработать три новых типа постквантовых алгебраических схем ЭЦП, отличающиеся приемами обеспечения высокой стойкости к подделке подписи с использованием вектора S в качестве подгоночного параметра атаки. В первом типе используется прием экспоненцирования произведения, в которое входит вектор S в большую степень, во втором типе – выполнение операции экспоненцирования в степень, равную значению хеш-функции, вычисляемой от S, и в третьем типе – комбинирование первых двух приемов. Осуществлены алгоритмические реализации схем ЭЦП каждого типа и показана корректность разработанных алгоритмов. Выполнены оценки стойкости к прямой атаке, атаке на основе известных подписей и к подделке подписи. Представлено сравнение предложенных алгоритмов ЭЦП с известными аналогами. В качестве приемов повышения производительности алгебраических алгоритмов ЭЦП использовано 1) задание КНАА по прореженным таблицам умножения базисных векторов и 2) умножение на скалярный вектор при вычислении вектора S. Научная и практическая значимость этих результатов состоит в апробации способа усиления рандомизации подписи, включающего вычисление подгоночного элемента подписи S в зависимости от произведения двух взаимно некоммутативных векторов и одного скалярного вектора при разработке алгебраических алгоритмов трех различных типов, представляющих интерес в качестве прототипа практичного постквантового стандарта ЭЦП.

Почему это так важно? Дело в том, что сейчас основные усилия криптографов во всем мире сосредоточены на разработке и стандартизации постквантовых криптографических механизмов, которые останутся актуальными даже после появления практически релевантных квантовых компьютеров. Так, Национальный институт стандартов и технологий (NIST) США (National Institute of Standards and Technology, NIST) по результатам конкурса среди

2 https://www.discovermagazine.com/technology/why-quantum-money-could-replace-blockchain-based-cryptocurrencies
3 https://arxiv.org/abs/2207.13135

69 алгоритмов-кандидатов по выбору лучших квантово-устойчивых криптографических схем инкапсуляции ключа и цифровой подписи (2017–2024 гг.) подготовил первые четыре стандарта.

FIPS 203 (ML-KEM) – на основе алгоритма CRYSTALS-Kyber (ML-KEM), базируется на сложности решения задачи M-LWE из алгебраической теории решеток. Предназначен для общего шифрования данных, обмена ключами и отличается высокой скоростью работы и компактностью ключей.

FIPS 204 (ML-DSA) – на основе алгоритма CRYSTALS-Dilithium (ML-DSA), базируется на сложности решения задач M-LWE и M-SIS из теории решеток. Предназначен для защиты цифровых подписей и обеспечивает надежную аутентификацию.

FIPS 205 (SLH-DSA) – альтернативный стандарт для постквантовой цифровой подписи на основе алгоритма SPHINCS+(SLH-DSA), базируется на сложности нахождения прообраза криптографической хэш-функции. Характеризуется более коротким открытым ключом, но обладает меньшей производительностью по сравнению с ML-DSA.

FIPS 206 (FN-DSA) – стандарт для постквантовой цифровой подписи минимального размера на основе алгоритма FALCON (FN-DSA), базируется на сложности решения задач из теории решеток. Стандартизированный вариант алгоритма FALCON поставляется под именем FN-DSA (быстрое преобразование Фурье, FFT над NTRU-Lattice Digital Signature Algorithm).

В России также проводятся подобные исследования и разработки. Так, экспертами-криптографами российской компании «Криптонит», участвующими в деятельности рабочей группы «Постквантовые криптографические механизмы» Технического комитета 26 Росстандарта (ТК26), разработан алгоритм электронной подписи «Шиповник», устойчивый к атакам с использованием квантового компьютера. Схема электронной подписи построена методом применения преобразования Фиата-Шамира к протоколу идентификации Штерна (с нулевым разглашением). Стойкость этой схемы подписи к подделке основана на сложности задачи декодирования случайного линейного кода. Еще в 1978 году профессором математики Элвином Берлекэмпом (англ. *Elwyn Berlekamp*, 6 сентября 1940 – 9 апреля 2019) было доказано, что эта задача относится к классу NP-сложных задач. Для задач данного класса до сих пор неизвестны эффективные алгоритмы решения ни на классическом компьютере, ни на квантовом. По данным компании «Криптонит» – лучшая известная атака с использованием классического компьютера на схему «Шиповник» – потребует 2^{256} битовых операций. То есть её невозможно выполнить за разумное время на самых быстрых суперЭВМ архитектуры фон Неймана. Теоретическая стойкость к «квантовой» атаке оценивается в 2^{170} операций, что так же делает её выполнение невозможным даже на квантовых компьютерах будущего с миллиардами рабочих кубитов. Открытая реализация отечественного постквантового алгоритма «Шиповник» подготовлена совместно компаниями «Криптонит» и «QApp». Проект написан на языке Си с оптимизацией под наборы команд SSE4.1, SSE2 и MMX. Исходный код доступен на GitHub. Он компилируется в библиотеку, которую можно встраивать в промышленные криптографические устройства и программные продукты. По данным компании «QApp», использование оптимизации кода приводит к высокой скорости реализации «Шиповника». В тестах на Intel Core i7-8700 выработка ключевой пары заняла 3 мс, подпись одного сообщения — 848 миллисекунд, а проверка подписи — всего 11 мс. В настоящее время постквантовый алгоритм «Шиповник» проходит процедуру сертификации.

Учитывая все выше сказанное, можем смело считать, что результат ученых Университета «Сириус» (Н.А. Молдовян, А.С. Петренко), полученный в ходе реализации Проекта ФТС-2024-2.3-VY-1160-5744 «Технологии противодействия ранее неизвестным квантовым киберугрозам» - построение трех новых постквантовых алгоритмов ЭЦП на основе НКАА с двумя скрытыми группами и их доведение до программной реализации является значимым событием в международном криптографическом сообществе и важной вехой в развитии отечественной постквантовой криптографии. Существенно, что это позволяет создавать надёжные реализации электронной подписи, устойчивые к атакам с использованием самых мощных суперкомпьютеров традиционной архитектуры фон Неймана и ещё только разрабатываемых практически значимых квантовых компьютеров.

В работе Д.К. Смирнова (МГУ имени М.В. Ломоносова, АО «ИнфоТеКС») и И.В. Чижова (МГУ имени М.В. Ломоносова, Федеральный исследовательский центр «Информатика и управление» РАН, АО «НПК "Криптонит"») выделены уязвимые вычислительные элементы протокола — сложение векторов по модулю 2 и умножение матрицы на вектор — и проанализированы основные методы защиты этих элементов от утечек по побочным каналам, такие как маскирование, балансирование и перемешивание. Предложен способ матричного умножения, устойчивый к горизонтальной корреляционной атаке, применявшейся против криптосистемы Мак-Элиса. Установлены основные требования к реализации схемы на ПЛИС, предложена модификация схемы с маскированием ключа, не нарушающая стойкость оригинальной, позволяющая защитить секрет при краже токена и предотвращающая атаки имперсонализации благодаря маскированию. Способ генерации

маски выбран таким образом, чтобы минимизировать место, занимаемое на ПЛИС, а именно хэширование парольной фразы функцией «Стрибог-К» со счётчиком. Показано, что стойкость модифицированного протокола идентификации Штерна совпадает со стойкостью оригинального протокола в модели без утечек по побочным каналам и превосходит в модели с ними. Результаты работы позволили реализовать постквантовый алгоритм подписи «Шиповник», разрабатываемый рабочей группой ТК26 и проходящий стандартизацию в настоящее время.

В работе И. Ю. Жукова (Группа компаний «Инфотактика») с коллегами М. А. Финошиным (Национальный исследовательский ядерный университет «МИФИ») и И. Д. Ивановой (Российский университет транспорта (МИИТ), в которой рассмотрены возможные приемы ускорения алгоритмов приведения чисел по модулю в постквантовой схеме FALCON.

В работе С. П. Кулика (Центр квантовых технологий, МГУ имени М. В. Ломоносова) и С. Н. Молоткова (Институт физики твердого тела имени Ю. А. Осипьяна РАН) рассмотрены актуальные вопросы квантового распределения ключей через недоверенные узлы в квантовых сетях. Отметим, что Центр квантовых технологий на физическом факультете МГУ имени М. В. Ломоносова достаточно успешно развивает направление квантовых коммуникаций через атмосферные и волоконно-оптические каналы связи; разрабатываются варианты сетевых решений аппаратуры доверенных промежуточных узлов, однофотонные приемники и источники фотонов, высокоскоростные квантовые генераторы случайных чисел, а также проводятся исследования в ряде сопутствующих направлений. Среди них исследование влияния турбулентности атмосферы на эффективность приема оптических квантовых состояний в протоколах квантового распределения ключей (КРК), а также исследование стойкости криптографических протоколов КРК, реализованных на основе как волоконно-оптических, так и атмосферных каналов. В том числе, внесли существенный вклад в разработку и обоснование «Временных требований к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну», утвержденных 20 июля 2017 года.

Выпуск завершается работой Д. А. Кронберга и академика РАН А. С. Холево (Математический институт им. В.А. Стеклова РАН), в которой представлены новые подходы к оценкам информации перехватчика в проблемах квантовой криптографии. Д. А. Кронберг – специалист по квантовой криптографии и постселективным преобразованиям ансамблей квантовых состояний. Им был разработан ряд эффективных стратегий подслушивания для квантовой криптографии, в том числе демонстрирующих уязвимость практически используемых протоколов квантового распределения ключей. А. С. Холево — выдающийся российский математик, внесший существенный вклад в математические основы квантовой теории, некоммутативную теорию вероятностей, квантовую теорию информации, случайных процессов и статистических решений. А. С. Холево является автором прорывных результатов, повлиявших на появление и развитие квантовой информатики – науки о квантовых коммуникациях и вычислениях, пользуется в мире репутацией основоположника в этих областях. В работах А. С. Холево создана математическая теория квантовых каналов связи, доказаны фундаментальные теоремы кодирования квантовой теории информации, решена проблема квантовых гауссовских оптимизаторов, построена некоммутативная теория статистических решений. Разработана теория квантовых случайных процессов, дано описание структуры генераторов ковариантных динамических полугрупп и квантовых марковских процессов, получены функциональные предельные теоремы о сходимости серий последовательных квантовых измерений к процессу непрерывного измерения (премия А. А. Маркова РАН, международная премия Quantum Communication Award, премия А. Гумбольдта, премия К. Шеннона).

Издание тематического или специального выпуска научного журнала «Вопросы кибербезопасности» посвящено 10-летию Образовательного центра «Сириус». Надеюсь, что оно будет полезно специалистам в области квантовой информатики и информационной безопасности, а также аспирантам и студентам, интересующимся этой перспективной областью исследований.

С уважением,
Ширяев Михаил Виссарионович

ТИПОВЫЕ УРАВНЕНИЯ ВЕРИФИКАЦИИ В АЛГЕБРАИЧЕСКИХ СХЕМАХ ЭЦП С ДВУМЯ СКРЫТЫМИ ГРУППАМИ

Молдовян Н. А.[1], Петренко А. С.[2]

DOI: 10.21681/2311-3456-2025-3-8-20

Цель работы: *повышение производительности постквантовых алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения больших систем степенных уравнений.*

Метод исследования: *применение двух скрытых коммутативных групп, элементы одной из которых некоммутативны с элементами другой, для обеспечения достаточной полноты рандомизации подписи в алгебраических схемах ЭЦП, стойкость которых основана на вычислительной трудности решения больших систем степенных уравнений в простом конечном поле GF(p). Вычисление подгоночного элемента ЭЦП в виде вектора S в зависимости от взаимно некоммутативных нескалярных векторов, выбираемых из скрытых групп, и случайного скалярного вектора. Применение конечных некоммутативных ассоциативных алгебр (КНАА) с хорошо изученным строением в качестве алгебраического носителя алгоритмов ЭЦП с проверочным уравнением с многократным вхождением вектора S. Задание КНАА по прореженным таблицам умножения базисных векторов.*

Результаты исследования: *предложены три типа постквантовых алгебраических схем ЭЦП, отличающихся приемами обеспечения высокой стойкости к подделке подписи с использованием вектора S в качестве подгоночного параметра атаки. В первом типе используется прием экспоненцирования произведения, в которое входит вектор S, в большую степень, во втором типе – выполнение операции экспоненцирования в степень, равную значению хеш-функции, вычисляемой от S, и в третьем типе – комбинирование первых двух приемов. Осуществлены алгоритмические реализации схем ЭЦП каждого типа и показана корректность разработанных алгоритмов. Выполнены оценки стойкости к прямой атаке, атаке на основе известных подписей и к подделке подписи. Представлено сравнение предложенных алгоритмов ЭЦП с известными аналогами. В качестве приемов повышения производительности алгебраических алгоритмов ЭЦП использовано 1) задание КНАА по прореженным таблицам умножения базисных векторов и 2) умножение на скалярный вектор при вычислении вектора S.*

Научная и практическая значимость *результатов статьи состоит в апробации способа усиления рандомизации подписи, включающего вычисление подгоночного элемента подписи S в зависимости от произведения двух взаимно некоммутативных векторов и одного скалярного вектора, при разработке алгебраических алгоритмов трех различных типов, представляющих интерес в качестве прототипа практичного постквантового стандарта ЭЦП.*

Ключевые слова: *конечная некоммутативная алгебра; ассоциативная алгебра; вычислительно трудная задача; скрытая коммутативная группа; цифровая подпись; рандомизация подписи; постквантовая криптография.*

Введение

В настоящее время исследования и разработки в области постквантовой криптографии с открытым ключом сохраняют достаточно высокую степень актуальности [1]. В основе стойкости постквантовых криптоалгоритмов с открытым ключом, в том числе алгоритмов электронной цифровой подписи (ЭЦП), лежат вычислительно трудные задачи, отличные от факторизации и дискретного логарифмирования. Это определяется тем, что для квантового компьютера известны полиномиальные по времени алгоритмы решения двух последних задач. В области постквантовой криптографии можно выделить следующие направления: разработка криптоалгоритмов на кодах [2–4], на группах [5], на алгебраических решетках [6], на трудно обратимых функциях [7,8], на однонаправленных отображениях с секретной лазейкой [9,10] и на некоммутативных алгебрах [11,12].

Использование нелинейных трудно обратимых отображений с секретной лазейкой в качестве постквантового криптографического примитива представляет значительный интерес, поскольку это приводит к построению двухключевых криптосхем, стойкость которых основана на вычислительной трудности решения систем многих степенных уравнений с многими неизвестными [13], т.е. на задаче, для решения которой квантовый компьютер не является эффективным. Существенным практическим недостатком постквантовых алгоритмов данного типа

1 Молдовян Николай Андреевич, доктор технических наук, профессор, главный научный сотрудник Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Россия. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 6603837461. E-mail: moldovan.NA@talantiuspeh.ru

2 Петренко Алексей Сергеевич, аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), Санкт-Петербург, младший научный сотрудник Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Россия. ORCID: https://orcid.org/0000-0002-9954-4643. Scopus Author ID: 57200260915. E-mail: a.petrenko1999@rambler.ru

является большая длина открытого ключа. Даже при применении способов реализации трудно обратимых отображений как операций экспоненцирования в векторном конечном поле [14,15], которые потенциально позволяют сократить размер открытого ключа в 10 и более раз, разрабатываемые постквантовые алгоритмы ЭЦП и открытого шифрования остаются ограниченно применимыми на практике.

Сравнительно недавно предложена новая парадигма построения постквантовых алгоритмов ЭЦП, основанных на вычислительной трудности решения больших систем степенных уравнений (БССУ) [16–19]. В рамках этой парадигмы в качестве алгебраического носителя используется многомерная конечная некоммутативная ассоциативная алгебра (КНАА), в которой в качестве одного из элементов секретного ключа задается коммутативная скрытая группа. При этом цифровая подпись вычисляется в виде двух элементов (e, $\mathbf{S}$), первый из которых является рандомизирующим натуральным числом, а второй – подгоночным вектором, обеспечивающим выполнение проверочного уравнения. При этом вектор $\mathbf{S}$ входит в проверочное уравнение в качестве множителя, что создает предпосылки для атак по подделке ЭЦП с использованием $\mathbf{S}$ как подгоночного параметра атаки. Обеспечение стойкости реализуется заданием проверочных уравнений с многократным вхождением вектора $\mathbf{S}$. Эффективность такого приема обусловливается свойством некоммутативности операции умножения в КНАА.

Процедура генерации ЭЦП в алгоритмах [16–19] включает вычисление вектора $\mathbf{S}$ в зависимости от двух фиксированных секретных векторов $\mathbf{D}$ и $\mathbf{F}$ и случайного вектора $\mathbf{H}$, выбираемого из скрытой коммутативной группы, по формуле:

$$\mathbf{S} = \mathbf{DHF}, \qquad (1)$$

Выбор вектора $\mathbf{H}$ определяется значениями рандомизирующих параметров и подписываемым документом M, т.е. является уникальным для каждого значения M. Однако в работах [20,21] была показана недостаточная полнота рандомизации подписи, задаваемая по формуле (1), создающая уязвимость к атакам на основе известных подписей, и предложен способ усиления рандомизации за счет включения в формулу для вычисления вектора $\mathbf{S}$ случайного обратимого вектора $\mathbf{V}$, выбираемого из всей КНАА, используемой в качестве алгебраического носителя. Предложенные в [20,21] алгоритмы ЭЦП используют удвоенное проверочное уравнение с однократным вхождением подгоночного элемента подписи $\mathbf{S}$, что приводит к увеличению размера открытого ключа и снижению производительности алгоритма ЭЦП. Однако основным недостатком использования приема удвоения проверочного уравнения по сравнению с использованием одного уравнения верификации с многократным вхождением вектора $\mathbf{S}$ является необходимость использования дополнительного механизма обеспечения стойкости к подделке подписи (атака, включающая формирование подписи без знания секретного ключа).

Представляет интерес способ усиления рандомизации, предложенный в [22] и заключающийся в вычислении элемента подписи $\mathbf{S}$ в зависимости от взаимно некоммутативных векторов $\mathbf{P}^b$ и $\mathbf{G}^n$, выбираемых их двух скрытых коммутативных групп по уникальным значениям степеней b и n, по следующей формуле

$$\mathbf{S} = \mathbf{DP}^b\mathbf{G}^n\mathbf{F}, \qquad (2)$$

В способе [22] усиление рандомизации ЭЦП обеспечивается за счет того, что вектор, равный произведению $\mathbf{P}^b\mathbf{G}^n$ ($\mathbf{P}$ имеет порядок $p^2 - 1$, а $\mathbf{G}$ – простой порядок $(p - 1)/2$), пробегает $\approx p^3$ значений, принадлежащих различным циклическим группам, содержащимся в четырехмерной КНАА, заданной над полем $GF(p)$, где простое число $p = 2q + 1$ при простом q, и используемой в качестве алгебраического носителя. Предложенный в [22] механизм обеспечения стойкости к подделке подписи основан на взаимной некоммутативности генераторов $\mathbf{P}$ и $\mathbf{G}$ скрытых групп и включает вычисление вспомогательного параметра рандомизации в виде значения ρ хеш-функции $\mathbf{\Phi}$ от вектора $\mathbf{S}$ и использование вспомогательного подгоночного элемента подписи в виде натурального числа s, задающего степень одной из операций экспоненцирования, выполняемых в ходе процедуры верификации ЭЦП. В алгоритме [22] также используются два проверочных уравнения.

Впервые алгоритмическая реализация способа рандомизации подписи по формуле (2) и механизма защищенности от подделки ЭЦП из [22] с использованием одного проверочного уравнения выполнена в работе [23]. Представляет интерес рассмотрение дополнительных механизмов снижения вычислительной сложности процедур генерации и верификации ЭЦП. В частности, повышение производительности алгебраического алгоритма ЭЦП с двумя скрытыми группами может быть достигнуто путем двукратного уменьшения битового размера порядка вектора $\mathbf{P}$, а именно, путем выбора вектора $\mathbf{P}$, имеющего порядок, равный $p + 1$ или p.

Формализация цели исследования

Для построения алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения БССУ, в качестве алгебраического носителя будем использовать четырехмерные КНАА, заданные над конечным простым полем $GF(p)$ простого порядка $p = 2q + 1$, где q – простое 128-битное число. Такой

выбор связан с тем, что декомпозиция таких алгебр, как некоммутативных колец на коммутативные подкольца порядка p^2, хорошо изучена [12,24] и показана общность свойств их разбиения независимо от вида таблицы умножения базисных векторов (ТУБВ), по которой задается операция умножения. В частности показано, что имеются только три типа таких колец, характеризующихся строением и значением порядка ($p^2 - 1$; $(p-1)^2$ и $p(p-1)$) их мультипликативных групп. При этом эти подкольца пересекаются строго в множестве скалярных векторов. Краткая сводка общих свойств разбиения четырехмерных КНАА, важных для построения алгоритмов ЭЦП и оценивания стойкости, представлена в работе [23].

Для достижения цели повышения производительности алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения БССУ, зададим вычисление подгоночного элемента подписи по следующей формуле

$$\mathbf{S} = \mathbf{D}\mathbf{P}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F}, \qquad (3)$$

где взаимно некоммутативные векторы $\mathbf{P}$ и $\mathbf{G}$ являются генераторами циклических групп порядка $p+1$, p или q, таких, что все их элементы являются нескалярными векторами, кроме единичного элемента $\mathbf{E}$; $\mathbf{L}$ – скалярный вектор порядка $p-1$. Легко показать, что вектор, равный поизведению $\mathbf{P}^b\mathbf{G}^n\mathbf{L}^u$, принимает $\approx p^3$ различных значений, принадлежащих $\approx p^2$ различным коммутативным подкольцам, содержащимся в четырехмерной КНАА, используемой в качестве алгебраического носителя. Обоснование достаточности рандомизации, задаваемой по формуле (3), выполняется аналогично обоснованию рандомизации подписи, задаваемой по формуле (2), которое представлено в [23].

Благодаря коммутативности векторов $\mathbf{L}^u$ со всеми элементами КНАА открытый ключ может быть сформирован таким образом, что в проверочном уравнении степени операции экспоненцирования имеющие битовый размер $|p^2|$ заменяются на степени размером $|p|$ ($|x|$ обозначает длину значения x в двоичном представлении). Задачей, решаемой в настоящей работе, является разработка алгебраических алгоритмов ЭЦП с двумя скрытыми коммутативными группами с использованием способа рандомизации, задаваемого формулой (3), и одного уравнения верификации подписи. При этом разрабатываются алгоритмы трех различных типов, отличающихся использованием 1) многократного вхождения вектора $\mathbf{S}$ в проверочное уравнение, 2) вычисления значения хеш-функции $\rho = \mathbf{\Phi}(\mathbf{S})$ как одной из степеней операции экспоненцирования, присутствующей в уравнении верификации ЭЦП, или 3) комбинирования первых двух приемов.

1. Варианты задания четырехмерных КНАА

Элементами конечной m-мерной алгебры являются векторы $\mathbf{V} = (v_0, v_1, v_2, \ldots v_{m-1})$, координатами которых являются элементы некоторого конечного поля. В нашем случае рассматривается задание векторов над простым конечным полем $GF(p)$ простого порядка $p = 2q + 1$, где q – простое 128-битное число. Операция сложения векторов описывается как сложение одноименных координат. Операция умножения векторов задается таким образом, что она является замкнутой и дистрибутивной слева и справа относительно операции сложения. Для использования конечных алгебр в качестве алгебраического носителя разрабатываемых алгоритмов требуется наличие следующих дополнительных свойств:

1) существование в алгебре глобальной двухсторонней единицы;
2) некоммутативность операции умножения;
3) ассоциативность операции умножения.

При упоминании о векторе, действующем как единичный элемент на каждый элемент алгебры при умножении слева и справа, мы используем термин двухсторонний, поскольку существуют КНАА с множеством глобальных односторонних (левосторонних или правосторонних) единиц [25]. Для формирования КНАА с глобальной двухсторонней единицей можно задать операцию умножения векторов

$$\mathbf{A} = \sum_{i=0}^{m-1} a_i e_i \text{ и } \mathbf{B} = \sum_{j=0}^{m-1} b_j e_j,$$

где e_i – базисные векторы, по формуле:

$$\mathbf{AB} = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j (e_i e_j) \qquad (4)$$

где вместо произведения пары базисных векторов $\mathbf{e}_i$ и $\mathbf{e}_j$ подставляется значение некоторого однокомпонентного вектора в соответствии с некоторой ТУБВ, обеспечивающей наличие требуемых свойств. Известен способ [26] построения таких ТУБВ для произвольных четных размерностей $m > 4$. Для интересующего нас случая $m = 4$ известны различные ТУБВ, в том числе прореженные ТУБВ, в которых половина из всевозможных произведений пар базисных векторов заменяется на нулевой вектор (вектор со всеми нулевыми координатами), в результате чего операция умножения двух четырехмерных векторов выполняется всего за восемь операций умножения в поле $GF(p)$. Таблицы 1–4 представляют различные ТУБВ, задающие четырехмерные КНАА с глобальной двухсторонней единицей.

Выполненные исследования декомпозиции четырехмерных КНАА с глобальной двухсторонней единицей, заданных по многим различным ТУБВ, в том числе прореженным, на множество коммутативных подколец порядка p^2 показали идентичность строения таких КНАА [12,24,28,29]. В связи с этим

Таблица 1.

Задание операции умножения в четырехмерной КНАА ($\lambda\mu \neq 1$) [11,27]

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mu\mathbf{e}_0$	$\mu\mathbf{e}_1$
$\mathbf{e}_2$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mu\mathbf{e}_2$	$\mu\mathbf{e}_3$

Таблица 2.

Прореженная ТУБВ ($\lambda \neq 0$) для задания КНАА с глобальной двухсторонней единицей (1, 1, 0, 0) [12]

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	0	0	$\mathbf{e}_3$
$\mathbf{e}_1$	0	$\mathbf{e}_1$	$\mathbf{e}_2$	0
$\mathbf{e}_2$	$\mathbf{e}_2$	0	0	$\lambda\mathbf{e}_1$
$\mathbf{e}_3$	0	$\mathbf{e}_3$	$\lambda\mathbf{e}_0$	0

Таблица 3.

Задание (при $\lambda = 1$) операции умножения матриц 2×2 как умножения в четырехмерной КНАА ($\lambda \neq 0$)

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	0	0
$\mathbf{e}_1$	0	0	$\lambda\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\lambda\mathbf{e}_3$	0	0
$\mathbf{e}_3$	0	0	$\mathbf{e}_2$	$\mathbf{e}_3$

Таблица 4.

Задание ($\lambda \neq 0$) четырехмерной КНАА с глобальной двухсторонней единицей (0, 0, 1, 1) [29]

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	0	$\lambda\mathbf{e}_3$	$\mathbf{e}_0$	0
$\mathbf{e}_1$	$\lambda\mathbf{e}_2$	0	0	$\mathbf{e}_1$
$\mathbf{e}_2$	0	$\mathbf{e}_1$	$\mathbf{e}_2$	0
$\mathbf{e}_3$	$\mathbf{e}_0$	0	0	$\mathbf{e}_3$

для получения более высокой производительности в данной работе предполагается реализация алгоритмов ЭЦП на четырехмерных КНАА, заданных по прореженным ТУБВ, например, представленных в табл. 2–4. Существуют и другие варианты прореженных ТУБВ. Заметим, что табл. 1 при $\lambda = \mu = 0$ задает четырехмерную КНАА с глобальной двухсторонней единицей $\mathbf{E} = (0, 1, 1, 0)$, при $\lambda = 0$ и $\mu \neq 0$ – четырехмерную КНАА с глобальной двухсторонней единицей $\mathbf{E} = (-\mu, 1, 1, 0)$, а при $\lambda \neq 0$ и $\mu = 0$ – четырехмерную КНАА с глобальной двухсторонней единицей $\mathbf{E} = (0, 1, 1, -\lambda)$.

2. Алгоритм ЭЦП первого типа

В алгоритмах первого типа стойкость к подделке подписи обеспечивается двукратным или многократным вхождением подгоночного элемента подписи $\mathbf{S}$ в проверочное уравнение. При таком построении алгоритма ЭЦП подделка подписи связана с решением проверочного уравнения относительно $\mathbf{S}$ как неизвестного вектора. Важным моментом является то, что хотя бы один раз вектор $\mathbf{S}$ входит в проверочное уравнение в некоторую группу сомножителей, возводимую в степень достаточно большого размера (больше 100 бит в нашем случае). Действительно, легко видеть, что в четырехмерной КНАА при известных векторах $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$ и $\mathbf{R}$ решение векторного уравнения вида

$$\mathbf{R} = \mathbf{A}\mathbf{S}^d\mathbf{B}\mathbf{S}^h\mathbf{C}. \qquad (5)$$

Сводится к решению системы из четырех скалярных уравнений степени $d + h$ в поле $GF(p)$. Естественным способом сделать такое сведение вычислительно невыполнимым является задание хотя бы одной из степеней d и h настолько большой, что степенные скалярные уравнения будут включать число слагаемых не менее 2^{80}. Это может быть обеспечено при $|d| > 100$ и/или $|h| > 100$ бит.

В приводимом ниже алгоритме ЭЦП в проверочное уравнение входит множитель $\mathbf{S}^{-1}$, для вычисления которого по известному вектору $\mathbf{S}$ из векторного уравнения $\mathbf{SX} = \mathbf{E}$ требуется выполнить не более 100 умножений в поле $GF(p)$, что вносит несущественный вклад в вычислительную сложность процедуры верификации ЭЦП. Включение множителя $\mathbf{S}^{-1}$ вместо $\mathbf{S}$ так же несущественно увеличивает вычислительную сложность подделки подписи.

Формирование секретного ключа выполняется как генерация 1) случайного примитивного элемента α по модулю p, 2) случайных натуральных чисел $w < q$, $x < q$, $y < q$ и $z < q$ и 3) случайных обратимых, нескалярных и попарно некоммутативных векторов $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{G}$, $\mathbf{K}$ и $\mathbf{P}$, причем таких, что векторы $\mathbf{G}$ и $\mathbf{P}$ имеют порядок равный $p + 1$ и q соответственно (общий размер секретного ключа равен ≈512 байт). Для формирования открытого ключа вычисляется вспомогательный вектор $\mathbf{L} = \alpha^2\mathbf{E}$ порядка q. Открытый ключ вычисляется в виде совокупности следующих десяти четырехмерных векторов $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{U}$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$ и $\mathbf{T}_5$ (с общим размером ≈640 байт) по формулам:

$$\mathbf{Y}_1 = \mathbf{AGA}^{-1};\ \mathbf{Z}_1 = \mathbf{KG}^x\mathbf{LK}^{-1};\ \mathbf{Y}_2 = \mathbf{BP}^x\mathbf{B}^{-1};$$
$$\mathbf{Z}_2 = \mathbf{BGL}^x\mathbf{B}^{-1};\ \mathbf{U} = \mathbf{DPD}^{-1}; \quad (6)$$

$$\mathbf{T}_1 = \mathbf{AG}^w\mathbf{K}^{-1};\ \mathbf{T}_2 = \mathbf{KG}^y\mathbf{F};\ \mathbf{T}_3 = \mathbf{DP}^w\mathbf{B}^{-1};$$
$$\mathbf{T}_4 = \mathbf{BP}^y\mathbf{D}^{-1};\ \mathbf{T}_5 = \mathbf{F}^{-1}\mathbf{G}^z\mathbf{B}^{-1}. \quad (7)$$

Предполагается, что при генерации и верификации подписи используется некоторая коллизионно стойкая 512-битная хеш-функция $\mathbf{\Phi}$, которая является частью рассматриваемой постквантовой схемы ЭЦП.

Алгоритм генерации ЭЦП

Процедура генерации ЭЦП к документу M включает следующие шаги:

1. Сгенерировать случайные натуральные числа $k < p + 1$, $t < q$ и $v < q$ и вычислить значение рандомизирующего вектора-фиксатора $\mathbf{R}$ по формуле: $\mathbf{R} = \mathbf{AG}^k\mathbf{P}^t\mathbf{L}^v\mathbf{B}^{-1}$.
2. Вычислить хеш-значение от документа M с присоединенным к нему вектором $\mathbf{R}$: $e = e_1||e_2||e_3||e_4 = \mathbf{\Phi}(M, \mathbf{R})$, где 512-битное хеш-значение e представлено в виде конкатенации четырех 128-битных натуральных чисел e_1, e_2, e_3 и e_4.
3. Вычислить натуральное число

$$n: n = -z - e_4 \bmod (p + 1).$$

4. Вычислить натуральное число

$$b: b = (e_1 - 1)^{-1}(t - e_2 - w - e_1e_3x - e_1y) \bmod q.$$

5. Вычислить натуральное число

$$u: u = (e_1 - 1)^{-1}(v - e_1 - e_1e_4x) \bmod q.$$

6. По формуле (3) вычислить подгоночный элемент ЭЦП в виде вектора $\mathbf{S} = \mathbf{DP}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F}$.
7. Вычислить вспомогательный подгоночный элемент подписи в виде числа

$$s: s = (k - w - e_1x - y + n) \bmod (p + 1).$$

Сгенерированная ЭЦП к документу M представляет собой тройку значений $(e, s, \mathbf{S})$ с общим размером ≈144 байт. Вычислительная сложность процедуры генерации ЭЦП главным образом определяется четырьмя операциями возведения в 128-битную степень в четырехмерной КНАА (вычисление векторов $\mathbf{P}^t$, $\mathbf{G}^k$, $\mathbf{P}^b$ и $\mathbf{G}^n$) и двумя операциями возведения в степень в поле $GF(p)$ (вычисление скалярных векторов $\mathbf{L}^v$ и $\mathbf{L}^u$), что составляет ≈6600 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП

Проверка подлинности подписи $(e, s, \mathbf{S})$ к документу M осуществляется с использованием 640-байтного открытого ключа $(\mathbf{Y}_1, \mathbf{Z}_1, \mathbf{Y}_2, \mathbf{Z}_2, \mathbf{U}, \mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3, \mathbf{T}_4, \mathbf{T}_5)$ по следующему алгоритму:

1. Вычислить вектор $\mathbf{R}'$ по следующей формуле (проверочное уравнение):

$$\mathbf{R}' = \mathbf{Y}_1^s\mathbf{T}_1\mathbf{Z}_1^{e_1}\mathbf{T}_2\mathbf{S}^{-1}\mathbf{U}^{e_2}\mathbf{T}_3(\mathbf{Y}_2^{e_3}\mathbf{T}_4\mathbf{S}\mathbf{T}_5\mathbf{Z}_2^{e_4})^{e_1}. \quad (8)$$

2. Вычислить хеш-функцию от документа M с присоединенным к нему вектором

$$\mathbf{R}'\colon \varepsilon = \varepsilon_1||\varepsilon_1||\varepsilon_1||\varepsilon_1 = \mathbf{\Phi}(M, \mathbf{R}'),$$

где 512-битное хеш-значение представлено в виде конкатенации четырех 128-битных чисел ε_1, ε_2, ε_3 и ε_4.
3. Если одновременно выполняются равенства $\varepsilon_1 = e_1$, $\varepsilon_2 = e_2$, $\varepsilon_3 = e_3$ и $\varepsilon_4 = e_4$, то подпись принимается как подлинная, иначе она отвергается как ложная.

Вычислительную сложность процедуры верификации ЭЦП можно оценить как шесть операций возведения четырехмерных векторов в 128-битную степень, что составляет ≈9200 операций умножения в поле $GF(p)$. Корректность этого алгоритма ЭЦП доказывается подстановкой в проверочное уравнение (8) элементов открытого ключа, выраженных через элементы секретного ключа, следующим образом.

Доказательство корректности алгоритма ЭЦП первого типа

Подставляя в проверочное уравнение (8) элементы открытого ключа, выраженные через элементы секретного ключа по формулам (6) и (7), для корректно сгенерированной подписи получаем:

$$\mathbf{R}' = \mathbf{Y}_1^s\mathbf{T}_1\mathbf{Z}_1^{e_1}\mathbf{T}_2\,\mathbf{S}^{-1}\mathbf{U}^{e_2}\mathbf{T}_3(\mathbf{Y}_2^{e_3}\mathbf{T}_4\mathbf{S}\,\mathbf{T}_5\mathbf{Z}_2^{e_4})^{e_1} =$$
$$= (\mathbf{AG}\,\mathbf{A}^{-1})^s\mathbf{A}\,\mathbf{G}^w\,\mathbf{K}^{-1}(\mathbf{K}\,\mathbf{G}^x\mathbf{L}\,\mathbf{K}^{-1})^{e_1}\mathbf{K}\,\mathbf{G}^y\mathbf{F}\times$$
$$\times(\mathbf{F}^{-1}\mathbf{L}^{-u}\mathbf{G}^{-n}\mathbf{P}^{-b}\mathbf{D}^{-1})\,(\mathbf{DP}\,\mathbf{D}^{-1})^{e_2}\,\mathbf{D}\,\mathbf{P}^w\mathbf{B}^{-1})\times$$
$$\times[(\mathbf{B}\,\mathbf{P}^x\mathbf{B}^{-1})^{e_3}\mathbf{B}\,\mathbf{P}^y\mathbf{D}^{-1}\,(\mathbf{D}\,\mathbf{P}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F})\,\mathbf{F}^{-1}\mathbf{G}^z\mathbf{B}^{-1}\times$$
$$\times(\mathbf{BG}\,\mathbf{L}^x\mathbf{B}^{-1})^{e_4}]^{e_1} = \mathbf{A}\,\mathbf{G}^s\mathbf{G}^w\mathbf{G}^{xe_1}\mathbf{L}^{e_1}\mathbf{G}^y\mathbf{L}^{-u}\mathbf{G}^{-n})\times$$
$$\times\,\mathbf{P}^{-b}\mathbf{P}^{e_2}\mathbf{P}^w\mathbf{B}^{-1}(\mathbf{B}\,\mathbf{P}^{xe_3}\mathbf{P}^y\mathbf{P}^b\mathbf{L}^u\mathbf{G}^n\mathbf{G}^z\mathbf{G}^{e_4}\mathbf{L}^{xe_4}\mathbf{B}^{-1})^{e_1} =$$
$$= \mathbf{A}\,\mathbf{G}^{s+w+xe_1+y-n}\mathbf{L}^{e_1-u}\mathbf{P}^{-b+e_2+w}\mathbf{B}^{-1}\times$$
$$(\mathbf{B}\,\mathbf{P}^{xe_3+y+b}\mathbf{G}^{n+z+e_4}\mathbf{L}^{u+xe_4}\mathbf{B}^{-1})^{e_1} = \mathbf{A}\,\mathbf{G}^{(k-w-xe_1-y+n)+w+xe_1+y-n}\times$$
$$\times\,\mathbf{L}^{e_1-u}\mathbf{P}^{-b\,+\,e_2\,+\,w}\,\mathbf{B}^{-1}(\mathbf{B}\,\mathbf{P}^{xe_3+y+b}\mathbf{G}^0\,\mathbf{L}^{u+xe_4}\mathbf{B}^{-1})^{e_1} =$$
$$= \mathbf{A}\,\mathbf{G}^k\mathbf{P}^{-b+e_2+w+e_1(xe_3+y+b)}\mathbf{L}^{e_1-u+e_1u+xe_4e_1}\mathbf{B}^{-1} =$$
$$= \mathbf{A}\,\mathbf{G}^k\mathbf{P}^t\mathbf{L}^v\mathbf{B}^{-1} = \mathbf{R}.$$

С учетом равенства $\mathbf{R} = \mathbf{R}'$ имеем $\varepsilon_1||\varepsilon_2||\varepsilon_3||\varepsilon_4 = \mathbf{\Phi}(M, \mathbf{R}') = \mathbf{\Phi}(M, \mathbf{R}) = e_1||e_2||e_3||e_4$, т. е. корректно сгенерированная подпись проходит процедуру верификации как подлинная подпись, что означает корректность разработанного алгоритма ЭЦП.

3. Алгоритмы ЭЦП второго типа

Второй тип алгебраических алгоритмов ЭЦП с двумя скрытыми группами характеризуется тем, что стойкость к атакам типа подделка подписи обеспечивается наличием в проверочном уравнении операций экспоненцирования, степень которых вычисляется как значение 128-битной хеш-функции $\mathbf{\Phi}''(\mathbf{S})$, вычисляемое от подгоночного элемента подписи $\mathbf{S}$. Формирование секретного ключа выполняется как генерация 1) случайного примитивного элемента

α по модулю p, 2) случайных натуральных чисел $w < q$, $x < q$, $y < q$ и $z < q$ и 3) случайных обратимых, нескалярных и попарно некоммутативных векторов $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{G}$, $\mathbf{K}$ и $\mathbf{P}$, причем таких, что векторы $\mathbf{G}$ и $\mathbf{P}$ имеют порядок равный $p + 1$ и q соответственно (общий размер секретного ключа равен ≈512 байт). Для формирования открытого ключа вычисляется вспомогательный вектор $\mathbf{L} = \alpha^z\mathbf{E}$. Открытый ключ вычисляется в виде совокупности следующих восьми четырехмерных векторов $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, и $\mathbf{T}_4$ (с общим размером ≈512 байт) по формулам:

$$\mathbf{Y}_1 = \mathbf{APA}^{-1};\ \mathbf{Z}_1 = \mathbf{FGF}^{-1};$$
$$\mathbf{Y}_2 = \mathbf{KG}^x\mathbf{K}^{-1};\ \mathbf{Z}_2 = \mathbf{BG}^y\mathbf{B}^{-1}; \quad (9)$$

$$\mathbf{T}_1 = \mathbf{AP}^x\mathbf{D}^{-1};\ \mathbf{T}_2 = \mathbf{FG}^w\mathbf{K}^{-1};$$
$$\mathbf{T}_3 = \mathbf{KP}^w\mathbf{D}^{-1};\ \mathbf{T}_4 = \mathbf{F}^{-1}\mathbf{G}^z\mathbf{B}^{-1}. \quad (10)$$

Алгоритм генерации ЭЦП

При генерации подписи к документу M выполняются следующие шаги:

1. Выбрать случайные натуральные числа $k < p + 1$, $t < q$ и $v < q$ и вычислить вектор $\mathbf{R} = \mathbf{AP}^t\mathbf{G}^k\mathbf{L}^v\mathbf{B}^{-1}$.
2. Используя некоторую специфицированную 256-битную хеш-функцию $\mathbf{\Phi}'$, вычислить хеш-значение $e = e_1||e_2 = \mathbf{\Phi}'(M, \mathbf{R})$, представленное в виде конкатенации двух 128-битных натуральных чисел e_1 и e_2.
3. Вычислить натуральную степень

$$n\colon n = k - z - ye_2 \bmod (p + 1).$$

4. Вычислить натуральное число

$$b\colon b = 2^{-1}(t - e_1 - x - w) \bmod q.$$

5. Вычислить натуральное число u: $u = 2^{-1}\ v \bmod q$.
6. По формуле (3) вычислить подгоночный элемент ЭЦП $\mathbf{S}$: $\mathbf{S} = \mathbf{DP}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F}$.
7. Вычислить вспомогательное рандомизирующее значение $\rho = \mathbf{\Phi}''(\mathbf{S})$.
8. Вычислить вспомогательный подгоночный элемент ЭЦП в виде числа

$$s\colon s = -(n + w + x\rho) \bmod (p + 1).$$

Сгенерированная ЭЦП к документу M представляет собой тройку значений $(e, s, \mathbf{S})$ с общим размером ≈112 байт. Вычислительная сложность процедуры генерации ЭЦП может быть оценена как четыре экспоненциирования в 128-битную степень в четырехмерной КНАА (вычисление векторов $\mathbf{P}^t$, $\mathbf{G}^k$, $\mathbf{P}^b$ и $\mathbf{G}^n$) и две операции возведения в степень в поле $GF(p)$ (вычисление скалярных векторов $\mathbf{L}^v$ и $\mathbf{L}^u$), что составляет ≈6600 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП

Проверка подлинности подписи $(e, s, \mathbf{S})$ к документу M осуществляется с использованием 512-байтного открытого ключа ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$) по следующему алгоритму:

1. Вычислить значение 128-битной хеш-функции $\mathbf{\Phi}''(\mathbf{S}) = \rho$ и вектор $\mathbf{R}'$ по следующей формуле (проверочное уравнение):

$$\mathbf{R}' = \mathbf{Y}_1^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{Z}_1^s\mathbf{T}_2\mathbf{Y}_2^{\mathbf{\Phi}''(\mathbf{S})}\mathbf{T}_3\mathbf{S}\mathbf{T}_4\mathbf{Z}_2^{e_2}. \quad (11)$$

2. Вычислить хеш-функцию от документа M с присоединенным к нему вектором

$$\mathbf{R}'\colon \varepsilon = \varepsilon_1||\varepsilon_2 = \mathbf{\Phi}'(\mathrm{M}, \mathbf{R}'),$$

где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных чисел ε_1 и ε_2.

3. Если одновременно выполняются равенства $\varepsilon_1 = e_1$ и $\varepsilon_2 = e_2$, то подпись принимается как подлинная, иначе она отклоняется.

Вычислительную сложность процедуры верификации ЭЦП можно оценить как четыре операции возведения четырехмерных векторов в 128-битную степень, что составляет ≈6150 операций умножения в поле $GF(p)$. Корректность этого алгоритма ЭЦП доказывается подстановкой в проверочное уравнение (11) элементов открытого ключа, выраженных через элементы секретного ключа по формулам (9) и (10).

Доказательство корректности алгоритма ЭЦП второго типа

Из проверочного уравнения (11) с учетом формул (9) и (10) для корректно вычисленной подписи $(e, s, \mathbf{S})$ получаем:

$$\mathbf{R}' = \mathbf{Y}_1^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{Z}_1^s\mathbf{T}_2\mathbf{Y}_2^{\mathbf{\Phi}''(\mathbf{S})}\mathbf{T}_3\mathbf{S}\mathbf{T}_4\mathbf{Z}_2^{e_2} =$$
$$= (\mathbf{APA}^{-1})^{e_1}\mathbf{AP}^x\mathbf{D}^{-1}(\mathbf{DP}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F})\ (\mathbf{FGF}^{-1})^s \times$$
$$\times\ \mathbf{FG}^w\mathbf{K}^{-1}(\mathbf{KG}^x\mathbf{K}^{-1})^\rho\mathbf{KP}^w\mathbf{D}^{-1}(\mathbf{DP}^b\mathbf{G}^n\mathbf{L}^u\mathbf{F}) \times$$
$$\times\ \mathbf{F}^{-1}\mathbf{G}^z\mathbf{B}^{-1}\ (\mathbf{BG}^y\mathbf{B}^{-1})^{e_2} = \mathbf{AP}^{e_1+x+u}\mathbf{G}^{n+s+w+x\rho}\mathbf{P}^{w+b} \times$$
$$\times\ \mathbf{G}^{n+z+ye_2}\mathbf{L}^{2u}\mathbf{B}^{-1} = \mathbf{AP}^{e_1+x+b}\mathbf{G}^{n+(-n-w-x\rho)+w+x\rho}\mathbf{P}^{w+b} \times$$
$$\mathbf{G}^{(k-z-ye_2)+z+ye_2}\mathbf{L}^{2u}\mathbf{B}^{-1} = \mathbf{AP}^{e_1+x+b}\mathbf{G}^0\mathbf{P}^{w+b}\mathbf{G}^k\mathbf{L}^{2u}\mathbf{B}^{-1} =$$
$$= \mathbf{AP}^{e_1+x+2b+w}\mathbf{G}^k\mathbf{L}^{2u}\mathbf{B}^{-1} = \mathbf{AP}^{e_1+x+(t-e_1-x-w)+w}\mathbf{G}^k\mathbf{L}^{2u}\mathbf{B}^{-1} =$$
$$= \mathbf{AP}^t\mathbf{G}^k\mathbf{L}^v\mathbf{B}^{-1} = \mathbf{R}.$$

С учетом равенства $\mathbf{R} = \mathbf{R}'$ имеем

$$\varepsilon_1||\varepsilon_2 = \mathbf{\Phi}(M, \mathbf{R}') = \mathbf{\Phi}(M, \mathbf{R}) = e_1||e_2,$$

т. е. корректно сгенерированная подпись проходит процедуру верификации как подлинная подпись, что означает корректность разработанного алгоритма ЭЦП.

4. Алгоритмы ЭЦП третьего типа

В третьем типе алгебраических алгоритмов ЭЦП, основанных на вычислительной сложности решения БССУ, объединяются приемы обеспечения стойкости к подделке подписи, используемые по отдельности в алгоритмах первого и второго типов. Секретный ключ и вспомогательный скалярный вектор $\mathbf{L}$ формируются в точности, как и в алгоритме первого типа

(см. раздел 2). Элементы открытого ключа ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{U}$, $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$, $\mathbf{T}_5$) вычисляются по следующим формулам:

$$\mathbf{Y}_1 = \mathbf{APA}^{-1};\ \mathbf{Z}_1 = \mathbf{KG}^{y}\mathbf{K}^{-1};\ \mathbf{Y}_2 = \mathbf{BG}^{z}\mathbf{B}^{-1};$$

$$\mathbf{Z}_2 = \mathbf{BGB}^{-1};\ \mathbf{U} = \mathbf{DP}^{x}\mathbf{D}^{-1};\ \mathbf{T}_0 = \mathbf{AP}^{y}\mathbf{L}^{x}\mathbf{B}^{-1}; \quad (12)$$

$$\mathbf{T}_1 = \mathbf{AP}^{w}\mathbf{D}^{-1};\ \mathbf{T}_2 = \mathbf{F}^{-1}\mathbf{G}^{x}\mathbf{K}^{-1};\ \mathbf{T}_3 = \mathbf{KG}^{w}\mathbf{A}^{-1};$$
$$\mathbf{T}_4 = \mathbf{BG}^{y}\mathbf{P}^{z}\mathbf{D}^{-1};\ \mathbf{T}_5 = \mathbf{F}^{-1}\mathbf{G}^{z}\mathbf{L}^{w}\mathbf{B}^{-1}. \quad (13)$$

Размер открытого ключа равен ≈704 байт.

Алгоритм генерации ЭЦП

При генерации подписи к документу M выполняются следующие шаги:

1. Сгенерировать случайные натуральные числа $k < p + 1$, $t < q$ и $v < q$ и вычислить вектор $\mathbf{R} = \mathbf{AP}^{t}\mathbf{G}^{k}\mathbf{L}^{v}\mathbf{B}^{-1}$.
2. Используя некоторую специфицированную 256-битную хеш-функцию $\mathbf{\Phi}'$, вычислить хеш-значение $e = e_1||e_2 = \mathbf{\Phi}'(M, \mathbf{R})$, представленное в виде конкатенации двух 128-битных натуральных чисел e_1 и e_2.
3. Вычислить натуральную степень

$$n: n = -x - ye_2 - w \bmod (p + 1).$$

4. Вычислить натуральную степень

$$b: b = -z - e_1 x \bmod q.$$

5. Вычислить первый вспомогательный подгоночный элемент подписи

$$s: s = (t - y)(e_1 + w + b)^{-1} \bmod q.$$

6. Вычислить натуральную степень

$$u: u = (v - x - w)(s + 1)^{-1} \bmod q.$$

7. По формуле (3) вычислить основной подгоночный элемент ЭЦП $\mathbf{S}$: $\mathbf{S} = \mathbf{DP}^{b}\mathbf{G}^{n}\mathbf{L}^{u}\mathbf{F}$.
8. Вычислить вспомогательное рандомизирующее значение $\rho = \mathbf{\Phi}''(\mathbf{S})$.
9. Вычислить вспомогательный подгоночный элемент ЭЦП в виде числа

$$\sigma: \sigma = (k - z\rho - y - n - z) \bmod (p + 1).$$

Сгенерированная ЭЦП к документу M представляет собой четверку значений (e, s, σ, $\mathbf{S}$) с общим размером ≈128 байт. Вычислительная сложность процедуры генерации ЭЦП может быть оценена как четыре операции возведения в 128-битную степень в четырехмерной КНАА (вычисление векторов $\mathbf{P}^{t}$, $\mathbf{G}^{k}$, $\mathbf{P}^{b}$ и $\mathbf{G}^{n}$) и две операции возведения в степень в поле $GF(p)$ (вычисление скалярных векторов $\mathbf{L}^{v}$ и $\mathbf{L}^{u}$), что составляет ≈6530 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП

Проверка подлинности подписи $(e, s, \sigma, \mathbf{S})$ к документу M осуществляется с использованием 704-байтного открытого ключа ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{U}$, $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$, $\mathbf{T}_4$, $\mathbf{T}_5$) по следующему алгоритму:

1. Вычислить значение 128-битной хеш-функции $\mathbf{\Phi}''(\mathbf{S}) = \rho$ и вектор $\mathbf{R}'$ по следующей формуле (проверочное уравнение):

$$\mathbf{R}' = (\mathbf{Y}_1^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{T}_2\mathbf{Z}_1^{e_2}\mathbf{T}_3)^{s}\mathbf{T}_0\mathbf{Y}_2^{\Phi''(\mathbf{S})}\mathbf{T}_4\mathbf{U}^{e_1}\mathbf{S}\mathbf{T}_5\mathbf{Z}_2^{\sigma}. \quad (14)$$

2. Вычислить хеш-функцию от документа M с присоединенным к нему вектором

$$\mathbf{R}'\colon \varepsilon = \varepsilon_1||\varepsilon_2 = \mathbf{\Phi}'(M, \mathbf{R}'),$$

где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных чисел ε_1 и ε_2.
3. Если одновременно выполняются равенства $\varepsilon_1 = e_1$ и $\varepsilon_2 = e_2$, то подпись принимается как подлинная, иначе она отклоняется.

Вычислительную сложность процедуры верификации ЭЦП можно оценить как шесть операций возведения четырехмерных векторов в 128-битную степень, что составляет ≈9200 операций умножения в поле $GF(p)$. Корректность этого алгоритма ЭЦП доказывается подстановкой в проверочное уравнение (14) элементов открытого ключа, выраженных через элементы секретного ключа по формулам (12) и (13).

Доказательство корректности алгоритма ЭЦП третьего типа

Из проверочного уравнения (14) с учетом формул (12) и (13) для корректно вычисленной подписи (e, s, σ, $\mathbf{S}$) получаем:

$$\mathbf{R}\text{^}' = (\mathbf{Y}_1^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{T}_2\mathbf{Z}_1^{e_2}\mathbf{T}_3)^{s}\mathbf{T}_0\mathbf{Y}_2^{\Phi''(\mathbf{S})}\mathbf{T}_4\mathbf{U}^{e_1}\mathbf{S}\mathbf{T}_5\mathbf{Z}_2^{\sigma} =$$
$$= [(\mathbf{APA}^{-1})^{e_1}\mathbf{AP}^{w}\mathbf{D}^{-1}(\mathbf{DP}^{b}\mathbf{G}^{n}\mathbf{L}^{u}\mathbf{F}) \times$$
$$\times \mathbf{F}^{-1}\mathbf{G}^{x}\mathbf{K}^{-1}(\mathbf{KG}^{y}\mathbf{K}^{-1})^{e_2}\mathbf{KG}^{w}\mathbf{A}^{-1}]^{s}\mathbf{AP}^{y}\mathbf{L}^{x}\mathbf{B}^{-1} \times$$
$$(\mathbf{BG}^{z}\mathbf{B}^{-1})^{\rho}\mathbf{BG}^{y}\mathbf{P}^{z}\mathbf{D}^{-1}(\mathbf{DP}^{x}\mathbf{D}^{-1})^{e_1}(\mathbf{DP}^{b}\mathbf{G}^{n}\mathbf{L}^{u}\mathbf{F}) \times$$
$$\mathbf{F}^{-1}\mathbf{G}^{z}\mathbf{L}^{w}\mathbf{B}^{-1}(\mathbf{BGB}^{-1})^{\sigma} =$$
$$= (\mathbf{AP}^{e_1+w+b}\mathbf{G}^{n+x+ye_2+w}\mathbf{L}^{u}\mathbf{A}^{-1})^{s}\mathbf{AP}^{y}\mathbf{L}^{x} \times$$
$$\times \mathbf{G}^{\rho z+y}\mathbf{P}^{z+xe_1+b}\mathbf{G}^{n+z+\sigma}\mathbf{L}^{u+w}\mathbf{B}^{-1} =$$
$$= (\mathbf{AP}^{e_1+w+b}\mathbf{G}^{0}\mathbf{L}^{u}\mathbf{A}^{-1})^{s}\mathbf{AP}^{y}\mathbf{G}^{\rho z+y}\mathbf{P}^{0}\mathbf{G}^{n+z+\sigma}\mathbf{L}^{u+w+x}\mathbf{B}^{-1} =$$
$$= \mathbf{AP}^{s(e_1+w+b)}\mathbf{L}^{su}\mathbf{P}^{y}\mathbf{G}^{\rho z+y+n+z+\sigma}\mathbf{L}^{u+w+x}\mathbf{B}^{-1} =$$
$$= \mathbf{AP}^{s(e_1+w+b)+y}\mathbf{G}^{k}\mathbf{L}^{u(s+1)+w+x}\mathbf{B}^{-1} = \mathbf{AP}^{t}\mathbf{G}^{k}\mathbf{L}^{v}\mathbf{B}^{-1} =$$
$$= \mathbf{R} \Rightarrow \varepsilon_1||\varepsilon_2 = \mathbf{\Phi}'(M,\mathbf{R}') = \mathbf{\Phi}'(M,\mathbf{R}) = e_1||e_2.$$

5. Обсуждение

Стойкость представленных типовых алгебраических алгоритмов ЭЦП основана на вычислительной трудности решения БССУ. Данная вычислительная задача достаточно хорошо изучена. Интерес к ней

возник с появлением криптоалгоритмов с открытым ключом, основанных на трудно обратимых отображениях с секретной лазейкой в 1988 году. К настоящему времени появились многочисленные алгоритмы открытого шифрования и ЭЦП, относящиеся к этому классу криптоалгоритмов, которые рассматриваются как постквантовые криптосхемы, поскольку применение квантового компьютера для решения БССУ не является эффективным. Предложенные в настоящей работе алгоритмы ЭЦП могут быть рассмотрены как кандидаты на прототипы практичных постквантовых стандартов ЭЦП. Их практичность связана с тем, что они обладают достаточно малыми размерами открытого ключа и подписи по сравнению с многочисленными известными постквантовыми алгоритмами. В рамках класса двухключевых криптосхем, использующих вычислительную трудность решения БССУ, алгебраические алгоритмы на КНАА свободны от существенного недостатка, чрезвычайно большого размера открытого ключа, который характерен криптоалгоритмам на трудно обратимых отображениях с секретной лазейкой.

Формула (3) обеспечивает принятие вектором $\mathbf{S}$ примерно p^3 различных обратимых значений в КНАА, используемой в качестве алгебраического носителя, что легко доказывается с использованием утверждений, доказанных в работе [23]. При этом эти значения распределяются по $\approx p^2$ различным коммутативным подалгебрам, на которые разбивается КНАА. Обоснование достаточности рандомизации, обеспечиваемое формулой (3) выполняется аналогично тому, как это сделано в [23]. Действительно, легко показать, что (3) сводится к формуле рандомизации подписи, использованной в [23], если учесть, что вектор, равный произведению $\mathbf{G}^k\mathbf{L}^u$, принимает значения в коммутативной группе порядка $p^2 - 1$. Достаточная полнота рандомизации подписи, обеспечиваемая формулой (3) показывает, что все три предложенных типовых алгоритма ЭЦП с двумя скрытыми группами являются стойкими к атакам на основе известных подписей, т.е. по совокупности известных подписей вычислительно невыполнимо нахождение секретных векторов $\mathbf{D}$, $\mathbf{F}$, $\mathbf{G}$, $\mathbf{P}$ и $\mathbf{L}$.

Следует отметить, что выполнение трех операций возведения в степень в формуле (3) практически не приводит к увеличению вычислительной сложности шага вычисления подгоночного элемента подписи $\mathbf{S}$ по сравнению с аналогичным шагом в алгоритме из [23], поскольку каждый из векторов $\mathbf{G}$, $\mathbf{P}$ и $\mathbf{L}$ возводится в 128-битную степень, тогда как в [23] выполняются две операции экспоненциирования – в 128-битную и в 256-битную степень. Введение скалярного множителя в формулы для вычисления рандомизирующего вектора-фиксатора и элементов открытого ключа позволило использовать проверочное уравнение с операциями возведения только в 128-битную степень, тогда как в алгоритме-прототипе используются также и операции возведения в 256-битую степень. В целом достигается существенное повышение производительности процедуры верификации подписи.

В использованном механизме рандомизации принципиальным моментом является использование двух скрытых коммутативных групп, которые взаимно некоммутативны. Выбор вектора $\mathbf{P}'$, принадлежащего одной из скрытых групп задается выбором некоторых степеней t и v' $(0 < t < q$ и $0 < v' < q)$ и вычислением вектора $\mathbf{P}' = \mathbf{P}^t\mathbf{L}^{v'}$, а элемента $\mathbf{G}'$ из второй – выбором некоторых степеней k и v'' $(0 < k < p + 1$ и $0 < v'' < q)$ и вычислением вектора $\mathbf{G}' = \mathbf{G}^k\mathbf{L}^{v''}$. Элементы открытого ключа вычисляются как замаскированные элементы скрытых групп при использовании умножения слева и справа на секретные векторы (маскирующие множители), причем при вычислении элементов открытого ключа, над которыми выполняется операция экспоненциирования в проверочном уравнении, левый и правый маскирующие множители являются взаимно обратными. Выбор маскирующих множителей осуществляется таким образом, что при записи элементов открытого ключа в проверочном уравнении, выраженных как произведения наборов секретных векторов, все пары соседних маскирующих множителей сокращаются и образуется длинная цепочка множителей, с некоторой очередностью выбираемых их двух взаимно некоммутативных скрытых групп. Это легко заметить при рассмотрении доказательства корректности каждого из трех предложенных типовых алгоритмов ЭЦП с двумя скрытыми группами. При этом наличие чередования множителей, принадлежащих взаимно некоммутативным скрытым группам, представляется имеющим принципиальное значение для обеспечения стойкости к гипотетическим атакам на основе потенциально возможных эквивалентных ключей. Наличие указанного чередования обусловливает необходимость задания в схеме ЭЦП дополнительного подгоночного элемента подписи s, за счет которого обеспечивается возможность вычисления значений ЭЦП, удовлетворяющих проверочному уравнению. (В алгоритмах ЭЦП, сочетающих в себе два различных механизма обеспечения стойкости к подделке подписи, возникает необходимость задания второго дополнительного подгоночного элемента подписи σ). В алгебраических алгоритмах ЭЦП

Таблица 5.

Сравнение предложенных алгоритмов ЭЦП с известными аналогами на четырехмерных КНАА

Алгоритм	Размер открытого ключа, байт	Размер подписи, байт	Сложность генерации подписи, умножений в $GF(p)$	Сложность верификации подписи, умножений в $GF(p)$	Уровень стойкости к прямой атаке
Первого типа	640	144	6600	9200	$>2^{100}$
Второго типа	512	112	6600	9200	$\approx 2^{100}$
Третьего типа	704	128	6530	7680	$\approx 2^{128}$
[17]	256	113	12300	9220	$<2^{80}$
[19]	768	160	49200	13800	$\approx 2^{80}$
[23]	512	144	9200	13800	$\approx 2^{100}$

с одной скрытой группой такой необходимости нет [17–19].

Прямой атакой на каждый из трех типовых разработанных алгебраических алгоритмов ЭЦП является решение системы векторных степенных уравнений, связывающих элементы открытого ключа с секретными векторами (элементами секретного ключа). Решение системы векторных степенных уравнений сводится к решению систем скалярных степенных уравнений. При этом знание декомпозиции четырехмерных КНАА с глобальной двухсторонней единицей на коммутативные подалгебры позволяет существенно уменьшить число скалярных степенных уравнений в решаемой БССУ, как это показано, например, в [23]. Применяя методику [23] оценивания стойкости к прямой атаке, были получены данные, представленные в табл. 5.

Наиболее близким аналогом для предложенных алгоритмов ЭЦП является описанный в работе [23]. В алгоритмах из работ [17] и [19], которые также уступают по производительности предложенным в настоящей статье, используется только одна скрытая коммутативная группа и рандомизация подписи является ограниченной, из-за чего имеет место уязвимость к атаке на основе известных подписей [20]. Эти сравнения показывают, что использованный прием выделения скалярного множителя $\mathbf{L}^u$ в формуле (3) и скалярного множителя $\mathbf{L}^v$ в формуле для вычисления рандомизирующего вектора-фиксатора $\mathbf{R}$ (см. п. 1 в процедурах генерации ЭЦП каждого из трех описанных типовых алгоритмов) позволяет существенно снизить вычислительную сложность процедур генерации и верификации ЭЦП и тем самым повысить производительность.

Естественным способом повышения уровня стойкости предложенных алгоритмов является их реализация на КНАА с размерностью $m > 4$, что приводит к существенному увеличению размера БССУ, сложность решения которых лежит в основе стойкости. Для случая $m = 6$ ($m = 8$) число совместно решаемых скалярных степенных уравнений возрастает в полтора (два) раза, что для алгоритма третьего типа соответствует уровню стойкости 2^{192} (2^{256}) к прямой атаке. Однако утверждение о решении проблемы разработки способов построения практичных постквантовых алгоритмов ЭЦП было бы преждевременным, поскольку, как показывает история многих известных криптосхем, требуются годы всесторонних исследований стойкости к различным возможным атакам до того, как криптосхемы нового типа признаются апробированными. Выполненные в данной работе разработки трех типовых алгебраических алгоритмов с двумя скрытыми группами являются шагом в направлении развития способа построения постквантовых схем ЭЦП, использующих в качестве алгебраического носителя КНАА. Достоинства алгебраических алгоритмов ЭЦП с двумя скрытыми группами представляются достаточным обоснованием для ожидания того, что в связи с актуальностью проблемы разработки практичного постквантового стандарта ЭЦП, они обусловят интерес к их анализу и использованию в качестве прототипов при разработке новых постквантовых схем ЭЦП со стороны независимых исследователей.

Выводы

Предложены три типа алгебраических алгоритмов ЭЦП с двумя скрытыми группами, отличающиеся различными механизмами обеспечения стойкости

к подделке подписи, в которых в качестве алгебраического носителя используются четырехмерные КНАА с операцией умножения, заданной по прореженным ТУБВ. Последнее является одним из использованных приемов повышения производительности алгоритмов. Второй использованный прием состоит в выделении скалярного множителя в формулах для вычисления подгоночного элемента ЭЦП, вектора-фиксатора и элементов открытого ключа, за счет чего обеспечивается возможность уменьшения (по сравнению с прототипом [23]) в два раза размера степеней операций экспоненциирования, выполняемых в процедурах генерации и верификации ЭЦП.

В качестве одного из дальнейших направлений развития постквантовых схем ЭЦП с двумя скрытыми группами является изучение особенностей их реализации на КНАА, обладающих размерностью размерности $m = 6$ и более.

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение №23–03 от 27.09.2024 г.)

Литература

1. Post-Quantum Cryptography. 15th International Conference, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings. Lecture Notes in Computer Science. 2024. V. 14771–14772. Springer, Cham.
2. Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme. Designs, Codes and Cryptography. 2017. V. 82. N. 1–2. P. 469–493.
3. Vedenev K.. Kosolapov Yu. Code-based cryptography // Lecture Notes in Computer Science. 2023. Vol. 14311. P. 35–55. DOI: 10.1007/978-3-031-46495-9_3.
4. D'Alconzo G. On two modifications of the McEliece PKE and the CFS signature scheme // International Journal of Foundations of Computer Science. 2024. Vol. 35. N. 5. P. 501–512. DOI: 10.1142/S0129054123500132.
5. Battarbee C., Kahrobaei D., Perret L., Shahandashti S.F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures // In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023 / Lecture Notes in Computer Science, 2023. V. 14154. P. 113–138. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_5.
6. Gärtner J. NTWE: A Natural Combination of NTRU and LWE // In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023 / Lecture Notes in Computer Science, 2023, vol 14154, pp. 321–353. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_12.
7. Li L., Lu X., Wang K. Hash-based signature revisited // Cybersecurity. 2022. V. 5. No. 13. https://doi.org/10.1186/s42400-022-00117-w.
8. Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing // In: Ding, J., Steinwandt, R. (eds) Post-Quantum Cryptography. PQCrypto 2019 / Lecture Notes in Computer Science. 2019. V. 11505. P. 329–349. Springer, Cham. https://doi.org/10.1007/978-3-030-25510-7_18.
9. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. Vol. 80. P. 7–23. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2.
10. Hashimoto Y. Recent Developments in Multivariate Public Key Cryptosystems // In: Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., Ikematsu, Y. (eds) International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry, 2021. Vol. 33. P. 209–229. Springer, Singapore. https://doi.org/10.1007/978-981-15-5191-8_16.
11. Moldovyan D.N. New Form of the Hidden Logarithm Problem and Its Algebraic Support // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. Vol. 93. No. 2. P. 3–10.
12. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. Vol. 29. No. 2(86). P. 206–226.
13. Ding J., Petzoldt A., Schmidt D.S. Solving Polynomial Systems // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. 2020. V. 80. P. 185–248. https://doi.org/10.1007/978-1-0716-0987-3_8.
14. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. No. 3 (103). P. 80–89. DOI: https://doi.org/10.56415/basm.y2023.i3.p80.
15. Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. V. 32. N. 1(94). P. 46–60. DOI: 10.56415/csjm.v32.04.
16. Moldovyan A.A., Moldovyan D.N. A New Method for Developing Signature Algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics, 2022. No. 1(98), pp. 56–65. DOI: https://doi.org/10.56415/basm.y2022.i1.p56.
17. Молдовян Д.Н., Молдовян А.А. Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2(48). С. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.

18. Молдовян А. А., Молдовян Н. А. Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. 2022. № 3(49). С. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.
19. Moldovyan D. N. A new type of digital signature algorithms with a hidden group // Computer Science Journal of Moldova. 2023, vol. .31, No. 1(91), pp. 111–124. doi:10.56415/csjm.v31.06.
20. Молдовян А. А., Молдовян Д. Н., Костина А. А. Алгебраические алгоритмы ЭЦП с полной рандомизацией подписи // Вопросы кибербезопасности. 2024. № 2(60). С. 93–100. DOI: 10.21681/2311-3456-2024-2-93-100.
21. Молдовян Д. Н., Костина А. А. Способ усиления рандомизации подписи в алгоритмах ЭЦП на некоммутативных алгебрах // Вопросы кибербезопасности. 2024. № 4(62). С. 71–81. DOI: 10.21681/2311-3456-2024-4-71-81.
22. Moldovyan A. A. Complete signature randomization in an algebraic cryptoscheme with a hidden group // Quasigroups and related systems. 2024. Vol. 32. No. 1, pp. 95–108. https://doi.org/10.56415/qrs.v32.08.
23. Молдовян Н. А, Петренко А. С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2024. № 6(64). С. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
24. Duong M. T., Moldovyan A. A., Moldovyan D. N., Nguyen M. H., Do B. T. (2024). Decomposition of Quaternion-Like Algebras into a Set of Commutative Subalgebras. In: Dang, T. K., Küng, J., Chung, T. M. (eds) Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications. FDSE 2024. Communications in Computer and Information Science, vol 2310, p. 119–131. Springer, Singapore. https://doi.org/10.1007/978-981-96-0437-1_9.
25. Moldovyan D. N. A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. Vol. 27. No. 2, pp. 293–308.
26. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions, Quasigroups and Related Systems. 2018. vol. 26, no. 2. P. 263–270.
27. Duong M. T., Moldovyan D. N., Do B. V., Nguyen M. H. Post-quantum signature algorithms on noncommutative algebras, using difficulty of solving systems of quadratic equations // Computer Standards and Interfaces. 2023. Vol. 86. P. 103740. DOI: 10.1016/j.csi.2023.103740.
28. Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix algebra // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т. 17. Вып. 3. С. 254–261. DOI 10.21638/11701/spbu10.2021.303.
29. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022, vol. 30, no. 1, pp. 133–140. https://doi.org/10.56415/qrs.v30.11.

ALGEBRAIC SIGNATURE ALGORITHMS WITH TWO HIDDEN GROUPS

Moldovyan N. A.[3], Petrenko A. S.[4]

Keywords: *finite non-commutative algebra; associative algebra; computationally difficult problem; hidden group; digital signature; signature randomization; post-quantum cryptography.*

Purpose of work *is improving the performance of post-quantum algebraic signature algorithms based on the computational difficulty of solving large systems of power equations.*

Research methods: *the use of two hidden commutative groups, the elements of one of which are non-commutative with the other, to ensure sufficient completeness of signature randomization in algebraic signature schemes, the security of which is based on the computational difficulty of solving large systems of power equations in the ground finite field* $GF(p)$*. Calculation of the fitting signature in the form of a vector* $\mathbf{S}$ *depending on mutually non-commutative non-scalar vectors selected from hidden groups and a random scalar vector. The use of finite non-commutative associative algebras (FNAA) with a well-studied structure as an algebraic carrier of signature algorithms with a verification equation with multiple occurrences of the vector* $\mathbf{S}$*. Defining the FNAAs by the sparse basic vector multiplication tables.*

Results of the study: *three types of post-quantum algebraic signature schemes are proposed, differing in techniques for ensuring high security to the forging signature attacks using vector* $\mathbf{S}$ *as a fitting parameter of the attacks. The first type uses the technique of exponentiating the product, which includes vector* $\mathbf{S}$*, to a large degree, the second type uses the exponentiation operation to a power equal to the value of the hash function calculated from* $\mathbf{S}$*, and the third type uses the combination of the first two techniques. Algorithmic implementations of signature schemes of each type are carried out*

3 Nikolay A. Moldovyan, Doctor of technical sciences, professor, Chief researcher of Scientific Center of Information Technologies and Artificial Intelligence of Sirius University of Science and Technology, Sirius Federal Territory, Russia. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 6603837461. E-mail: moldovan.NA@talantiuspeh.ru

4 Alexei S. Petrenko, PhD student of Saint Petersburg State Electrotechnical University «LETI», St. Petersburg, Russia, junior researcher of Scientific Center of Information Technologies and Artificial Intelligence of Sirius University of Science and Technology, Sirius Federal Territory, Russia. ORCID: https://orcid.org/0000-0002-9954-4643. Scopus Author ID: 57200260915. E-mail: a.petrenko1999@rambler.ru

and the correctness of the developed algorithms is shown. Security to direct attack, to attack based on known signatures, and to signature forgery was assessed. A comparison of the proposed signature algorithms with known analogues is presented. The multiplication by a scalar vector when calculating vector $\mathbf{S}$ *and setting the FNAAs by the sparse basis vector multiplication tables are used as techniques for improving the performance of algebraic signature algorithms.*

Practical relevance: *the significance of the results of the article consists in testing a method for enhancing signature randomization, including calculating the signature fitting element* $\mathbf{S}$ *depending on the product of two non-commutative vectors, while developing algebraic algorithms of three different types, which are of interest as a prototype of a practical post-quantum signature standard.*

The results were obtained *with the financial support of the project «Technologies for countering previously unknown quantum cyber threats», implemented within the framework of the state program of the «Sirius» Federal Territory «Scientific and technological development of the «Sirius» Federal Territory (Agreement No. 23-03 dated September 27, 2024).*

References

1. Post-Quantum Cryptography. 15th International Conference, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings. Lecture Notes in Computer Science. 2024. V. 14771–14772. Springer, Cham.
2. Alamelou Q., Blazy O., Cauchie S., Gaborit Ph. A code-based group signature scheme. Designs, Codes and Cryptography. 2017. V. 82. N. 1–2. P. 469–493.
3. Vedenev K.. Kosolapov Yu. Code-based cryptography // Lecture Notes in Computer Science. 2023. Vol. 14311. P. 35–55. DOI: 10.1007/978-3-031-46495-9_3.
4. D'Alconzo G. On two modifications of the McEliece PKE and the CFS signature scheme // International Journal of Foundations of Computer Science. 2024. Vol. 35. N. 5. P. 501–512. DOI: 10.1142/S0129054123500132.
5. Battarbee C., Kahrobaei D., Perret L., Shahandashti S.F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures // In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023 / Lecture Notes in Computer Science, 2023. V. 14154. P. 113–138. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_5.
6. Gärtner J. NTWE: A Natural Combination of NTRU and LWE // In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023 / Lecture Notes in Computer Science, 2023, vol 14154, pp. 321–353. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_12.
7. Li L., Lu X., Wang K. Hash-based signature revisited // Cybersecurity. 2022. V. 5. No. 13. https://doi.org/10.1186/s42400-022-00117-w.
8. Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing // In: Ding, J., Steinwandt, R. (eds) Post-Quantum Cryptography. PQCrypto 2019 / Lecture Notes in Computer Science. 2019. V. 11505. P. 329–349. Springer, Cham. https://doi.org/10.1007/978-3-030-25510-7_18.
9. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. Vol. 80. P. 7–23. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2.
10. Hashimoto Y. Recent Developments in Multivariate Public Key Cryptosystems // In: Takagi, T., Wakayama, M., Tanaka, K., Kunihiro, N., Kimoto, K., Ikematsu, Y. (eds) International Symposium on Mathematics, Quantum Theory, and Cryptography. Mathematics for Industry, 2021. Vol. 33. P. 209–229. Springer, Singapore. https://doi.org/10.1007/978-981-15-5191-8_16.
11. Moldovyan D.N. New Form of the Hidden Logarithm Problem and Its Algebraic Support // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. Vol. 93. No. 2. P. 3–10.
12. Moldovyan D.N. A practical digital signature scheme based on the hidden logarithm problem // Computer Science Journal of Moldova. 2021. Vol. 29. No. 2(86). P. 206–226.
13. Ding J., Petzoldt A., Schmidt D.S. Solving Polynomial Systems // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. 2020. V. 80. P. 185–248. https://doi.org/10.1007/978-1-0716-0987-3_8.
14. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. No. 3 (103). P. 80-89. DOI: https://doi.org/10.56415/basm.y2023.i3.p80.
15. Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. V.32. N.1(94). P. 46–60. DOI: 10.56415/csjm.v32.04.
16. Moldovyan A.A., Moldovyan D.N. A New Method for Developing Signature Algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics, 2022. No. 1(98), pp. 56–65. DOI: https://doi.org/10.56415/basm.y2022.i1.p56.
17. Moldovjan D.N., Moldovjan A.A. Algebraicheskie algoritmy JeCP, osnovannye na trudnosti reshenija sistem uravnenij // Voprosy kiberbezopasnosti. 2022. № 2(48). S. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
18. Moldovjan A.A., Moldovjan N.A. Algoritmy JeCP na konechnyh nekommutativnyh algebrah nad poljami harakteristiki dva // Voprosy kiberbezopasnosti. 2022. № 3(49). S. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.
19. Moldovyan D.N. A new type of digital signature algorithms with a hidden group // Computer Science Journal of Moldova. 2023, vol. .31, No. 1(91), pp. 111–124. doi:10.56415/csjm.v31.06.
20. Moldovjan A.A., Moldovjan D.N., Kostina A.A. Algebraicheskie algoritmy JeCP s polnoj randomizaciej podpisi // Voprosy kiberbezopasnosti. 2024. № 2(60). S. 93–100. DOI: 10.21681/2311-3456-2024-2-93-100.

21. Moldovjan D. N., Kostina A. A. Sposob usilenija randomizacii podpisi v algoritmah JeCP na nekommutativnyh algebrah // Voprosy kiberbezopasnosti. 2024. № 4(62). S. 71–81. DOI: 10.21681/2311-3456-2024-4-71-81.
22. Moldovyan A. A. Complete signature randomization in an algebraic cryptoscheme with a hidden group // Quasigroups and related systems. 2024. Vol. 32. No. 1, pp. 95–108. https://doi.org/10.56415/qrs.v32.08.
23. Moldovjan N. A, Petrenko A. S. Algebraicheskij algoritm JeCP s dvumja skrytymi gruppami // Voprosy kiberbezopasnosti. 2024. № 6(64). S. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
24. Duong M. T., Moldovyan A. A., Moldovyan D. N., Nguyen M. H., Do B. T. (2024). Decomposition of Quaternion-Like Algebras into a Set of Commutative Subalgebras. In: Dang, T. K., Küng, J., Chung, T. M. (eds) Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications. FDSE 2024. Communications in Computer and Information Science, vol 2310, p. 119–131. Springer, Singapore. https://doi.org/10.1007/978-981-96-0437-1_9.
25. Moldovyan D. N. A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. Vol. 27. No. 2, pp. 293–308.
26. Moldovyan N. A. Unified method for defining finite associative algebras of arbitrary even dimensions, Quasigroups and Related Systems. 2018. vol. 26, no. 2. P. 263–270.
27. Duong M. T., Moldovyan D. N., Do B. V., Nguyen M. H. Post-quantum signature algorithms on noncommutative algebras, using difficulty of solving systems of quadratic equations // Computer Standards and Interfaces. 2023. Vol. 86. P. 103740. DOI: 10.1016/j.csi.2023.103740.
28. Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix algebra // Vestnik Sankt-Peterburgskogo universiteta. Prikladnaja matematika. Informatika. Processy upravlenija. 2021. T. 17. Vyp. 3. S. 254–261. DOI:10.21638/11701/spbu10.2021.303.
29. Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022, vol. 30, no. 1, pp. 133–140. https://doi.org/10.56415/qrs.v30.11.

МЕТОДЫ ЗАЩИТЫ ОТ АТАК ПО ПОБОЧНЫМ КАНАЛАМ АППАРАТНОЙ РЕАЛИЗАЦИИ СХЕМ ПОСТКВАНТОВОЙ ПОДПИСИ, ПОСТРОЕННЫХ НА ОСНОВЕ ПРОТОКОЛА ИДЕНТИФИКАЦИИ ШТЕРНА

Смирнов Д. К.[1], Чижов И. В.[2]

DOI: 10.21681/2311-3456-2025-3-21-28

Цель исследования: *разработка протокола идентификации Штерна, устойчивого к атакам по побочным каналам.*

Метод(ы) исследования: *изучение современных методов атак на криптографические схемы со схожими вычислительными элементами, способов защиты от этих атак, модификация схемы с целью защиты приватного ключа при краже токена.*

Результат(ы) исследования: *выделены уязвимые вычислительные элементы протокола – сложение векторов по модулю 2 и умножение матрицы на вектор – и проанализированы основные методы защиты этих элементов от утечек по побочным каналам, такие как маскирование, балансирование и перемешивание. Предложен способ матричного умножения, устойчивый к горизонтальной корреляционной атаке, применявшейся против криптосистемы Мак-Элиса. Установлены основные требования к реализации схемы на ПЛИС, предложена модификация схемы с маскированием ключа, не нарушающая стойкость оригинальной, позволяющая защитить секрет при краже токена и предотвращающая атаки имперсонализации благодаря маскированию. Способ генерации маски выбран таким образом, чтобы минимизировать место, занимаемое на ПЛИС, а именно хэширование парольной фразы функцией «Стрибог-К» со счётчиком. Показано, что стойкость модифицированного протокола идентификации Штерна совпадает со стойкостью оригинального протокола в модели без утечек по побочным каналам и превосходит в модели с ними.*

Научная новизна: *результаты работы позволяют реализовать постквантовый алгоритм подписи «Шиповник», разрабатываемый рабочей группой ТК26 и проходящий стандартизацию в настоящее время.*

Ключевые слова: *синдромное декодирование, схема подписи «Шиповник», корреляционная атака, атака по электромагнитному излучению, атака по энергопотреблению, атака с внесением ошибок.*

Введение

В ответ на возрастающую угрозу построения квантового компьютера множество исследователей посвящают себя изучению и развитию постквантовой криптографии. В частности, силами рабочей группы ТК26 разрабатывается постквантовый алгоритм подписи «Шиповник», основанный на протоколе идентификации Штерна.

Известно, что идеальная математическая абстракция существует лишь в теоретическом мире. При реализации криптографических алгоритмов легко допустить ошибку, способную уничтожить всю теоретическую стойкость. Классические ЭВМ работают благодаря электричеству, которое, проходя по проводнику, способно менять окружающее электромагнитное поле. Изменение данных на регистрах устройства требует более высокого энергопотребления. Всё это может нести информацию о секретных данных, нарушая секретность по Шеннону. Именно этим и пользуются злоумышленники, проводя атаки по побочным каналам.

Эти атаки можно провести без использования квантового компьютера на классическом вычислителе. Поэтому данная работа ставит конечной целью разработку протокола идентификации Штерна как основной части алгоритма подписи «Шиповник» на ПЛИС таким образом, чтобы она была устойчивой к атакам по побочным каналам.

Вопрос реализации протокола Штерна, устойчивой к атакам по побочным каналам, уже изучался в работе [22]. Однако подход, предложенный в ней, требует дважды вычислять матричное умножение, причём алгоритм этого умножения подвержен утечкам, генерировать маску для каждого раунда протокола и предполагает хранение приватного ключа на устройстве без маски. В этой статье предлагается устойчивый к данному типу атак вариант матричного умножения, который требуется вычислить только один раз, а модифицированная версия протокола позволяет хранить и проводить вычисления над приватным ключом в маскированном виде.

1 Смирнов Дмитрий Константинович, магистр, МГУ имени М. В. Ломоносова, АО «ИнфоТеКС», г. Москва, Россия. E-mail: s02190708@stud.cs.msu.ru

2 Чижов Иван Владимирович, кандидат физико-математических наук, доцент, МГУ имени М. В. Ломоносова, Федеральный исследовательский центр «Информатика и управление» РАН, АО «НПК «Криптонит», г. Москва, Россия. E-mail: ichizhov@cs.msu.ru

Описание протокола идентификации Штерна

Протокол идентификации Штерна – интерактивный протокол с нулевым разглашением, предложенный Ж. Штерном в 1993 году [1]. Его стойкость основана на сложности задачи синдромного декодирования. Пусть выбрана некоторая хэш-функция $h(\cdot) : \{0,1\}^* \longrightarrow \{0,1\}^l$. Выбран также код, исправляющий ошибки, длины n, размерности k, с кодовым расстоянием ω. Матрица $H \in \{0,1\}^{(n-k)\times n}$ – его проверочная матрица, $s = \{0,1\}^n$ – приватный ключ подписывающего абонента P, $y = Hs^T$ – его публичный ключ. Слово $A\|B$ – конкатенация слов A и B. Абонент P (Prover) выбирает случайное n-битное слово u и случайную перестановку σ на множестве целых чисел $\{1..n\}$, вычисляет:

$$c_0 = h(\sigma\|Hu^T)$$
$$c_1 = h(\sigma(u))$$
$$c_2 = h(\sigma(u \oplus s))$$

и отправляет c_0, c_1, c_2 проверяющему абоненту V (Verifier).

Абонент V выбирает случайное число $b \in \{0,1,2\}$ и посылает абоненту P. На основании b абонент P раскрывает некоторую пару значений абоненту V:

если $b = 0$, то $r_0 = \sigma$, $r_1 = u$;
если $b = 1$, то $r_0 = \sigma$, $r_1 = u \oplus s$;
если $b = 2$, то $r_0 = \sigma(u)$, $r_1 = \sigma(s)$.

Последним шагом V проверяет равенства:

если $b = 0$, то $c_0 = h(r_0\|Hr_1^T)$, $c_1 = h(r_0(r_1))$;
если b = 1, то $c_0 = h(\sigma\|Hr_1^T \oplus y)$, $c_2 = h(r_0(r_1))$;
если b = 2, то $c_1 = h(r_0)$, $c_2 = h(r_0 \oplus r_1)$, $wt(r_1) = \omega$.

Если они оказываются верными, абонент P считается идентифицированным.

Противник без знания секретного ключа может успешно пройти проверку с вероятностью 2/3, поэтому необходимо повторять протокол k раз. Это влечёт за собой нагрузку на сеть из-за большого количества пересылок между абонентами. Решением этой проблемы может быть применение преобразования Фиата-Шамира [2, 3].

Модели утечек

Как правило, рассматриваются 2 модели утечек:

1) Модель расстояния Хэмминга. Она основана на предположении, что потребляемая мощность зависит от расстояния Хэмминга $\rho_H(x_{old}, x_{new})$ между старым x_{old} и новым x_{new} значением на шине.
2) Модель веса Хэмминга. Является частным случаем предыдущей модели с допущением, что старое значение было нулевым:

$$\rho(0, x_{new}) = wt(0 \oplus x_{new}) = wt(x_{new}), \quad (1)$$

где $wt(\cdot)$ – вес Хэмминга.

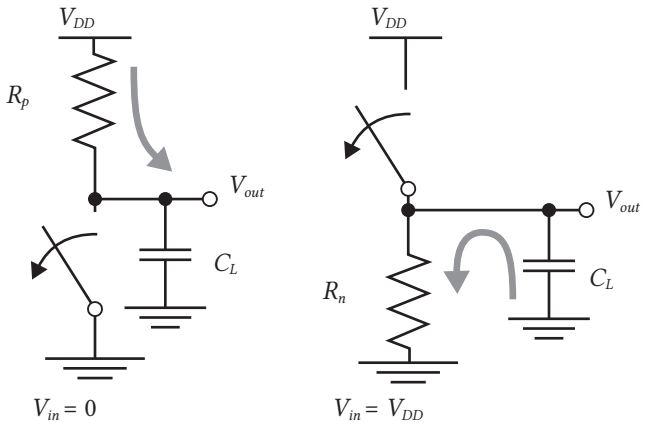


Рис. 1. КМОП-инвертор [5]

Атаки по энергопотреблению

Большинство ПЛИС используют память, реализуемую на КМОП (см. рис. 1). Особенность такой памяти заключается в том, что на статичное хранение информации энергии требуется значительно меньше, чем на её изменение. Это объясняется тем, что когда состояние схемы не меняется, между источником питания и землёй закрыт хотя бы один транзистор. Таким образом, КМОП вентиль имеет мощность рассеивания порядка 0,01 мВ в статичном состоянии, 1 мВ и 5 мВ при изменении состояния на частотах 1 МГц и 10 МГц соответственно [4].

Именно эта особенность и даёт возможность отследить изменения данных на шине. За один такт перехода из разряженного в заряженное состояние и обратно «идеальной» КМОП схемой потребляется энергия:

$$E_s = C_L V_{DD}^2, \quad (2)$$

где C_L – ёмкость нагрузки транзистора, V_{DD} – напряжение источника питания. На практике энергия зарядки и разрядки может различаться, так как эти процессы происходят в разных элементах схемы – n-МОП и p-МОП транзисторах. Они могут обладать разными ёмкостями и сопротивлением [5].

Рассмотрим метод корреляционной атаки, использующей замеры энергопотребления, описанный в [6]. В качестве функции шифрования используют сложение по модулю 2. Атакующий строит предположение о наборе вероятных значений секрета на некотором этапе криптографического алгоритма. Выбрав за модель утечек модель расстояния Хэмминга, вычисляет

$$H_{i,R} = wt(M_i \oplus R), \quad (3)$$

где R – неизвестное предыдущее состояние регистра, а M_i – некоторые известные данные. Далее вычисляет коэффициенты корреляции между набором измерений W_i и набором предположений $H_{i,R}$:

$$\rho_{WH}(R) = \frac{N\sum W_i H_{i,R} - \sum W_i \sum H_{i,R}}{\sqrt{N\sum W_i^2 - (\sum W_i)^2}\,\sqrt{N\sum H_{i,R}^2 - (\sum H_{i,R})^2}}, \quad (4)$$

где N – размер каждого из наборов, а суммирование проводится от 1 до N. Перебирая R и вычисляя значение $\rho_{WH}(R)$ для каждого из них, атакующий находит такое R, которое даёт максимальный коэффициент корреляции.

Как утверждает П. Кохер и др. в [7], для защиты от анализа энергопотребления стоит реализовывать алгоритм таким образом, чтобы в программе не было ветвлений, балансировать вес Хэмминга переменных значений (на регистрах или шине) и физически экранировать устройство. Хотя все эти меры и не смогут полностью исключить возможность успешной атаки.

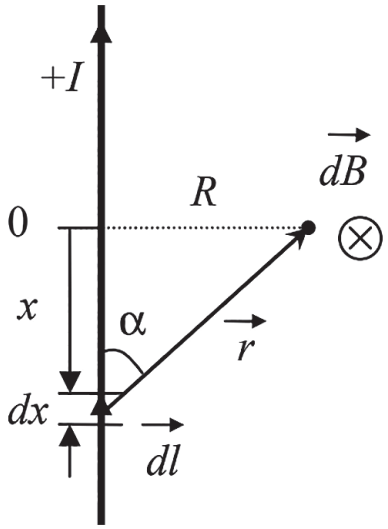


Рис. 2. Иллюстрация закона Био-Савара-Лапласа

Атаки по электромагнитному излучению

Хорошо известен закон Био-Савара-Лапласа (см. рис. 2), определяющий вектор индукции магнитного поля, порождаемого постоянным электрическим током:

$$d\vec{B} = \frac{\mu_0}{4\pi}\frac{I[d\vec{l} \times \vec{r}]}{r^3}, \quad (5)$$

где μ_0 – магнитная постоянная, I – ток в проводнике, $d\vec{l}$ – элемент проводника, $\vec{r}$ – радиус-вектор от элемента проводника до точки, в которой измеряется индукция магнитного поля. Направление $d\vec{B}$ перпендикулярно плоскости, в которой лежат $d\vec{l}$ и $\vec{r}$, и определяется правилом правого винта.

При зарядке и разрядке КМОП инвертора происходит движение электронов. Причём, в первом случае оно имеет одно направление, а в другом – противоположное (см. рис. 1). Тот факт, что направление вектора магнитной индукции будет зависеть от направления тока, даёт возможность определить характер изменения состояния схемы: с 0 на 1 или с 1 на 0.

Э. Питерс и др. исследовали возможность такой атаки [8]. Хотя такой способ позволяет не подключаться к сети напрямую, он более сложный в исполнении. Авторы использовали маленькую пружинку, которую нужно было разместить точно над шиной. Для этого может потребоваться микроскопическое исследование схемы ПЛИС.

Атаки с внесением ошибок

Эти атаки изучались во множестве работ [9–12]. Самые простые варианты атак заключаются в изменении напряжения питания, добиваясь сбоев в синхронизирующем сигнале CLK, более сложные требуют использования лазера, успешность которых опирается на эффект ионизации элементов КМОП. С этой проблемой сталкиваются, например, спутники, попадающие под ионизирующее излучение Солнца. По этой причине в спутниках используются коды Рида-Соломона [13].

Контролируемое внесение лазером ошибок в криптографические алгоритмы позволяют использовать дифференциальный анализ [14].

Корреляционная атака на криптосистему Мак-Элиса

В 2023 году была опубликована атака на криптосистему Мак-Элиса, использующая данные энергопотребления во время вычисления синдрома секретного вектора ошибки $H_{pub}e = s$ [15]. Выше была описана общая схема атаки, которой придерживались и авторы указанной статьи. Они искали корреляцию измерений со столбцами матрицы H_{pub}: если в e на позиции i стоит единица, на результирующую сумму повлияет i-тый столбец H_{pub}, а значит изменится и состояние регистра с промежуточным результатом. После сортировки массива коэффициентов корреляции по убыванию отбираются первые t элементов, соответствующих некоторым наиболее вероятным столбцам. Поскольку при реальном проведении атаки во время замеров неизбежно будут шумы, может произойти ошибка, и на самом деле вместо единицы на какой-то позиции будет стоять 0. А из условия $wt(e) = t$ следует, что «пропавшая» единица должна соответствовать элементу из оставшихся $n - t$.

В связи с этим авторы использовали подход, являющийся развитием предложенного Ю. Пранджем [16], который позволяет смягчить требование к столбцам матрицы H_{pub}: t столбцов, соответствующих единицам в e, не обязаны быть первыми t столбцами, а могут находиться среди первых $n - k$ столбцов.

Балансирование

Согласно работе [7], балансирование веса Хэмминга на регистрах может быть эффективным способом защиты. Однако в статье [17] приводится аргумент против такого метода: вычисление балансирующего значения будет немного сдвинуто по времени, и злоумышленник сможет манипулировать внешними условиями (такими, как напряжение питания), чтобы увеличить этот отрезок времени.

Перемешивание

Другим популярным способом защиты является перемешивание независящих друг от друга операций, например, чтение S-box'ов DES в случайном порядке. То есть, если один из них будет прочитан первым с вероятностью 1/8, то усреднив 64 запуска атаки можно получить исходный сигнал и обойти защиту [17].

Маскирование

Суть этого метода заключается в том, что на регистрах хранят данные не в открытом виде, а в преобразованном:

$$x = x_1 \circ x_2 \circ \ldots \circ x_d, \quad (6)$$

где x – преобразованный секрет, $\circ$ – некоторая групповая операция, а набор x_i называется набором долей. Как правило, в качестве групповой операции подразумевается сложение по модулю 2, за x_1 берут секрет, а за остальные доли – маски. При анализе атак по побочным каналам на криптосистему NTRU, другого кандидата на постквантовый криптографический стандарт, маскирование секретного ключа оказалось наиболее эффективным способом защиты среди различных перемешиваний и маскирования шифртекста [18]. Более того, стойкость этого метода можно доказать [19].

Теневой регистр

Автор во время исследования существующего опыта обнаружил лишь попытки маскировать регистр, на котором содержится секретный вектор e, во время вычисления $H_{pub}e = s$, но не нашёл предложений складывать не только столбцы, соответствующие единицам, но и нулям: тогда атаки по энергопотреблению с корреляционным анализом, например, из [15], окажутся неэффективными. Рассмотрим кратко идею.

Будем читать секретный вектор e по битам. Если очередной бит e_i равен нулю, то i-тая строка H_{pub} складывается с регистром reg_0, иначе – с reg_1. Оба регистра инициализированы нулём. В итоге мы используем все строки матрицы независимо от секретного вектора. В качестве результата такого умножения вектора на матрицу выдаём reg_1.

Замеры энергопотребления не будут зависеть от секрета. Но если у злоумышленника удастся разместить пробирующую пружинку, как это сделали в [8], точно над регистром reg_1, то он заметит области, в которых электромагнитное поле почти не изменяется, – это будут строки, соответствующие нулям. Поэтому, хотя это и довольно сильное предположение, одного метода защиты недостаточно.

Маскирование ключа

Секретный ключ будет храниться в маскированном виде и все вычисления над ним будут проводиться с той же маской. Маска вырабатывается из пароля, который известен пользователю. Для этого можно воспользоваться хэш-функцией «Стрибог-K». Уже доказано, что «Стрибог» неразличим от случайного оракула в модели идеального блочного шифра, то есть, является псевдослучайной функцией [20]. А из псевдослучайной функции можно построить псевдослучайный генератор [21].

Что может позволить такая конструкция? Дело в том, что большинство рассмотренных атак требуют физического доступа к устройству. Предполагая, что противник обладает возможностями по внесению ошибок, замерам напряжения или электромагнитного излучения, или, даже в более сильных предположениях, прочитать хранящиеся значения в памяти ПЛИС, секретный ключ может быть раскрыт противником. Более того, существует угроза подписи им сообщений даже при неизвестном ключе, для чего ему не требуется проведения никаких атак. Однако если ключ дополнительно будет маскирован с помощью пароля, это сильно затруднит реализацию угроз.

Сейчас нам требуется изменить вычислительный алгоритм таким образом, чтобы алгоритм самого протокола не изменился, но стал учитывать вышеописанные рассуждения. Пусть мы получаем пароль $Pass \in \{0,1\}^t$, $t < 512$ и генерируем из него маску $M = F(Pass) \in \{0,1\}^n$. Абонент P обладает маскированным ключом $s' = s \oplus M$. Теперь ему требуется вычислить

$$u' = u \oplus M;$$
$$c_0 = h(\sigma \| Hu'^T),$$
$$c_1 = h(\sigma(u')),$$
$$c_2 = h(\sigma(u \oplus s')) = h(\sigma(u' \oplus s)).$$

На основании выбора абонента V вернуть:

если $b = 0$, то $r_0 = \sigma$, $r_1 = u'$;
если $b = 1$, то $r_0 = \sigma$, $r_1 = u \oplus s' = u' \oplus s$;
если $b = 2$, то $r_0 = \sigma(u')$, $r_1 = \sigma(s') \oplus \sigma(M) = \sigma(s)$.

Для получения открытого ключа вычисляется $y = Hs'^T \oplus HM^T = Hs^T$. Теперь можно заметить, что над секретным ключом не проводятся вычисления без маски.

Генерация маски

Ключ, по имеющимся на данный момент оценкам [3], имеет длину 2896 бит, что превышает длину хэш-функции «Стрибог-512» более, чем в 5 раз. Поэтому вычисления одного хэша будет недостаточно. Если каждый последующий блок будет зависеть лишь от предыдущего, злоумышленник сможет воспользоваться особенностью ключа, а именно его малым весом. Если предположить, что в первом 512-битном блоке не содержится ни одной единицы, то первые 512 бит s' представляют собой сам хэш. Если противник сможет извлечь весь вектор s', то ему будет

достаточно продолжить хэширование со второго блока, используя первый, и тогда он сможет восстановить секретный ключ. Поэтому каждый блок должен зависеть от пароля и не быть одинаковым. Например, можно использовать «Стрибог-K» с сообщением-счётчиком, равным номеру блока.

В части «Матричное умножение» была освещена атака с восстановлением ключа. Однако она требует физического доступа к устройству и вычислений с известным ключом (который в данном случае является паролем $Pass$). Но при известном пароле злоумышленнику не нужна эта атака, поскольку он сможет самостоятельно сгенерировать маску M.

Стратегии противника

Рассмотрим возможные стратегии злоумышленника для обмана абонента V.

Стратегия 0: нечестный доказывающий предполагает, что $b \neq 0$. Он выбирает $t = \{0,1\}n$, $wt(t) = \omega$.

$$c_0 = h(\sigma \| H(u \oplus t)^T \oplus y);$$
$$c_1 = h(\sigma(u));$$
$$c_2 = h(\sigma(u \oplus t)).$$

Далее в зависимости от выбора b:

если $b = 1$, то $r_0 = \sigma$, $r_1 = u \oplus t$;
если $b = 2$, то $r_0 = \sigma(u)$, $r_1 = \sigma(t)$.

Если предположение верно, проверяющий будет обманут:

если $b = 1$, то $c_0 = h(\sigma \| Hr_1^T \oplus y)$, $c_2 = h(r_0(r_1))$;
если $b = 2$, то $c_1 = h(r_0)$, $c_2 = h(r_0 \oplus r_1)$, $wt(r_1) = \omega$.

Стратегия 1: нечестный доказывающий предполагает, что $b \neq 1$. Он выбирает $t = \{0,1\}^n$, $wt(t) = \omega$.

$$c_0 = h(\sigma \| Hu^T);$$
$$c_1 = h(\sigma(u));$$
$$c_2 = h(\sigma(u \oplus t)).$$

Далее в зависимости от выбора b:

если $b = 0$, то $r_0 = \sigma$, $r_1 = u$;
если b = 2, то $r_0 = \sigma(u)$, $r_1 = \sigma(t)$.

Если предположение верно, проверяющий будет обманут:

если $b = 0$, то $c_0 = h(\sigma \| Hr_1^T)$, $c_1 = h(r_0(r_1))$;
если $b = 2$, то $c_1 = h(r_0)$, $c_2 = h(r_0 \oplus r_1)$, $wt(r_1) = \omega$.

Стратегия 2: нечестный доказывающий предполагает, что $b \neq 2$. Он выбирает $t = \{0,1\}^n$: $Ht^T = y$. Заметим, что в этом случае противник надеется, что проверки на вес не будет, поэтому достаточно найти любое подходящее решение, что можно сделать, например, методом Гаусса.

$$c_0 = h(\sigma \| Hr^T);$$
$$c_1 = h(\sigma(u));$$
$$c_2 = h(\sigma(u \oplus t)).$$

Далее в зависимости от выбора b:

если $b = 0$, то $r_0 = \sigma$, $r_1 = u$;
если $b = 1$, то $r_0 = \sigma$, $r_1 = u \oplus t$.

Если предположение верно, проверяющий будет обманут:

если $b = 0$, то $c_0 = h(\sigma \| Hr_1^T)$, $c_1 = h(r_0(r_1))$;
если $b = 1$, то $c_0 = h(\sigma \| Hr_1^T \oplus y)$, $c_2 = h(r_0(r_1))$.

Стойкость модифицированной схемы

Будем называть $SC_1{:}T_1 \longrightarrow s$ и $SC_2{:}(T_1,T_2) \longrightarrow (s',M)$ такие машины Тьюринга, которые получают на вход наборы различных измерений напряжения и электромагнитного излучения, полученных в ходе работы устройства честного доказывающего абонента P, и возвращающие предполагаемый приватный ключ и маску. T_1 содержит информацию о приватном ключе, T_2 – о маске.

Первая машина соответствует оригинальному алгоритму Штерна, вторая – модифицированному. Пусть T_{SC_1}, T_{SC_2} – их время работы в тактах. Так как второй машине требуется вычислить помимо ключа ещё и маску, не умаляя общности, можно считать, что SC_1 содержится в SC_2 и

$$T_{SC_1} < T_{SC_2}. \quad (7)$$

Назовём $A = (A_1,A_2)$ машину Тьюринга, успешно обманывающую честного проверяющего абонента V в оригинальной схеме идентификации Штерна за T_A тактов. Машина состоит из двух частей, каждая из которых соо тветствует одному из шагов схемы.

$A(u,\sigma,y,b,\hat{b},s)$:
$(c_0,c_1,c_2,r_0',r_1',r_0'',r_1'') \longleftarrow A_1\,(u,\sigma,y,\hat{b},s)$,
$(r_0,r_1) \longleftarrow A_2\,(b,\hat{b},r_0',r_1',r_0'',r_1'')$.

Вернуть (c_0,c_1,c_2,r_0,r_1).

Здесь и далее используются величины: $\hat{b}$ – выбор стратегии противника; r_0', r_1', r_0'', r_1'' – наборы ответов противника, соответствующие выбранной им стратегии.

Назовём $B = (B_1,B_2)$ машину Тьюринга, успешно обманывающую честного проверяющего абонента V в модифицированной схеме идентификации Штерна за T_B тактов. Машина состоит из двух частей, каждая из которых соответствует одному из шагов схемы.

$B(u,\sigma,y,b,\hat{b},s',M)$:
$(c_0,c_1,c_2,r_0',r_1',r_0'',r_1'') \longleftarrow B_1\,(u,\sigma,y,\hat{b},s',M)$,
$(r_0,r_1) \longleftarrow B_2\,(b,\hat{b},r_0',r_1',r_0'',r_1'')$.
Вернуть (c_0,c_1,c_2,r_0,r_1).

Определим теперь машины Тьюринга $\hat{A}$ и $\hat{B}$, использующие, помимо описанных стратегий, утечки по побочным каналам:

$\hat{A}(u,\sigma,y,b,\hat{b},T_1)$:
$s \leftarrow SC_1(T_1)$,
$(c_0,c_1,c_2,r_0,r_1) \leftarrow A(u,\sigma,y,b,\hat{b},s)$.

Вернуть (c_0,c_1,c_2,r_0,r_1).

$\hat{B}(u,\sigma,y,b,\hat{b},T_1,T_2)$:
$(s',M) \leftarrow SC_2(T_1,T_2)$,
$(c_0,c_1,c_2,r_0,r_1) \leftarrow B(u,\sigma,y,b,\hat{b},s',M)$.

Вернуть (c_0,c_1,c_2,r_0,r_1).

Обозначим за $T_{\hat{A}}$ и $T_{\hat{B}}$ время их работы в тактах.

Машины принимают на вход секретный ключ и маску, которые можно заменить случайными векторами при отсутствии физической возможности у противника выполнить атаку по побочным каналам, не нарушая общности.

Теорема 1: Время работы машин A и B совпадает.

Доказательство.

$A(u,\sigma,y,b,\hat{b},s) = B(u,\sigma,y,b,\hat{b},s,0)$,
$B(u,\sigma,y,b,\hat{b},s',M) = A(u \oplus M,\sigma,y,b,\hat{b},s' \oplus M)$.

Поскольку каждую из машин Тьюринга можно определить через другую, и считая дополнительные расходы в виде двух побитовых сложений пренебрежимо малыми, получаем

$$T_A = T_B.$$

Теорема 2: Время работы машины $\hat{A}$ меньше времени работы $\hat{B}$.

Доказательство. В силу определений заметим, что:

$$T_{\hat{A}} = T_{SC_1} + T_A,$$
$$T_{\hat{B}} = T_{SC_2} + T_B.$$

Используя теорему 1 и (7) получим

$$T_{\hat{A}} < T_{\hat{B}}.$$

Таким образом, без нарушения стойкости в модели без использования утечек по побочным каналам модификация схемы становится более устойчивой в модели с использованием утечек.

Заключение

Атаки по побочным каналам – серьёзная угроза безопасности не только классических криптографических схем, основанных на задачах теории чисел, но и постквантовых. Помимо аппаратной защиты устройств, стоит предусматривать и логическую, разрабатывая алгоритмы таким образом, чтобы потребляемое напряжение и излучаемые электромагнитные волны были максимально декоррелированы с секретными данными, над которыми проводятся вычисления.

Авторами был предложен вариант матричного умножения, повышающий стойкость схемы к этим атакам, и модификация схемы, позволяющая хранить и использовать приватный ключ в маскированном виде. Благодаря этому можно реализовывать схемы, основанные на протоколе идентификации Штерна, требующие от противника использовать более сложные и дорогостоящие методы атак.

Литература

1. Stern J. A new identification scheme based on syndrome decoding // Advances in Cryptology – CRYPTO' 93 / под ред. D. R. Stinson. – Berlin, Heidelberg : Springer Berlin Heidelberg, 1994. – С. 13–21.
2. Fiat A., Shamir A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems // Advances in Cryptology – CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings. Т. 263. – Springer, 1986. – С. 186–194. – (Lecture Notes in Computer Science). – DOI: 10.1007/3-540-47721-7_12.
3. Vysotskaya, V. V. The security of the code-based signature scheme based on the Stern identification protocol / V. V. Vysotskaya, I. V. Chizhov // Applied Discrete Mathematics. – 2022. – No. 57. – P. 67–90. – DOI 10.17223/20710410/57/5.
4. Mano M. M., Ciletti M. D. Digital Design (4th Edition). – USA : Prentice-Hall, Inc., 2006. – С. 500–501.
5. Rabaey J. Digital Integrated Circuits: A Design Perspective. – Prentice Hall, 1996. – (Prentice Hall International editions).
6. Brier E., Clavier C., Olivier F. Correlation Power Analysis with a Leakage Model // Т. 3156. – 08.2004. – С. 16–29. – DOI: 10.1007/978-3-540-28632-5_2.
7. Kocher P. C., Jaffe J., Jun B. Differential Power Analysis // Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15–19, 1999, Proceedings. Т. 1666. – Springer, 1999. – С. 388–397. – (Lecture Notes in Computer Science). – DOI: 10.1007/3-540-48405-1_25.
8. Peeters E., Standaert F.-X., Quisquater J.-J. Power and electromagnetic analysis: Improved model, consequences and comparisons // Integration. – 2007. – Янв. – Т. 40. – С. 52–60. – DOI: 10.1016/j.vlsi.2005.12.013.
9. Laser attack benchmark suite / B. Amornpaisannon [и др.] // In: 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD). – 2020. – С. 1–9. – DOI: 10.1145/3400302.3415646.
10. Korkikian R., Pelissier S., Naccache D. Blind Fault Attack against SPN Ciphers // Proceedings - 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2014. – 2014. – Дек. – С. 94—103. – DOI: 10.1109/FDTC.2014.19.
11. J. Breier and X. Hou Breier J., Hou X. How Practical Are Fault Injection Attacks, Really? // IEEE Access. – 2022. – Т. 10. – С. 113122–113130. – DOI: 10.1109/ACCESS.2022.3217212.
12. Lomné V., Roche T., Thillard A. On the Need of Randomness in Fault Attack Countermeasures - Application to AES //. – 09.2012. – С. 85–94. – DOI: 10.1109/FDTC.2012.19.
13. Reed-Solomon Codes for Satellite Communications / Y. Liu [и др.] // 2009 IITA International Conference on Control, Automation and Systems Engineering (case 2009). – 2009. – С. 246–249. – DOI: 10.1109/CASE.2009.30.
14. AlTawy R., Youssef A. M. Differential Fault Analysis of Streebog // Information Security Practice and Experience / под ред. J. Lopez, Y. Wu. – Cham : Springer International Publishing, 2015. – С. 35–49.

15. Horizontal Correlation Attack on Classic McEliece / B. Colombier [и др.]. – 2023. – Cryptology ePrint Archive, Paper 2023/546.
16. Prange E. The use of information sets in decoding cyclic codes // IRE Trans. Inf. Theory. – 1962. – Т. 8. – С. 5–9. – URL: https://api.semanticscholar.org/ CorpusID:3351723.
17. Towards Sound Approaches to Counteract Power-Analysis Attacks / S. Chari [и др.] // Annual International Cryptology Conference. – 1999. – URL: https://api.semanticscholar.org/CorpusID:16695847.
18. Rabas T., Buček J., Lorencz R. Single-Trace Side-Channel Attacks on NTRU Implementation // SN Computer Science. – 2024. – Т. 5. – DOI: 10.1007/s42979-023-02493-7.
19. Prouff E., Rivain M. Masking against Side-Channel Attacks: A Formal Security Proof // Advances in Cryptology – EUROCRYPT 2013 / под ред. T. Johansson, P.Q. Nguyen. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2013. – С. 142–159.
20. L.R. Akhmetzyanova, A.A. Babueva, A.A.B. Streebog as a random oracle // ПДМ. – 2024. – № 64. – С. 27–42. – DOI: 10.17223/20710410/64/3.
21. Rosulek M. The Joy of Cryptography // – 2017. – URL: https://api.semanticscholar.org/CorpusID:199008788.
22. Cayrel P.-L., Gaborit P., Prouff E. Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices // Smart Card Research and Advanced Applications / под ред. G. Grimaud, F.-X. Standaert. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2008. – С. 191–205. – DOI: 10.1007/978-3-540-85893-5_14.

METHODS OF PROTECTION AGAINST SIDE-CHANNEL ATTACKS IN THE HARDWARE IMPLEMENTATION OF POST-QUANTUM SIGNATURE SCHEMES BASED ON THE STERN IDENTIFICATION PROTOCOL

Smirnov D.K.[3], Chizhov I.V.[4]

Keywords: *syndrome decoding, «Shipovnik» signature scheme, correlation attack, electromagnetic radiation attack, energy consumption attack, fault injection attack.*

Purpose of the study: *the development of a secure Stern identification protocol resistant to side-channel attacks.*

Methods of research: *the study of modern techniques for attacking cryptographic systems with similar computational components, methods to protect against these attacks, and modifications to the system in order to safeguard the private key in the event of a token theft.*

Result(s): *Vulnerable computational elements of the protocol, such as addition of vectors modulo 2 and matrix multiplication by a vector, are identified. The main methods of protecting these elements from leakage through side channels, including masking, balancing, and mixing, are analyzed. A matrix multiplication method resistant to horizontal correlation attacks used against the McEliece cryptosystem is proposed. The basic requirements for implementing the scheme on field-programmable gate arrays (FPGAs) are established. A modification of the scheme with key masking that does not compromise the strength of the original scheme is proposed to protect the secret in the event of token theft and prevent impersonation attacks due to key masking. The method of key mask generation is selected to minimize the amount of space occupied on an FPGA, specifically by hashing the passphrase using the «Stribog-K» function with a counter. It has been shown that the stability of the modified Stern identification protocol is the same as the stability of the original protocol in a model without side channel leakage, and it is even better in a model with side channel leakage.*

Scientific novelty: *the results of the work allow us to implement the post-quantum signature algorithm «Shipovnik», which is being developed by the TK26 working group and is currently being standardized.*

References

1. Stern, J. (1994). A New Identification Scheme Based on Syndrome Decoding. Advances in Cryptology – CRYPTO' 93, 773, 13–21. https://doi.org/10.1007/3-540-48329-2_2.
2. Fiat, A., & Shamir, A. (1986). How To Prove Yourself: Practical Solutions to Identification and Signature Problems. Advances in Cryptology — CRYPTO' 86, 263, 186–194. https://doi.org/10.1007/3-540-47721-7_12.
3. Vysotskaya, V., Chizhov, I. (2022). The security of the code-based signature scheme based on the Stern identification protocol. Prikladnaya diskretnaya matematika, (57), 67–90. https://doi.org/10.17223/20710410/57/5.
4. Mano M.M., Ciletti M.D. (2006). Digital Design (4th ed.). Prentice-Hall, Inc.
5. Rabaey, J.M., Chandrakasan, A.P., & Nikolić, B. (2003). Digital Integrated Circuits: A Design Perspective (2nd ed.). Pearson Education.
6. Brier, E., Clavier, C., Olivier, F. (2004). Correlation Power Analysis with a Leakage Model. Cryptographic Hardware and Embedded Systems – CHES 2004, 3156. https://doi.org/10.1007/978-3-540-28632-5_2.
7. Kocher, P., Jaffe, J., Jun, B. (1999). Differential Power Analysis. Advances in Cryptology – CRYPTO' 99, 1666. https://doi.org/10.1007/3-540-48405-1_25.

3 Dmitrii K. Smirnov, master, Lomonosov Moscow State University, Moscow, Russia. E-mail: s02190708@stud.cs.msu.ru
4 Ivan V. Chizhov, Ph.D., Lomonosov Moscow State University, Federal Research Center «Informatics and Control» of Russian Academy of Science, JSC «NPK Kryptonite», Moscow, Russia. E-mail: ichizhov@cs.msu.ru

8. Peeters E., Standaert F.-X., Quisquater J.-J. (2007). Power and electromagnetic analysis: Improved model, consequences and comparisons. Integration, 40, 52-60. https://doi.org/10.1016/j.vlsi.2005.12.013.
9. Amornpaisannon, B., Diavastos, A., Peh, L., & Carlson, T. E. (2020). Laser Attack Benchmark Suite. Proceedings of the 39th International Conference on Computer-Aided Design, 1–9. https://doi.org/10.1145/3400302.3415646.
10. Korkikian, R., Pelissier, S., & Naccache, D. (2014). Blind Fault Attack against SPN Ciphers. 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, 94–103. https://doi.org/10.1109/FDTC.2014.19.
11. Breier, J., & Hou, X. (2022). How Practical Are Fault Injection Attacks, Really? IEEE Access, 10, 113122–113130. https://doi.org/10.1109/ACCESS.2022.3217212.
12. Lomné, V., Roche, T., & Thillard, A. (2012). On the Need of Randomness in Fault Attack Countermeasures – Application to AES. 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, 85–94. https://doi.org/10.1109/FDTC.2012.19.
13. Liu, Y., Guan, Y., Zhang, J., Wang, G., & Zhang, Y. (2009). Reed-Solomon Codes for Satellite Communications. 2009 IITA International Conference on Control, Automation and Systems Engineering (Case 2009), 246–249. https://doi.org/10.1109/CASE.2009.30.
14. AlTawy, R., Youssef, A.M. (2015). Differential Fault Analysis of Streebog. Information Security Practice and Experience, 9065. https://doi.org/10.1007/978-3-319-17533-1_3.
15. Colombier, B., Grosso, V., Cayrel, P., & Drăgoi, V. (2023). Horizontal Correlation Attack on Classic McEliece. https://eprint.iacr.org/2023/546.
16. Prange, E. (1962). The Use of Information Sets in Decoding Cyclic Codes. IRE Transactions on Information Theory, 8(5), 5–9. https://doi.org/10.1109/TIT.1962.1057777.
17. Chari, S., Jutla, C.S., Rao, J.R., Rohatgi, P. (1999). Towards Sound Approaches to Counteract Power-Analysis Attacks. Advances in Cryptology – CRYPTO' 99, 1666. https://doi.org/10.1007/3-540-48405-1_26.
18. Rabas, T., Buček, J., & Lórencz, R. (2024). Single-Trace Side-Channel Attacks on NTRU Implementation. SN Computer Science, 5(2), 239. https://doi.org/10.1007/s42979-023-02493-7.
19. Prouff, E., Rivain, M. (2013). Masking against Side-Channel Attacks: A Formal Security Proof. Advances in Cryptology – EUROCRYPT 2013, 7881. https://doi.org/10.1007/978-3-642-38348-9_9.
20. Akhmetzyanova, L.R., Babueva, A.A., & Bozhko, A.A. (2024). Streebog as a Random Oracle. PDM, 64, 27–42. https://doi.org/10.17223/20710410/64/3.
21. Rosulek, M. (2017). The Joy of Cryptography.
22. Cayrel, P.L., Gaborit, P., Prouff, E. (2008). Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices. Smart Card Research and Advanced Applications, 5189. https://doi.org/10.1007/978-3-540-85893-5_14.

О ПРИМЕНИМОСТИ ПОСТКВАНТОВОГО СТАНДАРТА ЭЛЕКТРОННОЙ ПОДПИСИ SLH-DSA В СМАРТ-КАРТАХ

Панасенко С. П.[1]

DOI: 10.21681/2311-3456-2025-3-29-37

Цель работы: *проанализировать влияние стандартного протокола обмена со смарт-картами на применимость ресурсоемких постквантовых алгоритмов электронной подписи в устройствах с ограниченными ресурсами на примере смарт-карт и дать рекомендации по модернизации стандартного протокола по результатам анализа.*

Методы исследования: *теория информации, системный анализ, объектно-ориентированный анализ.*

Результаты исследования: *проанализированы различные сценарии взаимодействия со смарт-картой при использовании стандартного протокола обмена на примере выполнения смарт-картой функции вычисления электронной подписи стандартизованным в США постквантовым алгоритмом SLH-DSA; в результате анализа показаны ограничения стандартного протокола обмена, напрямую препятствующие применимости алгоритма SLH-DSA (и схожих с ним по характеристикам алгоритмов) в смарт-картах.*

Научная новизна: *по результатам проведенного анализа предложено направление модернизации стандартного протокола обмена со смарт-картами для его адаптации к характеристикам ресурсоемких постквантовых алгоритмов электронной подписи; предложенная модернизация протокола позволит использовать ряд постквантовых криптоалгоритмов в смарт-картах.*

Ключевые слова: *электронная подпись, постквантовая криптография, смарт-карта, протокол APDU, алгоритм SLH-DSA.*

Введение

Значительная часть традиционных асимметричных криптоалгоритмов базируется на сложности факторизации целых чисел или дискретного логарифмирования, в т. ч. в группе точек эллиптической кривой. Данные проблемы могут быть легко разрешимы с помощью алгоритмов для квантовых или гибридных вычислений, основанных на алгоритме Шора [1], при условии появления квантового компьютера, обладающего достаточными ресурсами. На текущий момент такие компьютеры по-прежнему являются гипотетическими, но технический прогресс в области их создания выглядит очевидным – уже сейчас с помощью существующих квантовых компьютеров (ресурсов которых пока, в общем случае, недостаточно для успешного криптоанализа реально используемых систем) решаются различные задачи с использованием эффекта квантового превосходства – см., например, [2].

В отчете [3] эксперты международной консалтинговой компании McKinsey предполагают, что к 2030 г. появятся квантовые компьютеры достаточной мощности для успешного криптоанализа реально применяемых классических асимметричных криптоалгоритмов, что делает крайне актуальной задачу перехода с текущих асимметричных криптографических алгоритмов на постквантовые алгоритмы, стойкие к криптоанализу с использованием квантовых вычислений. Усугубляющим данную проблему фактором также является распространенность в настоящее время метода HNDL (Harvest Now, Decrypt Later – «Собери сейчас, расшифруй позже»), состоящего в сборе и хранении злоумышленниками зашифрованных современными криптоалгоритмами данных (предположительно, имеющих ценность) в надежде на относительно скорое появление квантовых компьютеров и возможность расшифрования собранных данных с их помощью.

Одним из ответов на потенциальную угрозу асимметричной криптографии со стороны квантовых компьютеров явился конкурс Национального института стандартов и технологий США (NIST – National Institute of Standards and Technology) по выбору алгоритмов электронной подписи (ЭП) и инкапсуляции ключей (KEM – Key Encapsulation Mechanism) для стандартизации[2]. Промежуточным результатом конкурса стал выход в 2024 г. трех стандартов на постквантовые криптоалгоритмы:

- FIPS (Federal Information Processing Standard – Федеральный стандарт обработки информации) 203[3] – на алгоритм KEM;
- FIPS 204[4] и 205[5] – на алгоритмы ЭП (со значительно различающимися между собой характеристиками).

1 Панасенко Сергей Петрович, кандидат технических наук, МСР, АО «Актив-софт», Москва, ORCID 0000-0001-6752-5117. E-mail: panasenko@guardant.ru
2 Post-Quantum Cryptography. https://csrc.nist.gov/pqc-standardization.
3 FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. https://doi.org/10.6028/NIST.FIPS.203.
4 FIPS 204. Module-Lattice-Based Digital Signature Standard. https://doi.org/10.6028/NIST.FIPS.204.
5 FIPS 205. Stateless Hash-Based Digital Signature Standard. https://doi.org/10.6028/NIST.FIPS.205.

Таблица 1.

Назначение основных параметров алгоритма SLH-DSA

Параметр	Стандартные значения	Назначение
n	16, 24, 32	Размер в байтах подписываемого хеш-кода и элементов ключей и подписи схемы WOTS+
d	7, 8, 17, 22	Количество уровней деревьев XMSS в гипердереве
h'	3, 4, 8, 9	Высота (количество уровней узлов/листьев) дерева XMSS
a	6, 8, 9, 12, 14	Количество элементов дерева схемы FORS
k	14, 17, 22, 33, 35	Размер элемента дерева схемы FORS в битах

Одной из явных проблем перехода на постквантовые криптоалгоритмы можно считать достаточно высокую (а в ряде случаев, например, в части стандартизованного в FIPS 205 алгоритма SLH-DSA (Stateless Hash-Based Digital Signature Algorithm – алгоритм электронной подписи на основе хеширования без сохранения состояния) – очень высокую) ресурсоемкость постквантовых криптоалгоритмов, включая стандартизованные, тогда как одно из востребованных потенциальных применений таких алгоритмов предполагает их реализацию в устройствах с ограниченными вычислительными ресурсами.

В качестве примера таких применений рассмотрим смарт-карты, представляющие собой защищенные микроэлектронные устройства (в общем случае, с ограниченными вычислительными ресурсами), обычно обладающие криптографическими возможностями, включая вычисление ЭП и выполнение протоколов аутентификации.

В данной работе проводится анализ применимости алгоритма SLH-DSA в смарт-картах, прежде всего, с точки зрения значительно увеличенных размеров его ЭП, и формулируются предложения по модификации стандартного протокола взаимодействия со смарт-картами с целью его адаптации под основные характеристики данного алгоритма.

Основные свойства алгоритма SLH-DSA приведены в разделе 1. Раздел 2 посвящен описанию основных стандартных протоколов информационного обмена между смарт-картами и считывателями, включая основные команды для использования криптографических возможностей смарт-карт в части ЭП. В разделе 3 сопоставляются характеристики алгоритма SLH-DSA и высвечиваются проблемные моменты при его применении с точки зрения протоколов обмена, описанных в разделе 2. Рекомендации по модификации данных протоколов для их адаптации к характеристикам постквантовых алгоритмов ЭП, включая SLH-DSA, даются в разделе 4.

1. Алгоритм SLH-DSA

SLH-DSA основывается на концепции применения одноразовых электронных подписей, в качестве которых используются модифицированная одноразовая электронная подпись Винтерница WOTS+ (Winternitz One Time Signature) [4] и схема электронной подписи с ограниченным количеством применений FORS (Forest of Random Subsets) [5] совместно с многоуровневой древовидной структурой расширенной одноразовой подписи Меркля XMSS (Extended Merkle Signature Scheme) [6]. Определяющий данный алгоритм стандарт FIPS 205 основан на проанализированном в рамках вышеописанного конкурса NIST алгоритме ЭП SPHINCS+ [5] с рядом изменений относительно оригинального алгоритма.

Алгоритм SLH-DSA является параметризуемым и имеет несколько вариантов с фиксированными параметрами, а также подварианты с детерминиро-

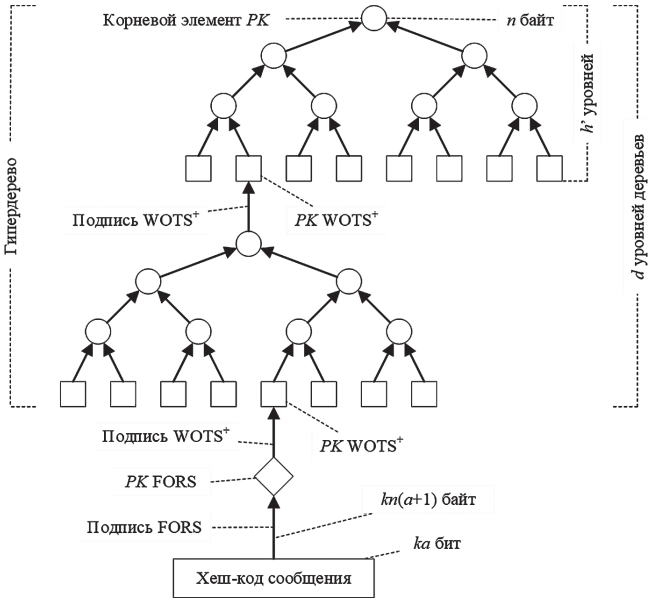


Рис. 1. Упрощенная схема структуры данных алгоритма SLH-DSA

ванным вычислением ЭП и с внешним хешированием. Описание параметров алгоритма приведено в табл. 1, а общая структура алгоритма – на рис. 1.

В числе прочего, параметры алгоритма определяют размеры секретного (SK) и открытого (PK) ключей, а также ЭП; зависимость данных размеров от параметров алгоритма приведена в табл. 2.

Таблица 2.

Размеры ключей и ЭП алгоритма SLH-DSA в зависимости от значений параметров

Элемент	Размер в байтах
Секретный ключ	$4n$
Открытый ключ	$2n$
ЭП	$n(1+k(1+a)+d(h'+2n+3))$

FIPS 205 описывает 12 вариантов алгоритма SLH-DSA: по 6 различных наборов параметров для вариантов данного алгоритма, основанных на хеш-функциях с переменным размером выходного значения SHAKE[6] или хеш-функциях семейства SHA-2[7]. Размеры ключей и ЭП стандартных вариантов алгоритма SLH-DSA приведены в табл. 3, где в наименовании варианта указано, какая хеш-функция в нем применяется; дополнительные индексы в названии каждого из вариантов («s» или «f») обозначают направление оптимизации конкретного варианта: с целью ускорения вычисления ЭП («f» от «fast») или с целью уменьшения ее размера («s» от «small»).

6 Определены в FIPS 202. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. http://dx.doi.org/10.6028/NIST.FIPS.202.

7 Определены в FIPS 180-4. Secure Hash Standard (SHS). http://dx.doi.org/10.6028/NIST.FIPS.180-4.

2. Стандартный протокол взаимодействия со смарт-картами

Различные характеристики смарт-карт (от физических параметров до команд прикладного уровня) стандартизованы в семействах стандартов ГОСТ Р ИСО/МЭК 7816 (контактные карты и общие свойства карт различных интерфейсов), 10536, 14443 и 15693 (бесконтактные карты с различной дальностью действия). Общим для смарт-карт различных типов является стандартный протокол логического уровня APDU (Application Protocol Data Unit)[8], краткое описание которого приведено далее.

2.1. Краткое описание протокола

Протокол APDU предполагает взаимодействие считывателя и карты с помощью двух следующих типов информационных пакетов:

- командный запрос C-APDU (Command APDU), направляемый считывателем карте;
- ответ на командный запрос R-APDU (Response APDU), возвращаемый картой считывателю.

Инициатором обмена данными со смарт-картой является считыватель: карта является ведомым устройством и только отвечает на командные запросы, при этом карта в работоспособном состоянии должна обязательно ответить на каждый запрос считывателя.

Команда C-APDU состоит из следующего набора элементов:

- заголовка фиксированного размера, состоящего из четырех однобайтных полей класса (CLA), кода (INS) и параметров команды (P1, P2);
- опциональных полей размера данных команды (Lc) и самих данных (если команда содержит данные);

8 Определен в ГОСТ Р ИСО/МЭК 7816-4-2013. Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена.

Таблица 3.

Размеры ключей и ЭП стандартных вариантов алгоритма SLH-DSA в байтах

Вариант алгоритма	Размер в байтах		
	Секретный ключ	Открытый ключ	ЭП
SLH-DSA-SHA2-128s SLH-DSA-SHAKE-128s	64	32	7856
SLH-DSA-SHA2-128f SLH-DSA-SHAKE-128f	64	32	17088
SLH-DSA-SHA2-192s SLH-DSA-SHAKE-192s	96	48	16224
SLH-DSA-SHA2-192f SLH-DSA-SHAKE-192f	96	48	35664
SLH-DSA-SHA2-256s SLH-DSA-SHAKE-256s	128	64	29792
SLH-DSA-SHA2-256f SLH-DSA-SHAKE-256f	128	64	49856

- опционального поля максимального размера данных ответа (Le – если команда подразумевает, что в ответе на нее должны быть переданы данные).

Ответ R-APDU содержит следующие элементы:

- опциональное поле данных ответа;
- двухбайтное поле статуса (SW) выполнения команды (SW1, SW2).

2.2 Команды протокола, относящиеся к электронной подписи

Поскольку выполнение криптографических операций является одним из основных назначений смарт-карт, стандартами ГОСТ Р ИСО/МЭК 7816 предусмотрен достаточно широкий набор команд для выполнения криптографических операций; команды, напрямую относящиеся к ЭП, приведены в табл. 4[9].

Таблица 4.

Команды, относящиеся к процедурам ЭП

Команда	Назначение
GENERATE ASYMMETRIC KEY PAIR	Генерация пары асимметричных ключей или запрос открытого ключа сгенерированной ранее пары
PERFORM SECURITY OPERATION, операция COMPUTE DIGITAL SIGNATURE	Вычисление электронной подписи
PERFORM SECURITY OPERATION, операция VERIFY DIGITAL SIGNATURE	Проверка электронной подписи

Помимо этого, процедуры вычисления и проверки ЭП могут быть использованы в некоторых из команд аутентификации, такие команды перечислены в табл. 5[10].

Таблица 5.

Команды аутентификации, в которых могут быть применены процедуры ЭП

Команда	Назначение
INTERNAL AUTHENTICATE	Аутентификация карты терминалом
EXTERNAL AUTHENTICATE	Аутентификация терминала картой
GENERAL AUTHENTICATE	Аутентификация карты терминалом, аутентификация терминала картой или взаимная аутентификация

9 Определены в ГОСТ Р ИСО/МЭК 7816-8-2011. Карты идентификационные. Карты на интегральных схемах. Часть 8. Команды для операций по защите информации.

10 Определены в ГОСТ Р ИСО/МЭК 7816-4-2013. Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена.

3. Проблемы применения алгоритма SLH-DSA в смарт-картах

Как видно из приведенной выше таблицы 3, размеры ключей алгоритма SLH-DSA являются относительно небольшими, тогда как размеры ЭП превышают размеры ЭП стандартизованных ранее в США алгоритмов ЭП[11] на 1–3 порядка (в зависимости от конкретного варианта алгоритма SLH-DSA и конкретного сравниваемого алгоритма).

Изначально, при формулировке требований к алгоритмам, подаваемым на конкурс по выбору постквантовых алгоритмов ЭП и KEM для последующей стандартизации, NIST определил уровень криптостойкости алгоритма как наиболее значимый фактор для его выбора, тогда как ресурсоемкость алгоритма (выраженная, прежде всего, в размерах ключей, подписи для алгоритма ЭП, шифртекста для KEM и ресурсах, требуемых для выполнения основных процедур алгоритма)[12] также рассматривалась, но как второстепенный по сравнению с криптостойкостью фактор выбора. При этом применимость алгоритмов в устройствах с ограниченными ресурсами при анализе ресурсоемкости алгоритма практически не рассматривалась.

В дальнейшем, при отборе алгоритмов в последующие этапы конкурса NIST четко следовал данной линии: решающим фактором при сравнении алгоритмов была их криптостойкость, важным фактором была диверсификация вычислительно сложных задач, на которых основаны отбираемые алгоритмы, с целью резервирования на случай появления в будущем быстрых методов решения конкретных задач, тогда как ресурсоемкость алгоритмов рассматривалась как менее важный фактор[13]. Аналогичного подхода NIST придерживается и в рамках проходящего сейчас дополнительного конкурса по отбору постквантовых алгоритмов ЭП[14].

Результатом такого подхода явился выбор SPHINCS+ в качестве одного из стандартизуемых алгоритмов, несмотря на значительные размеры ключей и ЭП, а также очень значительную ресурсоемкость данного алгоритма, процедуры которого выполняются, в общем случае, на несколько порядков

11 Определенных в FIPS 186-5. Digital Signature Standard (DSS). https://doi.org/10.6028/NIST.FIPS.186-5.

12 Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

13 См. отчеты NIST: 1) NIST IR 8240. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8240. 2) NIST IR 8309. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8309. 3) NIST IR 8413-upd1. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8413-upd1.

14 См.: 1) Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf. 2) NIST IR 8528. Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8528.

медленнее традиционных стандартных алгоритмов ЭП[15]. Таким образом, реализация алгоритма SLH-DSA в устройствах с ограниченными ресурсами представляет собой весьма сложную задачу, что в той или иной степени свойственно многим из постквантовых алгоритмов ЭП [7].

Возможны различные аспекты ограничений ресурсов смарт-карт, включая:

- ограниченность вычислительных ресурсов микроконтроллера смарт-карты;
- ограниченность энергонезависимой и (особенно) оперативной памяти;
- ограниченность энергопитания смарт-карты;
- ограниченная полоса пропускания канала связи между смарт-картой и считывателем.

При этом существуют относительно высокопроизводительные смарт-карты, которым практически не свойственны первые два из перечисленных выше ограничений; ограниченность энергопитания, прежде всего, характерна для бесконтактных смарт-карт, питающихся за счет наведенного считывателем сигнала, тогда как ограничение полосы пропускания является свойством стандартного протокола обмена.

4. Подходы к реализации обмена данными между смарт-картой и терминалом в части применения алгоритма SLH-DSA

Рассмотрим возможные варианты организации вычисления ЭП смарт-картой и передачи результатов вычислений (в частности, в рамках выполнения операции COMPUTE DIGITAL SIGNATURE команды PERFORM SECURITY OPERATION) от смарт-карты к считывателю с учетом свойственных смарт-картам ограничений.

4.1. Последовательная реализация вычислений и обмена данными

Схема взаимодействия считывателя и смарт-карты при последовательном вычислении ЭП и передаче результатов приведена на рис. 2.

15 Согласно замерам производительности, выполняемым в рамках проекта eBACS: ECRYPT Benchmarking of Cryptographic Systems. https://bench.cr.yp.to.

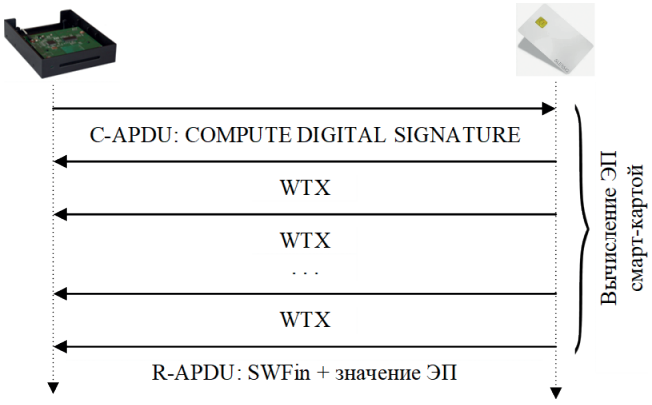


Рис. 2. Схема последовательного взаимодействия

Данная схема основана на следующих предположениях:

- ресурсов смарт-карты (вычислительных ресурсов, оперативной и энергонезависимой памяти) достаточно для размещения программного кода (в случае программной реализации), вычисления ЭП и размещения необходимых для вычисления данных и результатов вычисления;
- смарт-карта поддерживает опциональный расширенный формат C-APDU и R-APDU, который допускает передачу до 2^{16}-1 байт данных команды и до 2^{16} байт данных ответа включительно, в отличие от короткого формата, максимальный размер данных в котором составляет 255 байт; в этом случае даже ЭП максимального размера, предусмотренного алгоритмом SLH-DSA (49856 байт) может быть передана в одном R-APDU; стоит отметить, что расширенный формат R-APDU при его поддержке реализуется путем пофрагментой (не более 256 байт в одном фрагменте) передачи данных нижележащим транспортным протоколом с подтверждением получения каждого фрагмента;
- смарт-карта поддерживает продление времени ожидания ответа на команду от смарт-карты (стандартом[16] предусмотрен таймаут ожидания ответа от карты на команду, который согласовывается в процессе установки соединения и может составлять до нескольких секунд; в случае превышения таймаута терминал имеет право предположить, что карта «зависла», и снять с нее питание) путем направления терминалу запросов WTX (Waiting Time Extension – расширение времени ожидания) на продление времени ожидания; в общем случае, вычисление ЭП с учетом высокой ресурсоемкости алгоритма SLH-DSA может не уложиться в таймаут.

Основным недостатком такого подхода можно считать относительно высокие требования к оперативной памяти, которой должно быть достаточно для хранения вычисленной ЭП целиком до ее отправки в ответе. В совокупности с изложенными выше предположениями о возможностях смарт-карты можно сделать вывод о том, что такой вариант взаимодействия может быть реализован только в смарт-картах, находящихся в верхней части спектра существующих смарт-карт с точки зрения оснащенности ресурсами.

4.2. Пофрагментная передача данных по мере вычисления

Согласно стандарту FIPS 205, ЭП алгоритма SLH-DSA имеет структуру, приведенную в табл. 6.

16 ГОСТ Р ИСО/МЭК 7816-4-2013. Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена.

Таблица 6.
Структура и размер компонентов ЭП алгоритма SLH-DSA

Компонент	Назначение	Размер в байтах
R	Псевдослучайное значение	n
SIG_{FORS}	ЭП алгоритма FORS	$nk(1+a)$
SIG_{HT}	ЭП гипердерева	$nd(h'+2n+3)$

При этом компоненты ЭП вычисляются последовательно:

- псевдослучайное значение R вычисляется на достаточно раннем этапе в результате хеширования компонента секретного ключа, случайного значения (при его использовании) и подписываемого сообщения;
- затем на основе хеш-кода сообщения и значения R, дополненных компонентами открытого ключа, вычисляется компонент SIG_{FORS}, причем вычисления производятся пофрагментно: выполняется k итераций, в каждой из которых вычисляется $1 + a$ фрагментов по n байт;
- на финальном этапе вычисляется компонент SIG_{HT}, также по-фрагментно: данный компонент состоит из d значений подписи XMSS, каждое из которых имеет размер $n(h'+2n+3)$ и при необходимости может рассматриваться как совокупность фрагментов меньшего размера: сначала – $2n + 3$ фрагментов, затем – h' фрагментов, каждый из них размером по n байт.

Таким образом, вместо последовательного вычисления ЭП и ее передачи выглядит возможным организовать передачу компонентов ЭП по мере их вычисления. Схема обмена данными при таком варианте приведена на рис. 3.

Данная схема по-прежнему предъявляет относительно высокие требования к оперативной памяти для хранения компонентов ЭП (не менее $nd(h'+2n+3)$ байт), а также требует поддержки смарт-картой расширенного формата R-APDU. При этом остается относительно большая вероятность, что вычисление каждого из компонентов не уложится в таймаут, поэтому на рис. 3. приведены запросы WTX для продления времени ожидания ответа.

Показанная на рис. 3 команда GET RESPONSE позволяет получить от карты данные, которые карта готова передать, но по каким-либо причинам не может передать в текущем R-APDU. В случае наличия таких данных об этом сигнализирует специальное значение статуса выполнения текущей команды (обозначено на рисунках как SWPart). Предполагается, что в случае отсутствия ошибок выполнения

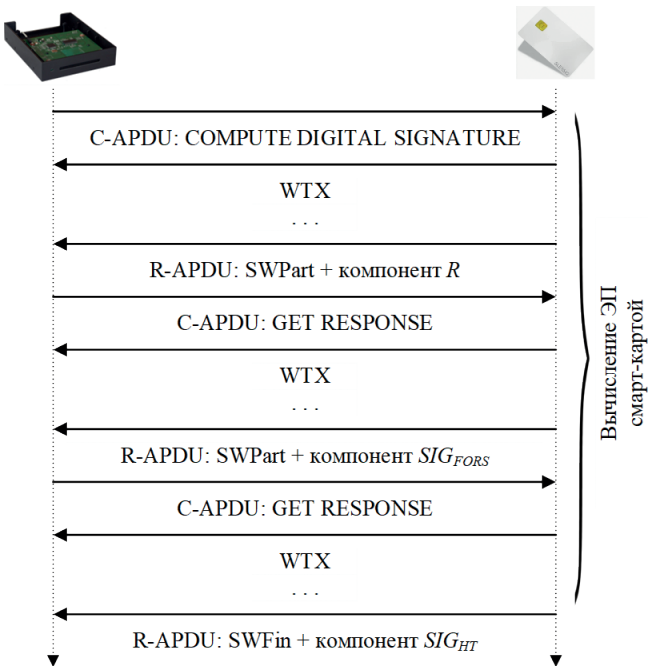


Рис. 3. Покомпонентная передача результатов вычисления

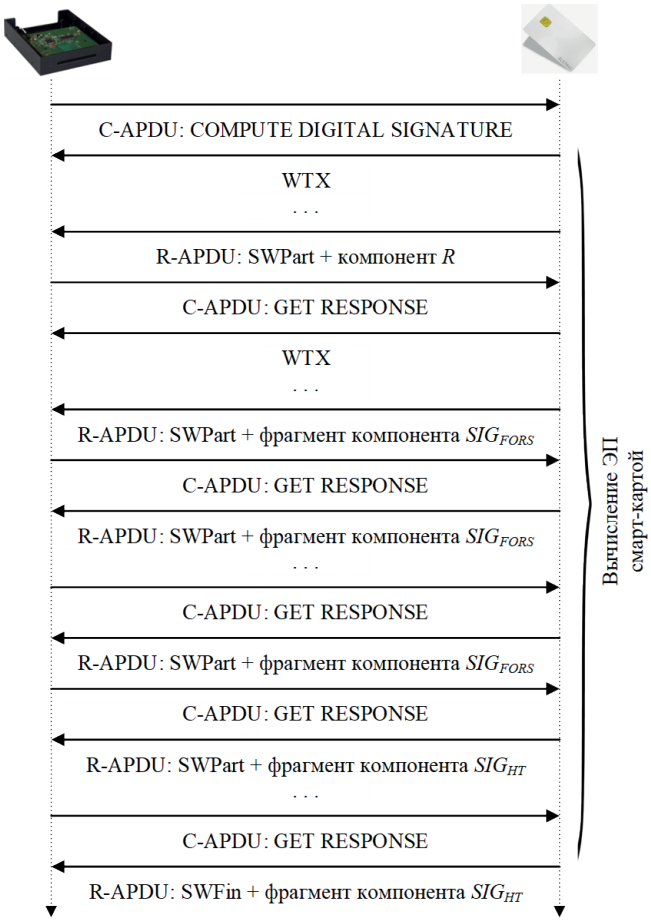


Рис. 4. Пофрагментная передача результатов вычисления

операции при передаче последнего фрагмента передается значение статуса, индицирующее корректное завершение обработки команды[17] (обозначено на рисунках как SWFin). Поскольку команда GET RESPONSE поддерживается не всеми нижележащими транспортными протоколами, вместо нее с тем же эффектом можно использовать цепочки команд C-APDU (устанавливаются определенным битом поля CLA, но поддерживаются не всеми типами смарт-карт) или проприетарные команды, реализующие аналогичный функционал.

Радикального уменьшения требований к оперативной памяти можно добиться дальнейшим разделением компонентов ЭП на n-байтные фрагменты и пофрагментой передачей результатов вычисления ЭП по мере вычисления таких фрагментов (всего $1 + k(1 + a) + d(h' + 2n + 3)$ фрагментов). Схема такого варианта приведена на рис. 4.

Помимо требований к оперативной памяти, данный вариант не требует поддержки картой расширенного формата R-APDU, поскольку n-байтный фрагмент заведомо помещается в 255-байтном блоке данных обязательного для поддержки короткого формата.

В этом случае также может потребоваться наличие запросов WTX в случаях выполнения относительно длительных вычислений перед передачей конкретного фрагмента ЭП. На рис. 4 показаны запросы WTX для таких случаев, которыми являются:

- передача значения R;
- передача первого фрагмента компонента SIG_{FORS}.

Данный вариант взаимодействия также имеет видимые недостатки:

- для эффективного взаимодействия по данной схеме требуется наличие в смарт-карте криптографического сопроцессора (см. далее) или отдельного блока, отвечающего за передачу данных (обычно передача данных управляется центральным процессором (ЦП) смарт-карты), поскольку выполнение генерации ЭП и передачи данных только под управлением ЦП (это справедливо и для описанного ранее варианта с покомпонентной передачей ЭП) по сути является последовательным и, следовательно, применение простой последовательной схемы будет наиболее эффективным для данного случая;
- значительно повышаются накладные расходы в части передачи данных, что, прежде всего, должно проявляться в задержках передачи: для передачи очередного фрагмента ЭП карта должна дождаться получения команды GET RESPONSE; следовательно, данный вариант можно считать эффективным только в том случае, когда время между началом передачи R-APDU с фрагментом данных и завершением получения следующей команды GET RESPONSE не превышает времени вычисления очередного фрагмента ЭП; поскольку расширенный APDU (при его поддержке картой) предполагает схожую пофрагментную передачу данных с квитированием на транспортном уровне, теоретически возможно передавать данные по мере их вычисления в таких фрагментах (путем прямого взаимодействия с транспортным уровнем), что выглядит несколько более эффективным с точки зрения общего времени передачи ЭП;
- важным недостатком можно считать отсутствие поддержки функционала команды GET RESPONSE в ряде протоколов транспортного уровня.

Криптографический сопроцессор смарт-карт при его наличии реализуется в виде отдельного модуля, способного производить вычисления независимо от ЦП (см., в частности, [8]). При этом функциональность такого сопроцессора может быть различной и варьироваться от выполнения конкретных преобразований в рамках алгоритма ЭП до вычисления ЭП целиком; возможности по распараллеливанию вычислений и передачи данных напрямую зависят от полноты реализации в нем процедуры вычисления ЭП. Необходимо отметить, что в бесконтактных смарт-картах параллельные вычисления могут быть ограничены во избежание наведения помех при передаче данных и с целью минимизации энергопотребления.

4.3. Предложения по модификации стандартного протокола обмена данными

С учетом вышесказанного, наиболее эффективным решением выглядела бы возможность передачи n-байтных фрагментов картой по мере их вычисления без ожидания дополнительных запросов от считывателя, что не соответствует протоколу APDU, в рамках которого карта может только отвечать на запросы считывателя определенным образом сформированными пакетами R-APDU. Вариант подобной, схожей с потоковой, передачи данных по мере их формирования стандартом не предусмотрен, но для его поддержки достаточно внесения относительно незначительных изменений в протокол APDU, заключающихся в следующем:

- введение дополнительного значения статуса (обозначим его SWMore), обозначающего тот факт, что в текущем R-APDU передается только часть данных и карта отправит дополнительный ответ с данными по мере их готовности;
- регламентация поведения считывателя при получении такого статуса: считыватель обязан сохранить

17 Команда и значения статуса определены в ГОСТ Р ИСО/МЭК 7816-4-2013. Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена.

полученные данные (или начать их обработку, если она допустима), продлить период ожидания ответа (аналогично запросу WTX) и ждать получения следующего R-APDU с недостающими данными или их частью.

Схема взаимодействия при реализации данного сценария приведена на рис. 5.

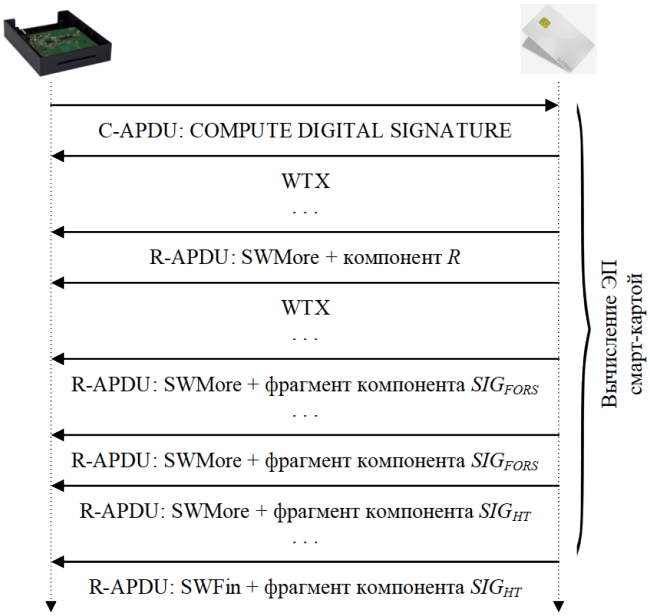


Рис. 5. Потоковая передача результатов вычисления

Данная схема позволит (при наличии у карты технической возможности) параллельно выполнять вычисления ЭП и передачу ее фрагментов сразу после вычисления, не дожидаясь каких-либо дополнительных команд от считывателя, что должно значительно снизить задержки взаимодействия и, таким образом, снизить общее время выполнения команды вычисления ЭП, включая время, требуемое на передачу результата вычисления.

При использовании предлагаемого варианта передачи картой результата вычисления ЭП значительно снижаются требования к карте в части наличия большого объема оперативной памяти и поддержки расширенного формата R-APDU. Тем не менее, поскольку алгоритм SLH-DSA обладает значительными требованиями к вычислительным ресурсам, может быть востребована точная оценка его требований к вычислительным ресурсам смарт-карты, в которой данный алгоритм может быть реализован, с учетом ограниченности времени выполнения его процедур.

Однозначным недостатком предложенной модернизации протокола APDU является предъявление требований к смарт-карте по наличию в ней дополнительных вычислителей, помимо ЦП: криптографического сопроцессора или модуля, управляющего приемом и передачей данных. Распараллеливание передачи данных и вычислений, кроме того, выглядит проблематичным при использовании бесконтактных смарт-карт. Однако необходимо отметить, что невозможность распараллеливания не помешает использованию модернизированного протокола, но сделает его применение неэффективным; в таких случаях могут быть применены стандартные схемы обмена данными, описанные в подразделах 4.1. и 4.2., при условии наличия необходимой поддержки в смарт-карте. Альтернативным вариантом является реализация пофрагментной передачи данных на транспортном уровне.

Еще одним недостатком предложенного подхода является необходимость доработки существующего стандарта, определяющего протокол APDU (стандарт принят достаточно давно, проверен временем и широко используется). Потребуется также модификация программного обеспечения считывателей для внесения предложенной функциональности. Поскольку изменения в протоколе не являются значительными и сохраняют совместимость с выпущенными ранее смарт-картами, модифицированные считыватели должны сохранить возможность взаимодействия как со смарт-картами, соответствующими текущему варианту протокола, так и с новыми смарт-картами с поддержкой предложенных возможностей.

Выводы

Особенности ряда постквантовых алгоритмов ЭП, включая их значительную ресурсоемкость, могут препятствовать применению таких алгоритмов в устройствах с ограниченными ресурсами, в частности, в смарт-картах. Предложенная в данной работе модернизация стандартного протокола APDU позволит снизить требования к смарт-картам, в которых могут быть реализованы ресурсоемкие постквантовые алгоритмы.

Вместе с тем, в ряде смарт-карт применение предложенного протокола не будет эффективным; кроме того, общая ресурсоемкость вычисления ЭП может быть настолько высока, что относительный выигрыш во времени от параллельных вычислений ЭП и передачи данных может быть незначительным.

Следовательно, выглядит востребованной разработка и стандартизация постквантовых криптоалгоритмов с пониженными требованиями к ресурсам для применения в устройствах с ограниченными ресурсами, включая смарт-карты.

Автор выражает благодарность К.Я. Мытнику (АО «НИИМЭ») за крайне ценные замечания по данной работе.

Литература
1. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 1997, 27(5).
2. Chen Z.-Y. et al. Enabling large-scale and high-precision fluid simulations on near-term quantum computers. Computer Methods in Applied Mechanics and Engineering, 2024, 432, Part B, 117428. DOI:10.48550/arXiv.2406.06063.
3. Baumgärtner L. et al. When – and how – to prepare for post-quantum cryptography [Electronic resource]. – URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography#/ (date of treatment: 31.01.2025) – McKinsey Digital – May 4, 2022.
4. Hülsing A. W-OTS+ – Shorter Signatures for Hash-Based Signature Schemes. Report 2017/965 – Cryptology ePrint Archive – TU Darmstadt – 2017.
5. Aumasson J.-P. et al. SPHINCS+. Submission to the NIST post-quantum project, v.3.1 [Electronic resource]. – URL: https://sphincs.org/data/sphincs+-r3.1-specification.pdf (date of treatment: 06.02.2025) – June 10, 2022.
6. Buchmann J., Dahmen E., Hülsing A. XMSS – A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions. Second Version. Report 2011/484 – Cryptology ePrint Archive – TU Darmstadt – November 26, 2011.
7. Liu T., Ramachandran G., Jurdak R. Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization. arXiv:2401.17538v1 – 31 Jan 2024.
8. Мытник К. Я., Панасенко С. П. Смарт-карты и информационная безопасность / под редакцией д. т. н., профессора В. Ф. Шаньгина. – М.: ДМК Пресс, 2019. – 516 с.

ON THE APPLICABILITY OF THE POST-QUANTUM ELECTRONIC SIGNATURE STANDARD SLH-DSA IN SMART CARDS

Panasenko S. P.[18]

Keywords: *electronic signature, post-quantum cryptography, smart card, APDU protocol, SLH-DSA algorithm.*

The aim of the work: *to analyze the influence of the standard protocol of exchange with smart cards on the applicability of resource-intensive post-quantum algorithms of electronic signature in devices with limited resources using smart cards as an example and to provide recommendations for upgrading the standard protocol based on the analysis results.*

Research methods: *information theory, systems analysis, object-oriented analysis.*

Research results: *various scenarios of interaction with a smart card using the standard protocol of exchange are analyzed using the example of the smart card performing the function of calculating an electronic signature using the SLH-DSA post-quantum algorithm standardized in the USA; as a result of the analysis, limitations of the standard protocol of exchange are shown, directly hindering the applicability of the SLH-DSA algorithm (and algorithms similar in characteristics) in smart cards.*

Scientific novelty: *based on the results of the analysis, a direction of modernization of the standard protocol of exchange with smart cards is proposed for its adaptation to the characteristics of resource-intensive post-quantum algorithms of electronic signature; The proposed protocol upgrade will allow the use of a number of post-quantum cryptographic algorithms in smart cards.*

References
1. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 1997, 27(5).
2. Chen Z.-Y. et al. Enabling large-scale and high-precision fluid simulations on near-term quantum computers. Computer Methods in Applied Mechanics and Engineering, 2024, 432, Part B, 117428.
3. Baumgärtner L. et al. When – and how – to prepare for post-quantum cryptography [Electronic resource]. – URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography#/ (date of treatment: 01/31/2025) – McKinsey Digital – May 4, 2022.
4. Hülsing A. W-OTS+ – Shorter Signatures for Hash-Based Signature Schemes. Report 2017/965 – Cryptology ePrint Archive – TU Darmstadt – 2017.
5. Aumasson J.-P. et al. SPHINCS+. Submission to the NIST post-quantum project, v.3.1 [Electronic resource]. – URL: https://sphincs.org/data/sphincs+-r3.1-specification.pdf (date of treatment: 02/06/2025) – June 10, 2022.
6. Buchmann J., Dahmen E., Hülsing A. XMSS – A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions. Second Version. Report 2011/484 – Cryptology ePrint Archive – TU Darmstadt – November 26, 2011.
7. Liu T., Ramachandran G., Jurdak R. Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization. arXiv:2401.17538v1 – 31 Jan 2024.
8. Mytnik K. Ya., Panasenko S. P. Smart cards and information security / edited by Doctor of Technical Sciences, Professor V. F. Shan'gin. – M.: DMK Press, 2019. – 516 p.

18 Sergey P. Panasenko, Ph.D., MCP, JSC Aktiv-soft, Moscow, Russia. ORCID 0000-0001-6752-5117. E-mail: panasenko@guardant.ru

УСКОРЕНИЕ АЛГОРИТМОВ ПРИВЕДЕНИЯ ЧИСЕЛ ПО МОДУЛЮ В ПОСТКВАНТОВОЙ СХЕМЕ ЭЦП FALCON

Финошин М. А.[1], Иванова И. Д.[2], Жуков И. Ю.[3]

DOI: 10.21681/2311-3456-2025-3-38-44

Цель исследования: *уменьшение объема предварительных вычислений и времени работы схемы подписи Falcon путем внедрения модифицированной версии алгоритма K-RED.*

Методы исследования: *оценка ресурсоемкости алгоритмов приведения чисел по модулю, математическое моделирование алгоритмов приведения, тестирование алгоритмов приведения в составе постквантовой схемы подписи.*

Результаты исследования: *умножение полиномов в факторкольце многочленов организовано в Falcon таким образом, что для его выполнения необходимо предварительно вычислить таблицы поиска, хранящие так называемые коэффициенты поворота. Алгоритмы приведения чисел по модулю, основанные на представлении чисел в специальной форме, требуют дополнительного масштабирования данных коэффициентов поворота на заданный фактор. На основе объема таблиц поиска, применяемых в процессе работы схемы подписи Falcon, в данном исследовании проведен сравнительный анализ ресурсоемкости алгоритмов Монтгомери и K-RED. Вследствие того, что расходы по памяти алгоритма K-RED превышают ресурсоемкость алгоритма Монтгомери почти в 2 раза, была рассмотрена его модификация, алгоритм K2-RED, которая позволяет добиться ускорения процесса приведения чисел по модулю при меньшем объеме масштабированных коэффициентов поворота. Доказана теорема, позволяющая обобщить алгоритм K-RED на случай, когда модуль приведения не является числом Прота. Также сформированы требования для размера факторов при представлении модуля приведения в форме модифицированного алгоритма K-RED, по которым было подобрано представление простых модулей в составе решения уравнения NTRU. Модифицированная версия алгоритма K-RED была реализована на языке программирования Си и внедрена в состав эталонной реализации схемы подписи Falcon. Проведено тестирование модифицированной версии алгоритма Falcon, в результате которого получено уменьшение времени выполнения процедур генерации ключей и проверки подписи.*

Научная новизна: *разработана модификация алгоритма приведения чисел по модулю K-RED, позволяющая применить модульную арифметику в форме K-RED к модулям общего вида. Данная модификация делает возможным внедрение быстрой арифметики в форме K-RED в процесс решения уравнения NTRU в составе схемы подписи Falcon, в ходе которого используются простые числа, не являющиеся числами Прота..*

Ключевые слова: *коэффициенты поворота, таблицы поиска, уравнение NTRU, преобразование NTT, алгоритм K-RED, алгоритм Монтгомери.*

Введение

Применение быстрых алгоритмов NTT, Кули-Тьюки и Джентельмена-Санде позволяет снизить исходную квадратичную сложность умножения полиномов до O(nlogn), однако достижение эффективного умножения исключительно посредством программной реализации по-прежнему остается сложной задачей. Так, последние исследования на тему ускорения операций умножения полиномов в схеме подписи Falcon направлены в основном на ее аппаратное усовершенствование за счет использования NEON-инструкций [1, 2] и RISC-V-инструкций [3]. Поскольку алгоритм Falcon является сильным кандидатом на внедрение в маломощные устройства [4], подход с использованием специализированных инструкций приводит к сужению области применения модифицированной версии Falcon. В частности, ее внедрение в иные устройства, не поддерживающие конкретные инструкции, может потребовать эмуляции NEON либо RISC-V. В таком случае предполагаемое ускорение вычислений может быть достигнуто не в полной мере.

Параллельно с этим в исследованиях производительности криптографических схем CRYSTALS при ускорении числового теоретического преобразования (от англ. Number Theoretic Transform, NTT) рассматривается алгоритм K-RED и его модификации в качестве алгоритма приведения чисел по модулю [5, 6]. Таким образом, на данный момент исследования в области ускорения схемы подписи Falcon охватывают только вопрос его аппаратной модификации, не учитывая возможности усовершенствования за счет внедрения новых математических подходов.

Настоящее исследование направлено на разработку и тестирование модифицированной версии схемы подписи Falcon, которая бы включала в себя

1 Финошин Михаил Александрович, старший преподаватель кафедры «Криптология и Кибербезопасность» Национального исследовательского ядерного университета «МИФИ», г. Москва, Россия. E-mail: mafinoshin@mephi.ru, ORCID 0000-0003-4374-1645.

2 Иванова Ирина Дмитриевна, ассистент кафедры «Высшая математика» Российского университета транспорта (МИИТ), г. Москва, Россия. E-mail: iid.ivanova@yandex.ru, ORCID 0000-0003-3022-8973.

3 Жуков Игорь Юрьевич, руководитель департамента разработок ООО Группа компаний «Инфотактика», г. Москва, Россия. E-mail: izhukov@infotaktika.ru, ORCID: 0000-0002-4429-8799.

более быстрый и менее ресурсоемкий алгоритм приведения чисел по модулю.

Ресурсоемкость алгоритмов приведения в составе схемы подписи Falcon

Алгоритм Falcon является финалистом конкурса NIST 2022 года среди постквантовых схем подписи, в котором также участвовали схемы подписи CRYSTALS-Dilithium и SPHINCS+. Алгоритм Falcon предлагает более компактные, нежели у других участников, размеры открытого ключа и подписей [7]. Алгоритм Falcon построен с использованием криптографии на основе теории решеток, и его безопасность обусловлена сложностью задачи нахождения кратчайшего целочисленного решения (от англ. Short integer problem, SIS). В задаче SIS вычисления проводятся над элементами кольца многочленов, и в алгоритме Falcon применяется факторкольцо $\mathbb{Z}_q[x] / (x^n + 1)$ по модулю простого числа q. При выполнении умножения полиномов в схеме подписи Falcon применяется быстрое преобразование Фурье (БПФ) и преобразование NTT.

БПФ используется при операциях с закрытым ключом (то есть в процедуре генерации подписи), а NTT – в операциях с открытым ключом (проверка подписи) и при генерации криптографических ключей. Преобразования Фурье работает с полем комплексных чисел C и вычисляется при помощи ω, примитивного корня степени $2n$ (в случае 1-го и 5-го уровней стойкости Falcon), определяемого как $\omega = e^{2i/2n}$ (где i – мнимая единица). Для многочлена a, представимого в виде вектора $a = (a[0], ..., a[n-1])$, форма преобразования Фурье $\hat{a}$ вычисляется как:

$$\hat{a}_i = \sum_{j=0}^{n-1} a_j (\omega^i)^j. \quad (1)$$

В случае преобразования NTT вычисления выполняются над конечным полем $\mathbb{Z}_q$, и ω определяется как примитивный корень степени $2n$ в $\mathbb{Z}_q$. Поскольку ω^i в преобразовании Фурье называют коэффициентами поворота (от англ. twiddle factor), в настоящем исследовании для обозначения степеней корня из единицы, применяемых в NTT, будет также использоваться данный термин.

Одним из базовых принципов оптимизации, применяемым во многих областях программирования, являются таблицы поиска (от англ. lookup table, LUT). Таблицы коэффициентов поворота для БПФ и NTT рассчитываются при помощи детерминированных функций и при ограниченном количестве входных значений, вследствие чего они также могут быть организованы как таблицы поиска [8]. В них ключами являются индекс частоты либо степень, в которую возводится корень из единицы $2n$-го порядка, а значения – коэффициентами поворота.

При нахождении формы NTT для коэффициентов полинома вычисления в формуле (1) выполняются по простому модулю q, который должен удовлетворять следующему условию [9]:

$$q \equiv 1 \bmod 2n. \quad (2)$$

В эталонной реализации[4] схемы подписи Falcon в качестве алгоритма приведения чисел по простому модулю используется алгоритм Монтгомери (с параметром $r = 2^k$, чтобы выполнялось условие НОД$(r,q) = 1$). В прошлой работе [10] было установлено, что в качестве более быстрой альтернативы может применяться алгоритм приведения чисел по модулю K-RED. Согласно исходной формулировке[5], алгоритм K-RED использует свойства чисел Прота, представимых как:

$$q = k \cdot 2^m + 1, \quad (3)$$

где $k < 2^m$ – малое нечетное натуральное число, m – натуральное число.

При применении оригинального алгоритма K-RED в ходе вычисление формы NTT для полинома необходимо одновременно применять две функции: K-RED и K-RED-2x, чтобы предотвратить возможное переполнение в случае большой длины полиномов n. При этом в функции K-RED вычисляется приведенное значение для kc:

$$kc \equiv kc_0 - c_1 \bmod q, \quad (4)$$

где $c_0 = c \bmod 2^m$, $c_1 = [\frac{c}{2^m}]$, а в функции K-RED-2x – для k^2 c:

$$k^2 \cdot c \equiv k^2 \cdot c_0 - kc_1 + c_2 \bmod q, \quad (5)$$

где $c_0 = c \bmod 2^m$, $c_1 = \frac{c}{2^m} \bmod 2^m$, $c_2 = [\frac{c}{2^{2m}}]$.

Таким образом, при прямом применении алгоритма K-RED выход является приведенной величиной не входного значения, а масштабированного – на фактор k либо k^2.

При быстрой реализации прямого преобразования NTT используется алгоритм Кули-Тьюки, который вычисляет коэффициенты полинома в форме NTT по формулам:

$$\hat{a}_i = \hat{a}_i' + \hat{a}_i'' \cdot \omega_i \bmod q, \quad (6)$$

$$\hat{a}_{i+\frac{n}{2}} = \hat{a}_i' - \hat{a}_i'' \cdot \omega_i \bmod q, \quad (7)$$

где $\hat{a}_i' = \sum_{j=0}^{\frac{n}{2}-1} a_{2j} (\omega^2)^{ij}$ и $\hat{a}_i'' = \sum_{j=0}^{\frac{n}{2}-1} a_{2j+1} (\omega^2)^{ij}$, а $i = 0, 1, ..., \frac{n}{2}-1$. Из формул (6) и (7) видно, что вычисление каждого нового коэффициента полинома в форме NTT требует одного умножения и операции сложения или вычитания. В обоих случаях, применяется ли алгоритм K-RED к промежуточному результату произведения либо к выходу операции сложения или вычитания, коэффициент $\hat{a}_i'$ будет требовать дополни-

4 Falcon source files (reference implementation). URL: https://falcon-sign.info/impl/vrfy.c.html

5 Longa P., Naehrig M. Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography. DOI:10.1007/978-3-319-48965-0_8

тельного масштабирования на такой фактор k^s (где s – целое число), которым обладает произведение $\hat{a}_i'' \cdot \omega^i$.

В случае такого подхода возникают следующие проблемы:

- учет значения s на каждом этапе вычисления «бабочек» Кули-Тьюки и Джентельмена-Санде;
- затраты на промежуточное масштабирование в ходе работы прямого и обратного преобразований NTT;
- затраты на «выходное» масштабирование, после которого полином должен быть передан в общем виде обратно в процедуру генерации ключей.

Решить их возможно за счет масштабирования коэффициентов поворота в ходе их предварительного вычисления. Аналогично тому, как эталонная реализация схемы подписи Falcon содержит таблицы коэффициентов поворота, вычисленные в форме Монтгомери, так и в случае применения алгоритма K-RED вместо значений $\omega^i \bmod q$ необходимо использовать значения $k^s \cdot \omega^i \bmod q$ (где $s = -1$ либо $s = -2$ для функций K-RED и K-RED-2x соответственно).

Однако данное условие порождает проблему того, что использование алгоритма K-RED требует вычисления двух таблиц масштабированных коэффициентов поворота на каждое значение модуля фактор-кольца q. Поэтому, хотя алгоритм K-RED выполняется быстрее алгоритма Монтгомери [11], он требует в два раза большие расходы памяти.

Разработка модификации алгоритма K-RED

Среди различных предлагаемых исследователями модификаций алгоритма K-RED компромисс между объемом предварительно вычисляемых таблиц поиска и применением беззнаковой арифметики (которая внедрена в эталонную реализацию алгоритма Falcon) достигается в алгоритме K2-RED [12]. Функция, реализующая данный алгоритм, содержит два шага применения функции K-RED, так что выходом является приведенное значение: $\bar{\bar{c}} \equiv k^2 \cdot c \bmod q$. Поэтапно для параметров q, k, m и входного числа c в представлении (3) данный алгоритм реализуется следующим образом:

1. Вычисление c_0 и c_1: $c_0 = c \bmod 2^m$ и $c_1 = [\frac{c}{2^m}]$.
2. Первый шаг приведения по модулю
$$(\bar{c} \equiv kc \bmod q)\colon \bar{c} = kc_0 - c_1.$$
3. Вычисление c_0' и c_1': $c_0' = \bar{c} \bmod 2^m$ и $c_1' = [\frac{\bar{c}}{2^m}]$.
4. Второй шаг приведения по модулю
$$(\bar{\bar{c}} \equiv k^2 \cdot c \bmod q)\colon \bar{\bar{c}} = kc_0' - c_1'.$$
5. Алгоритм возвращает с $\bar{\bar{c}}$.

В отличие от классического K-RED, в котором во избежание переполнения на отдельных итерациях преобразования NTT необходимо заменять функцию K-RED на функцию K-RED-2x, алгоритм K2-RED не требует дополнительных шагов приведения чисел по модулю. Это позволяет сократить объем предварительно вычисляемых таблиц масштабированных коэффициентов до одной таблицы поиска на каждый модуль приведения. Кроме того, применение алгоритма K2-RED облегчает задачу анализа и устранения дополнительных факторов k^s, которые «зашумляют» выходное значение вследствие дополнительных итераций использования K-RED-2x. Таким образом, в ходе масштабирования на фактор n^{-1} внутри обратного преобразования NTT:

- дополнительное масштабирование на степень фактора k не требуется, если алгоритм K2-RED применялся исключительно в ходе прямого и обратного преобразований NTT;
- дополнительное масштабирование на степень фактора k производится в соответствии с применением алгоритма K2-RED в ходе покомпонентного умножения полиномов.

Преобразование NTT применяется в алгоритме Falcon в процессе генерации ключей и проверки подписи. При проверке подписи используется фиксированный модуль приведения, имеющий вид $q = 12289 = 3 * 2^{12} + 1$. Таким образом, факторы k и m для него также являются фиксированными, к тому же k является малым нечетным числом. В то же время процедура генерации ключей применяет хотя и заранее определенное, но целое множество простых модулей.

Закрытый ключ задается как кортеж полиномов (f, g, F, G), где полиномы f и g генерируются случайным образом как элементы факторкольца многочленов $\mathbb{Z}[x] / (x^n + 1)$ (при этом f должен быть обратимым многочленом в кольце $\mathbb{Z}_q[x] / (x^n + 1)$, а полиномы F и G вычисляются путем решения уравнения NTRU [13]:

$$fG - gF = q \bmod (x^n + 1). \quad (8)$$

Для решения уравнения применяется китайская теорема об остатках [14], вследствие чего выбирается подмножество простых чисел $\{p_i\}$, по модулю которых проводятся операции над полиномами, в частности, их умножение. Именно на этом этапе в модуле keygen.c, реализующем процедуру генерации ключей, применяется преобразование NTT. Это возможно за счет вида применяемых простых модулей:

$$p_i \equiv 1 \bmod 2n. \quad (9)$$

Поскольку размерность пространства n является степенью двойки (512 для версии Falcon 1-го уровня стойкости и 1024 для 5-го уровня стойкости), тождество (9) удовлетворяет условию (3) для применения

алгоритма приведения числа по модулю K-RED, а значит и K2-RED. Однако ввиду того, что модули $\{p_i\}$ подбираются в алгоритме Falcon таким образом, чтобы быть немногим меньше 2^{31}, подавляющее большинство из них не являются числами Прота, вследствие чего фактор k в представлении (3) оказывается большим нечетным числом. Данный факт затрудняет применение как алгоритма K-RED, так и алгоритма K2-RED при решении уравнения NTRU.

В исходной статье, предлагающей алгоритм приведения K-RED, упоминается, что данный алгоритм может быть обобщен также на случай, когда модуль приведения представим в виде:

$$q = k \cdot 2^m \pm l, \quad (10)$$

где k и l натуральные нечетные и $k \geq 3$, а $l \geq 1$.

С этой целью докажем следующую теорему:

Теорема. (Модульная арифметика для модуля вида $q = k \cdot 2^m \pm l$). Для модуля q вида (10) и любого целого числа с выполняется:

$$kc \equiv kc_0 \mp lc_1 \bmod q, \quad (11)$$

где $c_0 = c \bmod 2^m$, $c_1 = [\frac{c}{2^m}]$.

Доказательство. Очевидно, что выполняется тождество:

$$c_1 \, q \equiv 0 \bmod q. \quad (12)$$

Используем вид представления модуля (10) и произведем подстановку:

$$c_1 \cdot (k \cdot 2^m + l) \equiv 0 \bmod q. \quad (13)$$

Разнесем слагаемые по разные стороны тождества:

$$c_1 \cdot k \cdot 2^m \equiv -lc_1 \bmod q. \quad (14)$$

Воспользуемся определением переменной c_1:

$$\frac{c - c_0}{2^m} \cdot k \cdot 2^m \equiv (c - c_0) \cdot k \equiv -lc_1 \bmod q. \quad (15)$$

Таким образом, получим:

$$kc \equiv kc_0 - lc_1 \bmod q. \quad (16)$$

Полученный вывод свидетельствует о том, что в общем случае, чтобы осуществить приведение по модулю по алгоритму K-RED либо K2-RED, необходимо предварительно определить параметры k, m и l в представлении модуля приведения по формуле (10). При решении уравнения NTRU данные значения разумно хранить в таблицах поиска.

Тестирование модифицированного алгоритма K-RED

При модификации алгоритма K-RED были совмещены техники с двойным приведением по модулю (как в алгоритме K2-RED) и представлением модуля приведения по формуле (10) в соответствии с доказанной теоремой. Как уже было упомянуто, простые модули для решения уравнения NTRU подобраны таким образом, чтобы быть немногим меньше числа 2^{31}. В процессе анализа массива PRIMES модуля keygen.c рассматривались представления p_i в виде формулы (10) для различных значений m – длины младшей части исходного числа c_0 из представления (4). К сожалению, данные простые числа не являются числами Прота, потому подобрать такое значение m, чтобы $l = \pm 1$, не представляется возможным. Однако, как было доказано в прошлом разделе данной работы, алгоритм K-RED приведения числа по модулю может быть обобщен на любое l. При условии, что умножение на k и l в формуле (16) должно быть эффективным, k и l следует подбирать таким образом, чтобы они были в некотором смысле «малы» относительно применяемого модуля p. Таким образом, если в представлении простого числа порядка 2^{31} фактор k имеет порядок 2^7, то в этом случае отношение k к p будет меньше, чем в предлагаемом разложении модуля q = 12289 с k = 3.

В ходе анализа обнаружено, что начиная с m = 24 приведенные в массиве PRIMES простые числа могут быть разложены при помощи одинаковых факторов: например, k = 127 при m = 24. При увеличении m опытным путем было получено, что с уменьшением фактора k происходит рост процентного отношения l к p. Таким образом, у разложения с m = 24 были обнаружены следующие преимущества:

1) равенство факторов k для всех p из массива PRIMES при фиксированном m = 24 (это позволяет сократить расходы на таблицы поиска, содержащие параметры k, k^{-2}, k^{-4}, m для различных p);
2) простота умножения на фактор k = 127:

$$127 \times k = k \times 2^7 - k;$$

3) относительно небольшой размер l (при больших значениях m значение l в процентном отношении к p возрастает).

Поскольку подобранное представление простых чисел p_i позволяет использовать одно и то же значение m для всех модулей приведения, для облегчения вычислений при выделении остатка от деления на 2^m возможно применять операцию логического «И» с предварительно вычисленной маской. Ниже приведен фрагмент реализации модифицированного алгоритма K-RED на языке программирования Си, используемом в эталонной реализации схемы подписи Falcon:

```
z0 = k * (z & mask) - l * (z >> m).
z1 = k * (z0 & mask) - l * (z0 >> m).
return z1.
```

В данном фрагменте z – исходное приводимое по модулю значение (масштабировано на фактор k^{-2} за счет умножения на масштабированный коэффициент поворота), k, m, l – факторы из представления

(10), mask – маска, вычисляемая по значению фактора m, **z1** – выходное значение, являющееся приведением по модулю q величины $z \cdot k^{-2}$.

Тестирование предлагаемой модификации алгоритма K-RED проводилось при помощи функции «test_nist_KAT» из модуля «test_falcon.c» эталонной реализации Falcon. Данная функция использует тестовые векторы согласно представленным NIST рекомендациям. Эти рекомендации были представлены в ходе проведения соревнования между постквантовыми криптографическими схемами [15]. Тестирование выполнено для векторов длиной n = 1024, алгоритм K-RED был внедрен в прямое и обратное преобразования NTT. Результаты вычислительного эксперимента приведены для процессора Intel® Celeron(R) N4000 CPU @ 1.10GHz × 2.

В таблице 1 представлены результаты тестирования эталонной реализации с использованием алгоритма Монтгомери при приведении чисел по модулю в процессе вычисления формы NTT и выполненной реализации с использованием модифицированного алгоритма K-RED. Единица измерения времени выполнения – такты процессора.

Частично данное уменьшение времени выполнения процедур генерации ключей и проверки подписи было достигнуто за счет сохранения дополнительных предвычисленных значений. Среди них в модуле keygen.c: фиксированные факторы k и m (применяются в процессе применения алгоритма приведения K-RED), по одной таблице поиска на k^{-2} и k^{-4} (нужны при масштабировании коэффициентов поворота) и одна таблица поиска со значениями фактора l для элементов массива PRIMES. В модуле vrfy.c масштабированная таблица коэффициентов поворота предварительно вычисляется и хранится аналогично таблице поиска для коэффициентов в форме Монтгомери. При этом значение фактора l фиксировано (равно 1), потому в сравнении с эталонной реализацией алгоритма Falcon изменения в затратах памяти не происходят.

В таблице 2 приведен сравнительный анализ затрат по памяти и по времени схемы подписи Falcon с использованием модифицированного алгоритма приведения K-RED в сравнении с эталонной реализацией.

Как видно из таблицы 2, форма модуля простого числа (10) незначительно влияет на прирост производительности в выполнения преобразования NTT, что позволяет утверждать, что предлагаемая модификация алгоритма K-RED с неединичным фактором l может быть эффективной альтернативой применяемому в эталонной реализации алгоритму Монтгомери. При этом общий прирост производительности в модуле keygen.c меньше, чем в vrfy.c, за счет более сложного алгоритма, также включающего в себя вычисления с плавающей запятой с применением БПФ.

Таблица 1.

Результаты тестирования эталонной реализации схемы подписи Falcon и с применением модифицированного алгоритма K-RED

Модуль, содержащий вычисления в форме NTT		**Эталонная реализация + Монтгомери**	**Эталонная реализация + модифицированный K-RED**
vrfy.c	Прямое преобразование NTT	6 845 т.	5 921 т.
	Обратное преобразование NTT	3 641 т.	3 271 т.
	Всего	17 630 т.	16 431 т.
keygen.c	Прямое преобразование NTT	11 452 т.	10 082 т.
	Обратное преобразование NTT	8 149 т.	7 415 т.
	Всего	56 588 т.	54 167 т.

Таблица 2.

Сравнительный прирост производительности эталонной реализации с применением модифицированного алгоритма K-RED

	Модуль, содержащий вычисления в форме NTT					
	vrfy.c			keygen.c		
Изменение затрат по памяти	–			+3 LUT		
Изменение времени выполнения	NTT	INTT	Всего	NTT	INTT	Всего
	14 %↓	10 %↓	7 %↓	12 %↓	9 %↓	4 %↓

Выводы

В результате настоящего исследования предложен и протестирован в составе схемы подписи Falcon модифицированный алгоритм K-RED. В ходе работы проведен анализ ресурсоемкости классического алгоритма K-RED в сравнении с алгоритмом Монтгомери, применяемым в эталонной реализации Falcon. Рассмотрен алгоритм K2-RED, являющийся модификацией алгоритма K-RED и позволяющий уменьшить объем требуемых предварительно вычисляемых значений, которые применяются при работе преобразования NTT. Доказана теорема, позволяющая обобщить алгоритм K-RED на простые числа, не являющиеся числами Прота. Выполнена модификация алгоритма K-RED, объединившая в себе техники из алгоритма K2-RED и выводы из доказанной в настоящем исследовании теоремы.

Модифицированная версия алгоритма K-RED была внедрена в состав эталонной реализации схемы подписи Falcon и протестирована, в результате чего получено уменьшение времени выполнения как процедуры проверки подписи, так и процедуры генерации ключей. Дополнительные расходы по памяти при этом составили 3 таблицы поиска, хранящие факторы формы K-RED. В дальнейших исследованиях планируется использовать модифицированную в настоящей работе схему подписи Falcon для сравнения производительности протокола TLS в случае применения классических и постквантовых схем подписи.

Литература

1. Accelerating Falcon on ARMv8 / Y. Kim, J. Song, S.C. Seo // IEEE Access. 2022. Vol. 10. p. 44446–44460. DOI: 10.1109/ACCESS.2022.3169784.
2. Nguyen D.T., Gaj K. Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions // International Conference on Cryptology in Africa. 2023. P. 417–441. DOI: 10.1007/978-3-031-37679-5_18.
3. Wang L.N. et al. Support Post Quantum Cryptography with SIMD Everywhere on RISC-V Architectures // Workshop Proceedings of the 53rd International Conference on Parallel Processing. 2024. P. 23–32. DOI: 10.1145/3677333.3678149.
4. Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms / M. Raavi, S. Wuthier, P. Chandramouli [et al] // International Conference on Applied Cryptography and Network Security. 2021. Vol. 12727. p. 424–447. DOI: 10.1007/978-3-030-78375-4_17.
5. HyperNTT: A Fast and Accurate NTT/INTT Accelerator with Multi-Level Pipelining and an Improved K2-RED Module / D.N. Nguyen, H.L. Pham, V.T.D. Le [et al] // 2024 International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC). 2024. P. 1–6. DOI: 10.1109/ITC-CSCC62988.2024.10628429.
6. High-Speed and Low-Complexity Modular Reduction Design for CRYSTALS-Kyber / M. Li, J. Tian, X. Hu [et al] // 2022 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS). 2022. P. 1–5. DOI: 10.1109/APCCAS55924.2022.10090253.
7. FalconSign: An Efficient and High-Throughput Hardware Architecture for Falcon Signature Generation / Y. Ouyang, Y. Zhu, W. Zhu [et al] // IACR Transactions on Cryptographic Hardware and Embedded Systems. 2024. Vol. 2025, № 1. P. 203–226. DOI: 10.46586/tches.v2025.i1.203-226.
8. Land G., Sasdrich P., Güneysu T. A Hard Crystal – Implementing Dilithium on Reconfigurable Hardware // International Conference on Smart Card Research and Advanced Applications. 2022. P. 210–230. DOI: 10.1007/978-3-030-97348-3_12.
9. Liang Z., Zhao Y. Number Theoretic Transform and Its Applications in Lattice-based Cryptosystems: A Survey // arXiv preprint arXiv:2211.13546. 2022. 35 p. DOI: 10.48550/arXiv.2211.13546.
10. Иваненко В.Г., Иванова И.Д., Иванова Н.Д. Вычисления над полиномами в постквантовых схемах подписи // Вопросы кибербезопасности. 2024. № 4(62) С. 65–70. DOI: 10.21681/2311-3456-2024-4-65-70.
11. Nguyen T.-H., Pham C.K., Hoang T.T. A High-Efficiency Modular Multiplication Digital Signal Processing for Lattice-Based Post-Quantum Cryptography // Cryptography. 2023. Vol. 7. No. 4. p. 46. DOI: 10.3390/cryptography7040046.
12. Bisheh-Niasar M., Azarderakhsh R., Mozaffari-Kermani M. High-Speed NTT-based Polynomial Multiplication Accelerator for Post-Quantum Cryptography // 2021 IEEE 28th symposium on computer arithmetic (ARITH). 2021. P. 94–101. DOI: 10.1109/ARITH51176.2021.00028.
13. Teixeira C., Gazzoni Filho D.L., Hernandez J.C.L. Improving FALCON's Key Generation on ARMv8-A Platforms // Anais do XXIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. 2023. P. 528–533. DOI: 10.5753/sbseg.2023.233093.
14. Efficient Hardware RNS Decomposition for Post-Quantum Signature Scheme Falcon / S. Coulon, P. He, T. Bao [et al] // 2023 57th Asilomar Conference on Signals, Systems, and Computers. 2023. P. 19–26. DOI: 10.1109/IEEECONF59524.2023.10476845.
15. PQC-HA: A Framework for Prototyping and In-Hardware Evaluation of Post-Quantum Cryptography Hardware Accelerators / R. Sattel, C. Spang, C. Heinz [et al] // arXiv preprint arXiv:2308.06621. 2023. 20 p. DOI: 10.48550/arXiv.2308.06621.

ACCELERATING MODULAR REDUCTION FOR FALCON SIGNATURE SCHEME

Finoshin M.A.[6], Ivanova I.D.[7], Zhukov I.Y.[8]

6 Mihail A. Finoshin, senior lecturer of the Cryptology and Cybersecurity Department at NRNU MEPhI, Moscow, Russia. E-mail: MAFinoshin@mephi.ru, ORCID 0000-0003-4374-1645.

7 Irina D. Ivanova, assistant of Department of Higher Mathematics, Russian University of Transport (MIIT), Moscow, Russia. E-mail: iid.ivanova@yandex.ru, ORCID 0000-0003-3022-8973

8 Igor Yu. Zhukov, head of the Development Department, group of companies «Infotaktika», Moscow, Russia. E-mail: izhukov@infotaktika.ru, ORCID: 0000-0002-4429-8799.

Keywords: *twiddle factors, lookup tables, NTRU equation, NTT, K-RED modular reduction, Montgomery multiplication.*

Purpose of the study: *precomputation reducing and execution time speeding up of Falcon signature scheme by implementing a modified version of the K-RED algorithm.*

Methods of research: *resource intensity evaluation of modular reduction algorithms, mathematical modeling of modular reduction algorithms, testing of modular reduction algorithms as part of the post-quantum signature scheme.*

Results: *multiplication of polynomials in the polynomial quotient ring is organized in Falcon in such a way that its execution requires precomputed lookup tables that store so-called twiddle factors. Modular reduction algorithms based on representing numbers in a special form require additional scaling of these twiddle factors by a given factor. Based on the size of the lookup tables used in Falcon signature scheme, a comparative analysis of the resource intensity of the Montgomery and K-RED algorithms has been conducted. Due to the fact that the memory consumption of the K-RED algorithm is almost twice that of the Montgomery algorithm, the K2-RED algorithm which allows for faster modular reduction with a smaller volume of scaled twiddle factors has been considered. A theorem that generalizes the K-RED algorithm to the case where the reduction modulus is not a Proth number has been proven. Additionally, requirements for the size of modified K-RED factors have been established, based on which representations of prime moduli in the NTRU equation solution have been selected. The modified K-RED algorithm has been implemented in C language and integrated into the Falcon reference implementation. Testing of modified Falcon has been conducted, resulting in a reduction in the execution time of key generation and signature verification procedures.*

Scientific novelty: *a modified version of the K-RED algorithm that allows the application of modular arithmetic in the K-RED form to general modules has been developed. The developed version of K-RED algorithm makes it possible to use fast arithmetic in the K-RED form during the process of solving the NTRU equation as part of Falcon.*

References

1. Kim, Y., Song, J., & Seo, S. C. (2022). Accelerating Falcon on ARMv8. IEEE Access, 10, 44446-44460. DOI: 10.1109/ACCESS.2022.3169784.
2. Nguyen, D.T., & Gaj, K. (2023, July). Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions. In International Conference on Cryptology in Africa, 417-441. DOI: 10.1007/978-3-031-37679-5_18.
3. Wang, L.N., Li, J.H., Kuan, C.B., & Su, Y.C. (2024, August). Support Post Quantum Cryptography with SIMD Everywhere on RISC-V Architectures. In Workshop Proceedings of the 53rd International Conference on Parallel Processing, 23-32. DOI: 10.1145/3677333.3678149.
4. Raavi, M., Wuthier, S., Chandramouli, P., Balytskyi, Y., Zhou, X., & Chang, S.Y. (2021, June). Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms. In International Conference on Applied Cryptography and Network Security, 424–447. DOI: 10.1007/978-3-030-78375-4_17.
5. Nguyen, D.N., Pham, H.L., Le, V.T.D., Lam, D.K., Tran, T.H., & Nakashima, Y. (2024, July). HyperNTT: A Fast and Accurate NTT/INTT Accelerator with Multi-Level Pipelining and an Improved K2-RED Module. In 2024 International Technical Conference on Circuits/Systems, Computers, and Communications (ITC-CSCC), 1-6. DOI: 10.1109/ITC-CSCC62988.2024.10628429.
6. Li, M., Tian, J., Hu, X., Cao, Y., & Wang, Z. (2022, November). High-Speed and Low-Complexity Modular Reduction Design for CRYSTALS-Kyber. In 2022 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 1–5. DOI: 10.1109/APCCAS55924.2022.10090253.
7. Ouyang, Y., Zhu, Y., Zhu, W., Yang, B., Zhang, Z., Wang, H., & Liu, L. (2025). FalconSign: An Efficient and High-Throughput Hardware Architecture for Falcon Signature Generation. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(1), 203–226. DOI: 10.46586/tches.v2025.i1.203-226.
8. Land, G., Sasdrich, P., & Guneysu, T. (2021, November). A Hard Crystal – Implementing Dilithium on Reconfigurable Hardware. In International Conference on Smart Card Research and Advanced Applications, 210–230. DOI: 10.1007/978-3-030-97348-3_12.
9. Liang, Z., & Zhao, Y. (2022). Number Theoretic Transform and Its Applications in Lattice-based Cryptosystems: A Survey. arXiv preprint arXiv:2211.13546. DOI: 10.48550/arXiv.2211.13546.
10. Ivanenko, V.G., Ivanova, I.D., & Ivanova N.D. (2024). Optimization of Computations over Polynomials in Post-Quantum Signature Scheme. Voprosy kiberbezopasnosti, (4), 62, 65–70. DOI: 10.21681/2311-3456-2024-4-65-70.
11. Nguyen, T.H., Pham, C.K., & Hoang, T.T. (2023). A High-Efficiency Modular Multiplication Digital Signal Processing for Lattice-Based Post-Quantum Cryptography. Cryptography, 7(4), 46. DOI: 10.3390/cryptography7040046.
12. Bisheh-Niasar, M., Azarderakhsh, R., & Mozaffari-Kermani, M. (2021, June). High-Speed NTT-based Polynomial Multiplication Accelerator for Post-Quantum Cryptography. In 2021 IEEE 28th symposium on computer arithmetic (ARITH), 94-101. DOI: 10.1109/ARITH51176.2021.00028.
13. Teixeira, C., Gazzoni Filho, D.L., & Hernandez, J.C.L. (2023, September). Improving FALCON's Key Generation on ARMv8-A Platforms. In Anais do XXIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 528-533. DOI: 10.5753/sbseg.2023.233093.
14. Coulon, S., He, P., Bao, T., & Xie, J. (2023, October). Efficient Hardware RNS Decomposition for Post-Quantum Signature Scheme Falcon. In 2023 57th Asilomar Conference on Signals, Systems, and Computers, 19-26. DOI: 10.1109/IEEECONF59524.2023.10476845.
15. Sattel, R., Spang, C., Heinz, C., & Koch, A. (2023). PQC-HA: A Framework for Prototyping and In-Hardware Evaluation of Post-Quantum Cryptography Hardware Accelerators. arXiv preprint arXiv:2308.06621. DOI: 10.48550/arXiv.2308.06621.

АЛГОРИТМ ЭЦП НА АЛГЕБРЕ МАТРИЦ 3×3, ИСПОЛЬЗУЮЩИЙ ДВЕ СКРЫТЫЕ ГРУППЫ

Захаров Д. В.[1], Костина А. А.[2], Морозова Е. В.[3], Молдовян Д. Н.[4]

DOI: 10.21681/2311-3456-2025-3-45-54

Цель работы: *повышение производительности алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения больших систем степенных уравнений.*

Метод исследования: *применение алгебры матриц размерности 3×3, заданных над конечным полем GF(p), в качестве алгебраического носителя. Выбор треугольных матриц как элементов простого порядка p. Применение автоморфного отображения некоммутативной конечной алгебры для генерации матриц требуемого порядка, имеющих общий вид.*

Результаты исследования: *впервые в качестве алгебраического носителя алгоритмов ЭЦП, стойкость которых основана на вычислительной сложности решения больших систем степенных уравнений, использована алгебра матриц размерности 3×3. Рандомизация подписи обеспечивается ее вычислением в зависимости от двух случайных элементов, выбираемых из двух скрытых коммутативных групп, элементы одной из которых является некоммутативными с элементами другой. Предложены алгоритмы вычисления генераторов скрытых групп порядков p, $p^2 - 1$ и $p^2 + p + 1$. Впервые при вычислении элементов открытого ключа по элементам секретного ключа в качестве маскирующего множителя использован алгебраический элемент порядка два и показано существование достаточно большого числа нескалярных матриц, обладающих порядком два. Дана оценка стойкости разработанного алгоритма.*

Научная и практическая значимость *результатов статьи состоит в повышении производительности постквантовых алгебраических алгоритмов ЭЦП, основанных на вычислительной трудности решения больших систем степенных уравнений.*

Ключевые слова: *конечная некоммутативная алгебра; ассоциативная алгебра; алгебра матриц, вычислительно трудная задача; скрытая коммутативная группа; цифровая подпись; рандомизация подписи; постквантовая криптография.*

Введение

Разработка постквантовых криптографических алгоритмов с открытым ключом в настоящее время привлекает существенное внимание мирового криптографического сообщества [1, 2]. Криптоалгоритмы, стойкость которых основана на вычислительной трудности решения больших систем степенных уравнений, представляют существенный интерес в качестве постквантовых криптосхем. До последнего времени такие алгоритмы строились на трудно-обратимых нелинейных отображениях с секретной лазейкой [3–5]. Основным недостатком известных алгоритмов данного типа является большой размер открытого ключа (от сотни килобайт до нескольких мегабайт). Даже способ многократного уменьшения размера открытого ключа, предложенный в работах [6-8], не решает в полной мере этой проблемы. Сравнительно недавно [9–11] предложены алгебраические алгоритмы ЭЦП со скрытой группой, использующие вычислительную трудность решения больших систем степенных уравнений. Алгоритмы последнего типа обладают сравнительно малыми размерами подписи и открытого ключа, однако для обеспечения достаточной рандомизации подписи в них используется удвоенное проверочное уравнение, что приводит к снижению производительности процедуры верификации ЭЦП.

В настоящей статье разрабатывается способ усиления рандомизации подписи за счет использования двух скрытых коммутативных групп и вычисления ЭЦП в зависимости от двух случайных взаимно некоммутативных элементов, выбираемых из скрытых групп. На основе предложенного способа реализован алгебраический алгоритм ЭЦП с одним проверочным уравнением, за счет чего достигнуто повышение производительности процедуры верификации ЭЦП. Для повышения стойкости в качестве алгебраического носителя используется конечная алгебра матриц 3×3. Выбор такой размерности связан с сочетанием возможности получения достаточно низкой сложности операции матричного умножения

1 Захаров Дмитрий Викторович, кандидат технических наук, научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук. Санкт-Петербург, Россия. ORCID: https://orcid.org0009-0004-5731-3611. E-mail: zakharov.dmitriy@gmail.com

2 Костина Анна Александровна, научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. ORCID: https://orcid.org/0009-0004-5784-7242. Scopus Author ID: 57218870628. E-mail: to.ann@inbox.ru

3 Морозова Елена Владимировна, кандидат технических наук, доцент кафедры Комплексного обеспечения информационной безопасности. Государственный университет морского и речного флота имени адмирала С. О. Макарова. Санкт-Петербург, Россия. E-mail: lenmor@mail.ru

4 Молдовян Дмитрий Николаевич, кандидат технических наук, доцент кафедры Информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ». Санкт-Петербург, Россия. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 36634567300. E-mail: mdn.spectr@mail.ru

и достаточно высокого коэффициента увеличения числа уравнений при сведении системе векторных степенных уравнений к соответствующей системе скалярных уравнений. Впервые в качестве маскирующего секретного множителя при вычислении элементов открытого ключа используется случайная матрица порядка два, отличная от скалярной матрицы.

Формализация цели исследования

Вычисление подгоночного элемента $\mathbf{S}$ подписи $(e, \mathbf{S})$ в алгебраических алгоритмах ЭЦП со скрытой группой [9], использующих конечную некоммутативную ассоциативную алгебру (КНАА), выполняется по формуле, включающей уникальный элемент $\mathbf{G}$ скрытой группы, вычисляемый в зависимости от рандомизирующего элемента подписи e:

$$\mathbf{S} = \mathbf{DGF}, \quad (1)$$

где $\mathbf{D}$ и $\mathbf{F}$ – секретные маскирующие множители (элементы секретного ключа). Несмотря на уникальность значения $\mathbf{G}$ для каждой подписи $(e, \mathbf{S})$, атака на основе набора известных подписей, позволяющая вычислить секретный элемент $\mathbf{D}$ и некоторый представитель $\mathbf{G}'$ скрытой группы, имеет сравнительно низкую вычислительную сложность, что означает снижение уровня стойкости. Эта уязвимость связана с неполнотой рандомизации подписи, обусловленной ограниченностью выбора элемента $\mathbf{G}$ из скрытой группы, имеющей порядок, намного меньший порядка КНАА.

Усиление рандомизации подписи в алгоритмах [11, 12] обеспечивается за счет того, что вычисление подгоночного элемента подписи $\mathbf{S}$ выполняется по формуле, включающей случайный обратимый элемент $\mathbf{V}$ конечной алгебры, используемой в качестве алгебраического носителя:

$$\mathbf{S} = \mathbf{DGV}. \quad (2)$$

Однако, использование случайного элемента $\mathbf{V}$ при вычислении подгоночного элемента подписи делает невозможным использование уравнения верификации ЭЦП с многократным вхождением значения $\mathbf{S}$, поэтому в алгоритмах [11, 12] используется процедура верификации ЭЦП по двум проверочным уравнениям. Использование такого приема создает предпосылки к подделке подписи с использованием элемента $\mathbf{S}$ в качестве подгоночного параметра атаки.

Для устранения такой потенциальной атаки используются вспомогательные приемы, требующие выполнения дополнительных операций, что приводит к дополнительному снижению производительности алгебраических алгоритмов ЭЦП со скрытой группой. Прием такого типа, предложенный в работе [13], связан с заданием двух скрытых коммутативных групп, элементы одной из которых являются некоммутативными с элементами другой, и использованием вспомогательного параметра рандомизации ρ, вычисляемого как хеш-значение от предварительно вычисленного значения $\mathbf{S}$, и вспомогательного подгоночного элемента подписи в виде натурального числа σ.

В работе [13] также показано, что включение в формулу (2) дополнительного случайного множителя в виде элемента $\mathbf{P}$ из второй скрытой группы вносит самостоятельное существенное усиление рандомизации подписи. При этом формула рандомизации подписи приобретает вид:

$$\mathbf{S} = \mathbf{DPGV} \quad (3)$$

с тремя уникальными (в каждой подписи) множителями $\mathbf{P}$, $\mathbf{G}$ и $\mathbf{V}$. В статье [13] показано, что выбор случайного обратимого элемента из всей КНАА, используемой в качестве алгебраического носителя, не обеспечивает безусловно полной рандомизации, так как следует учесть, что для обеспечения корректности работы алгоритма ЭЦП случайный вектор $\mathbf{V}$ также входит и в формулу для вычисления рандомизирующего вектора $\mathbf{R}$, значение которого восстанавливается в ходе процедуры верификации ЭЦП и позволяет составить по известным подписям систему степенных уравнений с числом неизвестных, меньшим числа уравнений.

В настоящей работе используется следующая формула усиленной (по сравнению с формулой (1)) рандомизации подписи:

$$\mathbf{S} = \mathbf{DPGF}. \quad (4)$$

При этом в процедуре верификации ЭЦП используется только одно проверочное уравнение, но с многократным вхождением подгоночного элемента подписи $\mathbf{S}$. Для обеспечения корректности работы алгоритма ЭЦП с двумя скрытыми коммутативными группами используется вспомогательный подгоночный элемент подписи в виде натурального числа σ.

1. Используемые свойства алгебры матриц 3×3

В качестве алгебраического носителя в разработанном алгоритме ЭЦП используется конечная алгебра матриц 3×3, заданная над простым конечным полем $GF(p)$. Такой носитель можно трактовать как девятимерная КНАА, заданная по таблице умножения базисных векторов (ТУБВ), представленной в виде табл. 1. В m-мерной КНАА векторы можно представить в виде упорядоченного набора координат $\mathbf{A} = (a_1, a_2, \ldots, a_m)$ и в виде суммы его компонент $\mathrm{A} = \sum_{i=1}^{m} a_i\, e_i$, где e_i – базисные векторы. Умножение двух векторов $\mathbf{A}$ и $\mathbf{B} = \sum_{j=1}^{m} b_j\, e_j$ обычно определяется как перемножение каждой компоненты $\mathbf{A}$ с каждой компонентой $\mathbf{B}$, а именно, по следующей формуле:

$$\mathbf{AB} = \sum_{i=1}^{m} \sum_{j=1}^{m} a_i\, b_j\, (e_i\, e_j), \quad (5)$$

в которой каждое из всех произведений пар базисных векторов вида $\mathbf{e}_i\mathbf{e}_j$ подлежит замене на некоторый однокомпонентный вектор вида $\lambda\mathbf{e}_k$ (в общем случае – на многокомпонентный вектор) в соответствии с некоторой ТУББ. Значение $\lambda \neq 1$ называется структурной константой. При этом левый множитель в произведении $\mathbf{e}_i\mathbf{e}_j$ указывает строку, а правый – столбец, пересечение которых выделяет ячейку, содержащую значение $\lambda\mathbf{e}_k$. При наличии многих ячеек, содержащих структурную константу, равную нулю, ТУББ называется прореженной. Далее матрицы будем обозначать жирными латинскими буквами.

Таблица 1 относится к прореженным ТУББ, обеспечивающим сравнительно низкую вычислительную сложность операции умножения векторов. Прореженные ТУББ известны для случая четырехмерных КНАА и используются в алгоритмах ЭЦП, предложенных в работах [12, 13]. Интерес к использованию четырехмерных КНАА, заданных над $GF(p)$, также обусловливается тем, что для них (в том числе для алгебры матриц 2×2) детально исследована декомпозиция на коммутативные подалгебры порядка p^2 [14, 15]. Знание строения КНАА имеет значение как для синтеза алгебраических алгоритмов ЭЦП, так и для анализа их стойкости к различным видам атак.

В общем случае изучение декомпозиции (на коммутативные подалгебры) КНАА размерности шесть и более представляет собой нетривиальную задачу. В случае алгебр матриц 3×3 частные детали строения, важные для разработки алгебраических алгоритмов ЭЦП, могут быть установлены. Рассмотрим некоторые из таких деталей, поясняющих выбор матриц в качестве элементов секретного ключа. В случае конечных групп невырожденных матриц $\mathbf{M}$ размерности $m \times m$, заданных над полем $GF(p)$, их порядок $\boldsymbol{\Omega}$ описывается следующей формулой[5]:

$$\boldsymbol{\Omega} = \prod_{i=0}^{m-1} p^i (p^{m-i} - 1). \quad (6)$$

В соответствии с теоремой Силова наличие простого делителя q порядка конечной некоммутативной группы показывает наличие элементов порядка q, содержащихся в таких группах. Такие элементы генерируют коммутативные группы, содержащиеся в алгебре матриц. Для случая размерности $m = 3$ порядок мультипликативной группы алгебры матриц равен

$$\boldsymbol{\Omega}_{3\times 3} = p^3(p-1)^3(p^2+p+1)(p+1). \quad (7)$$

Из формулы (7) видим, что существуют матрицы простого порядка p, причем для заданного значения битовой длины простое значение p может быть выбрано таким, что число $q = p^2 + p + 1$ также является простым. Примеры таких случаев представлены в табл. 2. Матрица порядка q генерирует коммутативную группу, включающую $q - 1$ нескалярных матриц. Учитывая наличие в некоммутативных группах автоморфного отображения вида

$$\mathbf{Y} = \mathbf{AQA}^{-1}, \quad (8)$$

где $\mathbf{A}$ – обратимая (невырожденная) матрица и $\mathbf{Q}$ – матрица порядка q, можно сделать заключение о достаточном числе различных циклических групп порядка q.

Утверждение 1. Пусть дано разрешимое уравнение $\mathbf{A} = \mathbf{XBX}^{-1}$ с неизвестной матрицей $\mathbf{X}$ при фиксированных нескалярных невырожденных матрицах $\mathbf{A}$ и $\mathbf{B} \neq \mathbf{A}$. Тогда данное уравнение имеет количество

5 Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. – М.: Физматлит, 1996. – 287 с.

Таблица 1.

Таблица умножения базисных векторов при трактовке матриц $||a_{ij}||$ размерности 3×3 как девятимерных векторов $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) = (a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33})$

.	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	0	0	0	0	0	0
$\mathbf{e}_1$	0	0	0	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	0	0	0
$\mathbf{e}_2$	0	0	0	0	0	0	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	0	0	0	0	0	0
$\mathbf{e}_4$	0	0	0	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	0	0	0
$\mathbf{e}_5$	0	0	0	0	0	0	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_6$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	0	0	0	0	0	0
$\mathbf{e}_7$	0	0	0	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$	0	0	0
$\mathbf{e}_8$	0	0	0	0	0	0	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_8$

Таблица 2.

ТПростые значения $q = p^2 + p + 1$ при небольших простых p

p	3	5	37	59	71	89	101	131
q	13	31	1723	3541	5113	8011	10303	17293

решений, равное числу всех матриц коммутативных с матрицей $\mathbf{B}$, включая саму матрицу $\mathbf{B}$.

Доказательство. Разрешимость матричного уравнения $\mathbf{A} = \mathbf{XBX}^{-1}$ означает существование некоторого решения $\mathbf{X}_0$. Каждый обратимый вектор $\mathbf{V}$, коммутативный с $\mathbf{B}$, задает уникальное решение $\mathbf{X} = \mathbf{X}_0\mathbf{V}$. Действительно, имеем

$$(\mathbf{X}_0\mathbf{V})\mathbf{B}(\mathbf{X}_0\mathbf{V})^{-1} = \mathbf{X}_0\mathbf{VBV}^{-1}\mathbf{X}_0^{-1} = \\ = \mathbf{X}_0\mathbf{BVV}^{-1}\mathbf{X}_0^{-1} = \mathbf{X}_0\mathbf{BX}_0^{-1} = \mathbf{A}.$$

Таким образом, имеем столько уникальных решений, сколько имеется невырожденных матриц, коммутативных с $\mathbf{B}$. Покажем, что других решений нет. Пусть имеется решение $\mathbf{X}_i$. Тогда имеем:

$$\{\mathbf{X}_i\mathbf{BX}_i^{-1} = \mathbf{X}_0\mathbf{BX}_0^{-1}\} \Rightarrow \{(\mathbf{X}_0^{-1}\mathbf{X}_i)\mathbf{B} = \mathbf{B}(\mathbf{X}_0^{-1}\mathbf{X}_i); \\ \mathbf{X}_i = \mathbf{X}_0(\mathbf{X}_0^{-1}\mathbf{X}_i)\}.$$

Последние два равенства показывают, что любое решение $\mathbf{X}_i$ представимо в виде произведения решения $\mathbf{X}_0$ на вектор $(\mathbf{X}_0^{-1}\mathbf{X}_i)$, который коммутативен с $\mathbf{B}$.

С учетом того, что матрица $\mathbf{Q}$, имеющая порядок q, является нескалярной матрицей, а значит базис <$\mathbf{Q}$, $\mathbf{L}$>, где $\mathbf{L}$ – скалярная матрица порядка $p - 1$, генерирует коммутативную группу порядка $(p^2 + p + 1)(p - 1)$, причем вне этой группы нет векторов, перестановочных с $\mathbf{Q}$, легко видеть, что имеется $(p^2 + p + 1)(p - 1)$ различных матриц $\mathbf{A}$, задающих один и тот же автоморфный образ циклической группы, генерируемой матрицей $\mathbf{Q}$. При подстановке всех невырожденных матриц 3×3 в формулу (8) в качестве матрицы $\mathbf{A}$ получаем η_q' различных матриц $\mathbf{Y}$. Для значения η_q имеем следующую формулу:

$$\eta_q' = p^3(p - 1)^2(p + 1). \qquad (9)$$

Доля матриц $\mathbf{Y}$ попадающих в одну и ту же коммутативную группу порядка $p^3 - 1$ является достаточно малой, поэтому количество различных коммутативных групп порядка $p^3 - 1$ (а значит и коммутативных групп порядка q) можно оценить значением $\eta_q' \approx \eta_q \approx p^6$. Рассмотрение числа η_p различных циклических групп порядка p также приводит к оценке $\eta_p \approx p^6$. При предполагаемом для использования 80-битном размере простого числа p доля матриц, входящих в циклические группы порядков p и q, достаточно велика, чтобы алгоритм генерации матриц простых порядков p и q, основанный на выборе случайных матриц, имел достаточную вычислительную эффективность.

Алгоритм генерации матрицы $\mathbf{Q}$ простого порядка $q = p^2 + p + 1$, например, может включать следующие шаги:

1. Сгенерировать случайную невырожденную матрицу $\mathbf{M}$ общего вида.
2. Вычислить значение $z = \Omega_{3\times3}(p^2 + p + 1)^{-1} = p^3(p - 1)^3(p + 1)$.
3. Вычислить матрицу $\mathbf{Q} = \mathbf{M}^z$ и проверить выполнимость неравенства $\mathbf{Q} \neq \mathbf{E}$. Если $\mathbf{Q} = \mathbf{E}$, то перейти к шагу 1.
4. Вывести матрицу $\mathbf{Q}$ как матрицу простого порядка $q = p^2 + p + 1$.

Для генерации матриц порядка p можно предложить алгоритм с более высокой вычислительной эффективностью, который основан на следующем утверждении.

Утверждение 2[6]. Невырожденные треугольные матрицы размерности 3×3 над конечным полем $GF(p)$ имеют простое значение порядка, равное p.

Доказательство. Возведение верхне-треугольной матрицы в квадрат дает следующее:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & a+a & b+ac+b \\ 0 & 1 & c+c \\ 0 & 0 & 1 \end{pmatrix} = \\ = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}. \qquad (10)$$

Допустим, что для произвольного целого $k \geq 2$ имеет место формула

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & ka & kb + \frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix}. \qquad (11)$$

Тогда возведение рассматриваемой матрицы в степень $k + 1$ дает

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{k+1} = \begin{pmatrix} 1 & ka & kb + \frac{k(k-1)}{2}ac \\ 0 & 1 & kc \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} =$$

6 Горячев А.А., Молдовян Д.Н., Куприянов И.А. Выбор параметров задачи скрытого дискретного логарифмирования для синтеза криптосхем // Вопросы защиты информации. 2011. 1. С. 19–23.

$$= \begin{pmatrix} 1 & a+ka & b+kac+kb+\frac{k(k-1)}{2}ac \\ 0 & 1 & c+kc \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & (1+k)a & (1+k)b+\frac{k(k+1)}{2}ac \\ 0 & 1 & (1+k)c \\ 0 & 0 & 1 \end{pmatrix}. \quad (12)$$

Формула (10) получается из (11) при подстановке значения степени $k = 2$. В соответствии с методом математической индукции делаем вывод, что формула (11) верна при произвольных натуральных степенях k. При $k = p$ получаем единичную матрицу, т.е. порядок рассматриваемой треугольной матрицы равен p. Аналогичным путем получаем следующую формулу для произвольной нижне-треугольной матрицы:

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & 0 & 0 \\ ka & 1 & 0 \\ kb+\frac{k(k-1)}{2}ac & kc & 1 \end{pmatrix}. \quad (13)$$

При $k = p$ правая часть формул (11) и (13) равна единичной матрице, что требовалось доказать.

Алгоритм генерации матрицы $\mathbf{P}$ порядка p включает следующие шаги:

1. Сгенерировать случайную треугольную матрицу $\mathbf{T}$ и случайную невырожденную матрицу $\mathbf{M}$ общего вида.
2. Вычислить матрицу $\mathbf{P}$ по формуле $\mathbf{P} = \mathbf{MTM}^{-1}$.

Для разработки алгоритмов ЭЦП со скрытой группой также представляет интерес использование матриц порядка $p - 1$. Для оценки доли таких матриц, содержащихся в мультипликативной группе алгебры матриц 3×3, интерес представляет следующее утверждение.

Утверждение 3. Множество невырожденных диагональных матриц размерности 3×3, заданных над конечным полем $GF(p)$, образуют коммутативную группу порядка $(p - 1)^3$.

Доказательство. Умножение двух произвольных матриц $(a_{11}, 0, 0, 0, a_{22}, 0, 0, 0, a_{33})$ и $(b_{11}, 0, 0, 0, b_{22}, 0, 0, 0, b_{33})$, где $0 < a_{11}, a_{22}, a_{33}, b_{11}, b_{22}, b_{33} < p$, по правилам матричного умножения дает в качестве результата матрицу $(a_{11}b_{11}, 0, 0, 0, a_{22}b_{22}, 0, 0, 0, a_{33}b_{33})$, т.е. все рассматриваемые матрицы коммутативны между собой и имеет место следующее тождество:

$$(a,0,0,0,b,0,0,0,c)^{p-1} = (a^{p-1},0,0,0,b^{p-1},0,0,0,c^{p-1}) = (1, 0, 0, 0, 1, 0, 0, 0, 1). \quad (14)$$

Из формулы (14) следует, что все матрицы диагонального вида имеют порядок, равный делителю числа $p - 1$, включая само это число. Легко видеть, что число таких матриц (порядок группы, который они образуют) равно $(p - 1)^3$. Естественным базисом коммутативной группы таких матриц является $<\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3>$, где $\mathbf{B}_1 = (\alpha, 0, 0, 0, 1, 0, 0, 0, 1)$; $\mathbf{B}_2 = (1, 0, 0, 0, \beta, 0, 0, 0, 1)$; $\mathbf{B}_3 = (1, 0, 0, 0, 1, 0, 0, 0, \delta)$; α, β и δ – примитивные элементы по модулю p. Будем обозначать коммутативные группы, порождаемые базисом из трех матриц порядка $p - 1$ как Γ_3. Учитывая автоморфизм, задаваемый формулой (8), легко видеть, что наличие группы диагональных матриц, относящихся к типу Γ_3, означает существование большого числа изоморфных Γ_3-групп, содержащих матрицы произвольно вида.

В соответствии с утверждением 1 разрешимое матричное уравнение

$$\mathbf{A} = \mathbf{XBX}^{-1}, \quad (15)$$

записанное для нескалярной матрицы $\mathbf{B}$, входящей в Γ_3-группу диагональных матриц имеет число различных решений, равное числу матриц, коммутативных с диагональной матицей $\mathbf{B}$. Число последних равно числу различных решений матричного уравнения

$$\mathbf{ZB} = \mathbf{BZ}. \quad (16)$$

Рассматривая систему из девяти линейных уравнений с девятью неизвестными координатами вектора $\mathbf{Z}$, к которой сводится последнее векторное уравнение, легко установить, что ранг главного определителя этой системы линейных уравнений равен шести, а значит, она имеет p^3 различных решений. Каждое из решений задает некоторую матрицу, вырожденную или невырожденную.

Легко подсчитать число вырожденных диагональных матриц (коммутативных с матрицей $\mathbf{B}$), которое оказывается равным $3p^2 - 3p + 1$. Суммируя вырожденные и невырожденные диагональные матрицы, получаем все p^3 решений матричного уравнения (16). Таким образом, все невырожденные решения уравнений (16) входят в рассматриваемую Γ_3-группу диагональных матриц. Последнее означает, что матричное уравнение (15) имеет $(p - 1)^3$ различных решений. Если в уравнении (15) при фиксированном значении матрицы $\mathbf{B}$ переменная $\mathbf{X}$ пробегает значения всех невырожденных матриц в мультипликативной группе алгебры матриц 3×3, то получим число различных матриц A, равное

$$\eta_3 = \Omega_{3\times3}(p - 1)^3 = p^3(p^2 + p + 1)(p + 1). \quad (17)$$

В общем случае некоторые пары различных матриц могут принадлежать одной и той же Γ_3-группе, поэтому число различных Γ_3-групп, содержащихся в мультипликативной группе рассматриваемой алгебры матриц, меньше значения η_3. Вывод формулы для числа различных Γ_3-групп представляется интересной и важной самостоятельной задачей, однако

в настоящем исследовании достаточен вывод что это число достаточно велико.

Легко показать, что каждая из изоморфных Γ_3-групп разбивается на большое число различных коммутативных циклических подгрупп порядка $p-1$ (число таких подгрупп равно примерно p^2), пересекающихся в единичной матрице $\mathbf{E}$ и семи различных матрицах $\mathbf{W}$ порядка два. Матрицы $\mathbf{W}$ порядка два могут трактоваться как квадратные корни из единичной матрицы $\mathbf{E} = (1, 0, 0, 0, 1, 0, 0, 0, 1)$. Все Γ_3-группы попарно пересекаются в циклической группе скалярных матриц, содержащей матрицу $\mathbf{W} = -\mathbf{E}$. В заданной Γ_3-группе число уникальных (по всей алгебре матриц 3×3) матриц $\mathbf{W}$ равно всего лишь шести, однако число Γ_3-групп велико, порядка p^6, т.е. число уникальных матриц $\mathbf{W}$ достаточно велико для того, чтобы они могли быть эффективно использованы как элемент секретного ключа. Следует заметить, что в рассматриваемой алгебре матриц содержатся и другие уникальные корни из $\mathbf{E}$, например, содержащиеся в циклических группах, генерируемых матрицами порядка $p+1$. Если известна нескалярная матрица $\mathbf{V}$ порядка $p-1$, то некоторую уникальную матрицу $\mathbf{W}$ порядка два можно вычислить по следующей формуле:

$$\mathbf{W} = \mathbf{V}^{(p-1)/2}. \quad (18)$$

В алгоритме ЭЦП, описываемом в следующем разделе, используются случайные нескалярные матрицы порядка p^2-1 и случайные матрицы $\mathbf{W} \neq -\mathbf{E}$. Для генерации таких матриц могут быть использованы следующие вычислительно эффективные алгоритмы.

Алгоритм генерации нескалярной матрицы $\mathbf{V}$ *порядка* $p-1$:

1. Сгенерировать случайные натуральные числа $b < p$ и $c < p$ и случайный примитивный элемент α по модулю p.
2. Сформировать диагональную матрицу $\mathbf{M} = (\alpha, 0, 0, 0, b, 0, 0, 0, c)$. порядка $p-1$.
3. Сгенерировать случайную невырожденную матрицу $\mathbf{X}$ и вычислить матрицу $\mathbf{V}$: $\mathbf{V} = \mathbf{X}\mathbf{M}\mathbf{X}^{-1}$.

Алгоритм генерации случайной матрицы $\mathbf{W}$ *порядка 2*:

1. Сгенерировать случайную нескалярную матрицу $\mathbf{V}$ порядка $p-1$.
2. Вычислить матрицу $\mathbf{W} = \mathbf{V}^{(p-1)/2}$.

Алгоритм генерации нескалярной матрицы $\mathbf{G}$ *порядка* p^2-1:

1. Сгенерировать случайную невырожденную матрицу $\mathbf{M}$ общего вида.
2. Вычислить значение $h = \Omega_{3\times3}(p^2-1)^{-1} = p^3(p-1)^2(p^2+p+1)$ и матрицу $\mathbf{X} = \mathbf{M}^h$.
3. Если $\mathbf{X} = \mathbf{E}$, то перейти к шагу 1.
4. Если для всех простых делителей δ числа p^2-1 выполняется неравенство $\mathbf{X}^{(p^2-1)/\delta} \neq \mathbf{E}$, то перейти к шагу 5, иначе перейти к шагу 1.
5. Взять матрицу $\mathbf{X}$ в качестве матрицы $\mathbf{G}$ порядка p^2-1.

Из последних трех алгоритмов существенно более высокую вычислительную сложность имеет последний алгоритм, поскольку в нем среднее число возвратов к шагу 1 составляет несколько десятков. Однако, для применения в процедуре формирования секретного и открытого ключа его производительность вполне достаточна.

3. Постквантовый алгебраический алгоритм на алгебре матриц 3×3

В разработанном алгоритме ЭЦП в качестве алгебраического носителя используется алгебра матриц 3×3, заданная над полем $GF(p)$ простого 80-битного порядка p, такого, что число $q = p^2+p+1$ является простым. Секретный ключ формируется путем генерации случайных натуральных чисел $w < q$, $x < q$, $y < q$ и $z < q$, случайной матрицы $\mathbf{W}$, такой, что $\mathbf{W}^2 = \mathbf{E}$, и случайных невырожденных нескалярных и попарно некоммутативных матриц $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{G}$, $\mathbf{K}$ и $\mathbf{P}$, причем таких, что матрицы $\mathbf{G}$ и $\mathbf{P}$ имеют порядок равный $q = p^2+p+1$ и p^2-1 соответственно (общий размер секретного ключа равен ≈710 байт). Формирование открытого ключа выполняется в соответствии со следующими формулами:

$$\mathbf{Y} = \mathbf{WGW}; \mathbf{Z} = \mathbf{KP}^z\mathbf{K}^{-1}; \mathbf{U} = \mathbf{BPB}^{-1}; \mathbf{T}_1 = \mathbf{WG}^x\mathbf{D}^{-1}; \quad (19)$$

$$\mathbf{T}_2 = \mathbf{F}^{-1}\mathbf{P}^w\mathbf{K}^{-1}; \mathbf{T}_3 = \mathbf{KP}^y\mathbf{G}^w\mathbf{W}; \mathbf{T}_4 = \mathbf{F}^{-1}\mathbf{P}^x\mathbf{B}^{-1}. \quad (20)$$

Общий размер открытого ключа равен ≈630 байт. В процедурах генерации и верификации ЭЦП предполагается использование некоторой специфицированной коллизионно стойкой 480-битной хеш-функции Φ, которая является частью рассматриваемого алгоритма ЭЦП.

Алгоритм генерации ЭЦП.

Процедура генерации ЭЦП к документу M включает следующие шаги:

1. Сгенерировать случайные натуральные числа $k < q$ и $t < p+1$ и вычислить значение матрицы $\mathbf{R}$ по формуле: $\mathbf{R} = \mathbf{WG}^k\mathbf{P}^t\mathbf{B}^{-1}$.
2. Вычислить хеш-значение от документа M с присоединенной к нему матрицей $\mathbf{R}$: $e = e_1||e_2||e_3 = \Phi(M, \mathbf{R})$, где 480-битное хеш-значение e представлено в виде конкатенации трех 160-битных натуральных чисел e_1, e_2 и e_3.
3. Вычислить натуральное число b: $b = -(w + ze_2 + y) \bmod (p^2-1)$.
4. Вычислить натуральное число n: $n = (k - x - e_2e_3 - we_3 - xe_3 - e_1e_3)(e_3+1)^{-1} \bmod q$.
5. Вычислить подгоночный элемент ЭЦП в виде матрицы $\mathbf{S}$ по формуле: $\mathbf{S} = \mathbf{DP}^b\mathbf{G}^n\mathbf{F}$.

6. Вычислить вспомогательный подгоночный элемент подписи в виде числа σ: $\sigma = (t - b - x) \bmod (p^2 - 1)$.

Сгенерированная цифровая подпись представляет собой тройку значений $(e, \sigma, \mathbf{S})$ с общим размером ≈170 байт. Вычислительная сложность процедуры генерации ЭЦП главным образом определяется четырьмя операциями возведения в 160-битную степень в алгебре матриц (вычисление матриц $\mathbf{P}^t$, $\mathbf{G}^k$, $\mathbf{P}^b$ и $\mathbf{G}^n$), что составляет ≈26000 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП.

Проверка подлинности 170-байтной подписи $(e, \sigma, \mathbf{S})$ к документу M осуществляется с использованием 630-байтного открытого ключа $(\mathbf{Y}, \mathbf{Z}, \mathbf{U}, \mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3, \mathbf{T}_4)$ по следующему алгоритму:

1. Вычислить матрицу $\mathbf{R}'$ по следующей формуле (проверочное уравнение):
$$\mathbf{R}' = (\mathbf{Y}^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{T}_2\mathbf{Z}^{e_2}\mathbf{T}_3\mathbf{Y}^{e_2})^{e_3}\mathbf{T}_1\mathbf{S}\mathbf{T}_4\mathbf{U}^{\sigma}. \quad (21)$$
2. Вычислить значение хеш-функции Φ от документа M с присоединенной к нему матрицей $\mathbf{R}'$: $\varepsilon = \varepsilon_1||\varepsilon_2||\varepsilon_3 = \Phi(M, \mathbf{R}')$, где 480-битное хеш-значение представлено в виде конкатенации трех 160-битных чисел ε_1, ε_2 и ε_3.
3. Если одновременно выполняются равенства $\varepsilon_1 = e_1$, $\varepsilon_2 = e_2$ и $\varepsilon_3 = e_3$, то ЭЦП принимается как подлинная, в противном случае она отвергается как ложная.

Вычислительную сложность процедуры верификации ЭЦП можно оценить как пять операций возведения матриц в 160-битную степень, что составляет ≈33000 операций умножения в поле $GF(p)$. Корректность этого алгоритма ЭЦП доказывается подстановкой в проверочное уравнение (21) элементов открытого ключа, выраженных через элементы секретного ключа, указанным ниже образом.

Доказательство корректности алгоритма ЭЦП.

Подставляя в проверочное уравнение (21) элементы открытого ключа, выраженные через элементы секретного ключа по формулам (19) и (20), для корректно сгенерированной подписи получаем:

$$\mathbf{R}' = (\mathbf{Y}^{e_1}\mathbf{T}_1\mathbf{S}\mathbf{T}_2\,\mathbf{Z}^{e_2}\mathbf{T}\mathbf{Y}^{e_2})^{e_3}\mathbf{T}_1\mathbf{S}\mathbf{T}_4\mathbf{U}^{\sigma} =$$
$$= [(\mathbf{WGW})^{e_1}\mathbf{WG}^x\mathbf{D}^{-1}(\mathbf{DG}^n\mathbf{P}^b\mathbf{F})\mathbf{F}^{-1}\mathbf{P}^w\mathbf{K}^{-1} \times$$
$$\times (\mathbf{KP}^z\mathbf{K}^{-1})^{e_2}\mathbf{K}\,\mathbf{P}^y\mathbf{G}^w\mathbf{W}(\mathbf{WGW})^{e_2}]^{e_3}\mathbf{WG}^x\mathbf{D}^{-1} \times$$
$$\times (\mathbf{DG}^n\mathbf{P}^b\mathbf{F})\mathbf{F}^{-1}\mathbf{P}^x\,\mathbf{B}^{-1}(\mathbf{BPB}^{-1})^{\sigma} =$$
$$= (\mathbf{WG}^{e_1+x+n}\mathbf{P}^{b+w+ze_2+y}\mathbf{G}^{w+e_2}\mathbf{W})^{e_3}\mathbf{WG}^{x+n}\mathbf{P}^{b+x+\sigma}\mathbf{B}^{-1} =$$
$$= (\mathbf{WG}^{e_1+x+n}\mathbf{P}^{0}\mathbf{G}^{w+e_2}\mathbf{W})^{e_3}\mathbf{WG}^{x+n}\mathbf{P}^{b+x+(t-b-x)}\mathbf{B}^{-1} =$$
$$= (\mathbf{WG}^{e_1+x+n+w+e_2}\mathbf{W})^{e_3}\mathbf{WG}^{x+n}\mathbf{P}^{t}\mathbf{B}^{-1} =$$
$$= \mathbf{WG}^{e_1e_3+xe_3+ne_3+we_3+e_2e_3+x+n}\mathbf{P}^{t}\mathbf{B}^{-1} =$$
$$= \mathbf{WG}^{n(e_3+1)+e_1e_3+xe_3+we_3+e_2e_3+x}\mathbf{P}^{t}\mathbf{B}^{-1} = \mathbf{WG}^{k}\mathbf{P}^{t}\mathbf{B}^{-1} = \mathbf{R}.$$

С учетом равенства $\mathbf{R} = \mathbf{R}'$ имеем $\varepsilon_1||\varepsilon_2||\varepsilon_3 = \Phi(M, \mathbf{R}') = \Phi(M, \mathbf{R}) = e_1||e_2||e_3$, т. е. корректно сгенерированная подпись проходит процедуру верификации как подлинная подпись, что означает корректность разработанного алгоритма ЭЦП.

4. Обсуждение

Представляет интерес реализация предложенного алгоритма с использованием в качестве секретной матрицы $\mathbf{G}$, имеющей порядок $p(p - 1)$. В такой версии алгоритма процедура верификации ЭЦП остается без изменения, а в процедуре генерации ЭЦП вычисление на шагах 3 и 6 будет выполняться по тем же формулам, но по модулю $p(p - 1)$ (вместо модуля $p^2 - 1$). Такое модифицирование алгоритма не влияет на его стойкость, однако несколько снижает вычислительную сложность процедуры формирования секретного ключа за счет возможности использования существенно более производительного алгоритма генерации матриц порядка $p(p - 1)$ по сравнению с алгоритмом генерации матриц порядка $p^2 - 1$.

Оценка стойкости разработанного алгоритма к атакам на основе известных подписей по способу, использованному в работах [13, 16], показала, что такие атаки связаны с решением системы матричных степенных уравнений, записанных по формуле формирования подгоночного элемента для десяти известных подписей. Это соответствует решению системы из 90 степенных скалярных уравнений в поле $GF(p)$.

Прямая атака на разработанный алгоритм связана с решением системы степенных матричных уравнений, связывающих элементы секретного ключа с элементами открытого ключа в соответствии с формулами (19) и (20). В такой системе матричных уравнений матрицы $\mathbf{G}^w$, $\mathbf{G}^x$, $\mathbf{P}^w$, $\mathbf{P}^x$, $\mathbf{P}^y$ и $\mathbf{P}^z$ рассматриваются как независимые неизвестные (в противном случае пришлось бы иметь дело с экспоненциальными матричными уравнениями), принадлежащие соответствующим скрытым группам. При этом матричные уравнения, выражающие условие коммутативности неизвестных, принадлежащих одной и той же скрытой группе, могут быть устранены при сведении решения системы матричных уравнений к соответствующей системе скалярных уравнений при наличии формул, выражающих все координаты векторов скрытой группы через координаты фиксированного представителя скрытой группы и три скалярных неизвестных.

Потенциально такие формулы могут быть выведены из рассмотрения декомпозиции алгебры матриц 3×3 на коммутативные подалгебры по аналогии с декомпозицией алгебры матриц 2×2 [15]. Вывод таких

Таблица 3.

Сравнение предложенного постквантового алгоритма ЭЦП с известными аналогами

Алгоритм и размер порядка поля *GF(p)*	Размер открытого ключа, байт	Размер подписи, байт	Сложность генерации подписи, умножений в *GF(p)*	Сложность верификации подписи, умножений в *GF(p)*	Уровень стойкости к прямой атаке
Предложенный, 80 бит	630	170	26000	33000	$\approx 2^{192}$
[16], 128 бит	512	144	9200	13800	$\approx 2^{100}$
[18] , 128 бит	387	97	12300	6100	$\approx 2^{100}$
[19] , 128 бит	256	113	12300	9220	$\approx 2^{80}$
[20], 128 бит	768	160	49200	13800	$\approx 2^{80}$

формул составляет самостоятельную задачу, однако такую потенциальную возможность следует учитывать при оценке стойкости к прямой атаке. С учетом такой возможности прямая атака оказывается связанной с решением системы из 63 степенных уравнений в поле $GF(p)$ 80-битного порядка p. При этом в систему входят 69 скалярных неизвестных. Оценка сложности решения такой системы в зависимости от числа степенных уравнений в системе, приводимая в работе [4], задает для разработанного алгоритма ЭЦП уровень стойкости $\approx 2^{192}$ к прямой атаке и $\approx 2^{256}$ к атаке на основе известных подписей. Заметим, что разработанный алгоритм ЭЦП с проверочным уравнением (21) может быть реализован на конечных некоммутативных ассоциативных алгебрах различных размерностей, например, заданных по методу [17].

Сравнение некоторых параметров разработанного алгебраического алгоритма ЭЦП с аналогами из статей [16, 18–20], использующими четырехмерные некоммутативные алгебры в качестве алгебраического носителя, приведено в табл. 3.

Выводы

Используя конечную алгебру матриц размерности 3×3, заданных над простым полем $GF(p)$, в качестве алгебраического носителя, разработан алгоритм ЭЦП с двумя скрытыми группами, стойкость которого основана на вычислительной трудности решения больших систем степенных уравнений. Алгоритм представляет интерес как потенциальный прототип для разработки практичного постквантового стандарта ЭЦП

Представляет интерес применение описанного построения схемы ЭЦП для реализации аналогичного алгоритма на алгебре матриц, заданных над конечным полем характеристики два. Важной задачей будущих исследований в затронутом направлении является исследование декомпозиции алгебры матриц 3×3 на коммутативные подалгебры. Также представляет интерес рассмотрение реализации аналога разработанного алгоритма с использованием в качестве алгебраического носителя алгебры матриц 5×5, заданных над конечным полем 32-битного порядка p.

Исследование выполнено частично за счет гранта Российского научного фонда № 24-41-04006, https://rscf.ru/project/24-41-04006/

Литература

1. Post-Quantum Cryptography. 15th International Conference, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings // Lecture Notes in Computer Science. 2024. V. 14771–14772. Springer, Cham.
2. Post-Quantum Cryptography. 14th International Conference, PQCrypto 2023, College Park, MD, USA, August 16–18, 2023, Proceedings // Lecture Notes in Computer Science. 2023. V. 14154. Springer, Cham.
3. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2022. P. 1–17. DOI: 10.1049/ise2.12092.
4. Ding J.,Petzoldt A.. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. Vol. 15. No. 4. P. 28–36.
5. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 7–23. DOI: 10.1007/978-1-0716-0987-3_2.
6. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. No. 3 (103). P. 80–89. DOI: https://doi.org/10.56415/basm.y2023.i3.p80.

7. Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. V.32. N. 1(94). P. 46–60. DOI: 10.56415/csjm.v32.04.
8. Moldovyan A.A. , Moldovyan N.A. Parameterized unified method for setting vector finite fields for multivariate cryptography // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2024. Т. 20. Вып. 4. С. 479–486. DOI: 10.21638/spbu10.2024.404.
9. Moldovyan A.A., Moldovyan D.N. A New Method for Developing Signature Algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics, 2022. No. 1(98). P. 56–65. DOI: 10.56415/basm.y2022.i1.p56.
10. Moldovyan N.A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022, vol. 30, no. 2(48), pp. 287–298. DOI: 10.56415/qrs.v30.24.
11. Moldovyan A.A. Complete signature randomization in an algebraic cryptoscheme with a hidden group // Quasigroups and related systems. 2024. Vol. 32. No. 1. P. 95–108. DOI: 10.56415/qrs.v32.08.
12. Молдовян А.А., Молдовян Д.Н., Костина А.А. Алгебраические алгоритмы ЭЦП с полной рандомизацией подписи // Вопросы кибербезопасности. 2024. № 2(60). С. 95–102. DOI: 10.21681/2311-3456-2024-2-95-102.
13. Молдовян Д.Н., Костина А.А. Способ усиления рандомизации подписи в алгоритмах ЭЦП на некоммутативных алгебрах // Вопросы кибербезопасности. 2024. № 4(62). С. 71–81. DOI: 10.21681/2311-3456-2024-4-71-81.
14. Moldovyan D.N., Moldovyan A.A., Moldovyan N.A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022, vol. 30, no. 1, pp. 133–140. DOI: 10.56415/qrs.v30.11.
15. Moldovyan N.A., Moldovyan A.A. Digital signature scheme on the 2x2 matrix algebra algebra // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т., 17 Вып. 3. С. 254–261. DOI: 10.21638/11701/spbu10.2021.303.
16. Молдовян Н.А, Петренко А.С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2024. № 6(64). С. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
17. Dinh K.L., Nguyen L.G, Do T.B., Moldovyan A.A., Moldovyan D.N., Kostina A.A. Defining High-Dimensional Non-Commutative Algebras as Carriers for Post-Quantum Digital Signature Algorithms // Proceedings of the 1st International Conference On Cryptography and Information Security (VCRIS), Hanoi, Vietnam, 2024. P. 1–5. DOI: 10.1109/VCRIS63677.2024.10813386.
18. Duong M.T., Moldovyan D.N., Do B.V., Minh Hieu Nguyen M.H. Post-quantum signature algorithms on noncommutative algebras, using difficulty of solving systems of quadratic equations // Computer Standards and Interfaces. 2023. Vol. 86. P. 103740. DOI: 10.1016/j.csi.2023.103740. ISSN 0920-5489.
19. Молдовян Д.Н., Молдовян А.А. Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2(48). С. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
20. Moldovyan D.N. A new type of digital signature algorithms with a hidden group // Computer Science Journal of Moldova. 2023, vol. .31, No. 1(91), pp. 111–124. DOI: 10.56415/csjm.v31.06.

A DIGITAL SIGNATURE ALGORITHM ON THE ALGEBRA OF 3×3 MATRICES, WHICH USES TWO HIDDEN GROUPS

Zakharov D. V.[7], Kostina A. A.[8], Morozova E. V.[9], Moldovyan D. N.[10]

Keywords: *finite non-commutative algebra; associative algebra; matrix algebra; computationally difficult problem; hidden group; digital signature; signature randomization; post-quantum cryptography.*

Purpose of work *is increasing the performance of algebraic digital signature algorithms based on the computational difficulty of solving large systems of power equations.*

Research methods: *application of the algebra of matrices of dimension 3×3 defined over a finite field GF(p) as an algebraic support. Selection of triangular matrices as the algebra elements of prime order p. Application of an automorphic mapping of a non-commutative finite algebra to generate the required-order matrices having a general form.*

Results of the study: *for the first time, the algebra of matrices of dimension 3×3 was used as an algebraic carrier of diital sinature algorithms, the security of which is based on the computational complexity of solving large systems of power equations. The randomization of the signature is provided by calculating it depending on two random elements selected from two hidden commutative groups, the elements of one of which are non-commutative with the elements of the other. Algorithms for calculating generators of hidden groups of orders p, $p^2 - 1$ and $p^2 + p + 1$ are proposed. For the first time, when calculating the elements of a public key from the elements of a secret key, an algebraic element of order two was used as a masking factor and the existence of a sufficiently large number of non-scalar matrices with order two was shown. An assessment of the security of the developed algorithm is given.*

7 Dmitriy V. Zakharov, Ph.D. (in Tech.), researcher of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: https://orcid.org0009-0004-5731-3611. E-mail: zakharov.dmitriy@gmail.com

8 Anna A. Kostina, researcher of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: https://orcid.org/0009-0004-5784-7242. Scopus Author ID: 57218870628. E-mail: to.ann@inbox.ru

9 Elena V. Morozova, Ph.D. (in Tech.), associate professor of Department of Integrated Information Security, Admiral Makarov State University of Maritime and Inland Shipping. E-mail: lenmor@mail.ru

10 Dmitriy N. Moldovyan, Ph.D. (in Tech.), associate professor of St. Petersburg State Electrotechnical University «LETI», St. Petersburg, Russia. ORCID: https://orcid.org/0000-0001-5039-7198. Scopus Author ID: 36634567300. E-mail: mdn.spectr@mail.ru

Practical relevance: *the scientific and practical significance of the results of the article consists in increasing the performance of post-quantum algebraic signature algorithms exploiting computational complexity of solving large systems of power equations.*

References

1. Post-Quantum Cryptography. 15th International Conference, PQCrypto 2024, Oxford, UK, June 12–14, 2024, Proceedings // Lecture Notes in Computer Science. 2024. V. 14771–14772. Springer, Cham.
2. Post-Quantum Cryptography. 14th International Conference, PQCrypto 2023, College Park, MD, USA, August 16–18, 2023, Proceedings // Lecture Notes in Computer Science. 2023. V. 14154. Springer, Cham.
3. Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2022. P. 1–17. DOI: 10.1049/ise2.12092
4. Ding J.,Petzoldt A.. Current State of Multivariate Cryptography // IEEE Security and Privacy Magazine. 2017. Vol. 15. No. 4. P. 28–36.
5. Ding J., Petzoldt A., Schmidt D.S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer, New York. 2020. V. 80. P. 7–23. DOI: 10.1007/978-1-0716-0987-3_2.
6. Moldovyan N.A. Finite algebras in the design of multivariate cryptography algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics. 2023. No. 3 (103). P. 80–89. DOI: https://doi.org/10.56415/basm.y2023.i3.p80.
7. Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. V.32. N. 1(94). P. 46–60. DOI: 10.56415/csjm.v32.04.
8. Moldovyan A.A. , Moldovyan N.A. Parameterized unified method for setting vector finite fields for multivariate cryptography // Vestnik Sankt-Peterburgskogo universiteta. Prikladnaja matematika. Informatika. Processy upravlenija. 2024. T. 20. Vyp. 4. S. 479–486. DOI: 10.21638/spbu10.2024.404
9. Moldovyan A.A., Moldovyan D.N. A New Method for Developing Signature Algorithms // Bulletin of Academy of Sciences of Moldova. Mathematics, 2022. No. 1(98). P. 56–65. DOI: 10.56415/basm.y2022.i1.p56.
10. Moldovyan N.A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022, vol. 30, no. 2(48), pp. 287–298. DOI: 10.56415/qrs.v30.24.
11. Moldovyan A.A. Complete signature randomization in an algebraic cryptoscheme with a hidden group // Quasigroups and related systems. 2024. Vol. 32. No. 1. P. 95–108. DOI: 10.56415/qrs.v32.08.
12. Moldovjan A.A., Moldovjan D.N., Kostina A.A. Algebraicheskie algoritmy JeCP s polnoj randomizaciej podpisi // Voprosy kiberbezopasnosti. 2024. № 2(60). S. 95–102. DOI: 10.21681/2311-3456-2024-2-95-102.
13. Moldovjan D.N., Kostina A.A. Sposob usilenija randomizacii podpisi v algoritmah JeCP na nekommutativnyh algebrah // Voprosy kiberbezopasnosti. 2024. № 4(62). S. 71–81. DOI: 10.21681/2311-3456-2024-4-71-81.
14. Moldovyan D.N., Moldovyan A.A., Moldovyan N.A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022, vol. 30, no. 1, pp. 133–140. DOI: 10.56415/qrs.v30.11.
15. Moldovyan N.A., Moldovyan A.A. Digital signature scheme on the 2x2 matrix algebra algebra // Vestnik Sankt_peterburgskogo universiteta. Prikladnaja matematika. Informatika. Processy upravlenija. 2021. T. 17 Vyp. 3. S. 254–261. DOI: 10.21638/11701/spbu10.2021.303
16. Moldovjan N.A, Petrenko A.S. Algebraicheskij algoritm JeCP s dvumja skrytymi gruppami // Voprosy kiberbezopasnosti. 2024. № 6(64). S. 98–107. DOI: 10.21681/2311-3456-2024-6-98-107.
17. Dinh K.L., Nguyen L.G, Do T.B., Moldovyan A.A., Moldovyan D.N., Kostina A.A. Defining High-Dimensional Non-Commutative Algebras as Carriers for Post-Quantum Digital Signature Algorithms // Proceedings of the 1st International Conference On Cryptography and Information Security (VCRIS), Hanoi, Vietnam, 2024. P. 1–5, DOI: 10.1109/VCRIS63677.2024.10813386.
18. Duong M.T., Moldovyan D.N., Do B.V., Minh Hieu Nguyen M.H. Post-quantum signature algorithms on noncommutative algebras, using difficulty of solving systems of quadratic equations // Computer Standards and Interfaces. 2023. Vol. 86. P. 103740. DOI: 10.1016/j.csi.2023.103740. ISSN 0920-5489.
19. Moldovjan D.N., Moldovjan A.A. Algebraicheskie algoritmy JeCP, osnovannye na trudnosti reshenija sistem uravnenij // Voprosy kiberbezopasnosti. 2022. № 2(48). S. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.
20. Moldovyan D.N. A new type of digital signature algorithms with a hidden group // Computer Science Journal of Moldova. 2023, vol. .31, No. 1(91), pp. 111–124. doi:10.56415/csjm.v31.06.

КВАНТОВО-УСИЛЕННЫЙ СИММЕТРИЧНЫЙ КРИПТОАНАЛИЗ S-AES

Моисеевский А.Д.[1], Манько С.Д.[2]

DOI: 10.21681/2311-3456-2025-3-55-62

Цель исследования: *исследование возможности снижения ресурсных требований к реализации атаки алгоритмом Гровера на блочные шифры на примере упрощённого шифра S-AES. Исследование возможностей учёта частичной утечки ключа. Оценка необходимых ресурсов и численное моделирование квантовой атаки на S-AES со сниженными требованиями.*

Методы исследования: *алгебраический анализ, численное моделирование.*

Результаты исследования: *продемонстрирована возможность существенного снижения числа кубитов за счёт оптимизации оракула при реализации атаки алгоритмом Гровера на симметричные блочные шифры на примере S-AES. Необходимые для моделирования квантовой атаки S-AES ресурсы снижены достаточно, чтобы стало возможным исследование данного алгоритма посредством численного моделирования на ПК с 400Мб ОЗУ за время порядка 30 минут (в зависимости от конфигурации CPU). Благодаря этому проведено численное моделирование квантовой атаки на S-AES для идеального случая и с учётом элементарных шумов квантового вычислителя.*

Научная новизна: *предложен новый алгоритм квантовой атаки на шифр S-AES с существенно сниженными требованиями по числу кубитов. Проведено численное моделирование атаки при помощи данного алгоритма, что для известных ранее атак было практически невозможно. Результаты иллюстрируют, что наши представления о ресурсных требованиях квантовой атаки и, как следствие, возможном горизонте её практической реализации могут быть существенно ошибочными, если будет найден альтернативный способ реализации даже уже известного концептуально и асимптотически не улучшаемого алгоритма квантовой атаки.*

Ключевые слова: *квантовые вычисления, квантовый криптоанализ, квантовая угроза, симметричное шифрование, S-AES.*

Введение

Наравне с алгоритмом Шора, алгоритм Гровера уже более 20 лет рассматривается как актуальная угроза информационной безопасности [1]. Для симметричных шифров именно асимптотическую устойчивость к атаке Гровера Национальный Институт Стандартов и Технологий (NIST) принимает за меру пост-квантовой стойкости криптографического алгоритма [2]. Данная атака позволяет корневым образом сокращать асимптотическую сложность перебора симметричного ключа. Следовательно, для сохранения прежней криптографической стойкости и ожидаемого времени конфиденциальности зашифрованных данных, возникает необходимость использовать в два раза более длинные ключи. Такая угроза не является критической для информационной безопасности в целом, однако может требовать внимания в случае перехвата сообщений, зашифрованных по не учитывающему данную угрозу стандарту. Оценка связанных с этим рисков требует понимания того, какими характеристиками должен обладать квантовый компьютер для реализации подобной атаки.

Реализации подобной угрозы препятствуют в основном два сдерживающих фактора: доступный размер регистра квантового вычислителя и ограниченное количество операций, которые можно произвести с кубитом за время его когерентности. Таким образом главным параметром шифра при оценке его подверженности квантовой атаке является длина ключа, которая определяет необходимое число кубитов для реализации алгоритма. При этом ограничение, связанное с конечным временем когерентности кубита и предельным количеством операций в алгоритме, хоть и также является крайне существенным, не настолько критично, поскольку влияние шумов, в отличие от числа кубитов, в большинстве случаев может быть уменьшено минимальным вмешательством в конструкцию аппаратной установки и использованием методов подавления ошибки [3]. Недостаток же числа кубитов на имеющимся аппаратном обеспечении является строгим ограничением, и может быть исправлен только существенной переработкой экспериментальной установки. Исключением, с некоторыми техническими оговорками, можно назвать архитектуру квантовых вычислителей на основе холодных атомов.

Количество кубитов, необходимых для атаки как симметричных, так и асимметричных шифров, в первую очередь определяется размером используемого

1 Моисеевский Алексей Денисович, АО «ИнфоТеКС», ООО «С-Квантум», Центр Квантовых Технологий МГУ им. М.В. Ломоносова. Москва, Россия. E-mail: Aleksey.Moiseevsky@infotecs.ru

2 Манько Софья Дмитриевна, АО «ИнфоТеКС». Москва, Россия. E-mail: Sofia.Manko@infotecs.ru

ключа. При этом длина ключа в симметричном стандарте AES составляет от 128 до 256 бит [4]. С 2011 г. существует также версия AES-512, однако данная версия не принята в настоящее время в качестве стандарта [5]. Рекомендуемая же длина ключа для асимметричного стандарта RSA составляет от 2048 бит [6]. Если не принимать во внимание работу [7], подвергнутую всесторонней критике [8, 9], то длину ключа можно рассматривать как неточную оценку снизу для объёма квантового регистра, необходимого для атаки. Крупнейшие на момент начала 2025 года квантовые вычислители обладают регистром в 1225 [10] и 1180 [11] физических кубитов, подверженных влиянию шумов. Таким образом сегодня не существует квантовых вычислителей, способных осуществлять полную атаку на какие-либо принятые стандарты шифрования. Но можно ожидать, что экспериментальная реализация квантовой атаки на шифры с закрытым ключом станет возможна значительно раньше, чем на методы асимметричной криптографии.

Предыдущие и новые результаты

Исследование аспектов практической реализации атаки алгоритмом Гровера на AES 128 было проведено в работе [12]. Представленные результаты позволяют реализовывать атаку Гровера на шифр AES-128 с использованием 264 кубитов. Поскольку асимптотически атака Гровера не может быть улучшена, интерес представляет исследование возможности ещё большего снижения данного значения, например за счёт частичной утечки ключа вследствие атаки по побочному каналу.

Поскольку моделирование 264-кубитного регистра находится далеко за рамками возможностей классических симуляторов квантового компьютера, первоначальное исследование было проведено для упрощённого шифра S-AES [13]. S-AES представляет собой блочный шифр с 16-битным ключом, 16-битным текстом и двумя раундами. Прямая атака Гровера на S-AES требует 32-кубитного регистра и принципиально может быть промоделирована с помощью классического симулятора, хотя данная процедура и потребует больших вычислительных ресурсов. Это открывает возможности для исследования концепций оптимизации атаки на примере данного упрощённого шифра. Всесторонний анализ вопросов реализации атаки алгоритмом Гровера на S-AES, включая построение квантовых вариантов преобразований S-Box и MixColumn проведён в работах [14, 15].

В данной работе описывается концепция квантовой атаки на S-AES с частичной утечкой ключа и идея общей оптимизации оракула. Оригинальная оптимизированная атака, названная в дальнейшем атакой разделением, позволяет производить ускоренный поиск ключа с использованием $23 - 4n$ кубитов, где $n \in [1;3]$ – число известных полубайтов ключа. Снижение требований для объёма квантового регистра до 23 кубитов в общем случае позволило моделировать квантовую атаку на ПК и с использованием графических ускорителей. Это, в свою очередь, позволило произвести оценку шумовой устойчивости квантового алгоритма к элементарным ошибкам.

Сравнительные данные по промоделированным в работе методам атаки, а также сравнение с прямой атакой на S-AES, описанной в [14], приведены в таблице 1. Приводятся результаты для обычной 32-кубитной атаки, атаки с утечкой первого байта ключа, атаки разделением и атаки разделением с утечкой одного байта ключа. Приводимые характеристики – число кубитов, необходимое для атаки, глубина схемы (число слоёв при максимальной параллелизации применения гейтов), общее число запутывающих двухкубитных гейтов CNOT, время симуляции на ПК с 8-ядерным ЦП 2,5 ГГц и 64 Гб RAM. Моделирование атаки разделением без утечки использует 400 Мб RAM. Моделирование прямой 32-кубитной атаки на ПК с данными характеристиками невозможно. Разброс в значении глубины схемы объясняется необходимостью многократной загрузки открытого текста и шифртекста в квантовый регистр в ходе итераций Гровера, что осуществляется с помощью классически-контролируемых гейтов, число которых определяется конкретным битовым представлением текста.

Таблица 1.

Соотношение ресурсов, необходимых для реализации и моделирования атаки Гровера на S-AES с различным типом оракула

Оракул	Число кубитов	Глубина	Число CNOT	$t_{симуляции}$
Обычный [14]	32	459 512 ± 100	478 380	–
С утечкой второго байта ключа	24	24 191 ± 9	19 092	60 с
Разделением	23	1 698 762 ± 1289	2 195 724	1080 с
Разделением, с утечкой одного байта ключа	15	73 678 ± 99	58 944	5 с

Прямая атака Гровера на S-AES

Изначально алгоритм Гровера является ускоренным алгоритмом поиска по неструктурированной базе данных [1]. Если для искомого элемента базы данных выполняется уравнение $f(x) = 1$, а для остальных $f(x) = 0$, и реализовано квантовое преобразование

$$\hat{U}|x\rangle = (-1)^{f(x)}|x\rangle, \quad (1)$$

алгоритм Гровера позволяет найти искомый элемент за число обращений к оператору $\hat{U}$, равное

$$R = \lfloor \frac{\pi}{4} \sqrt{\frac{N}{M}} \rfloor. \quad (2)$$

Здесь N – общее число элементов базы данных, M – число элементов, удовлетворяющих уравнению $f(x) = 1$. В случае поиска по множеству n-битных ключей, $N = 2n$. Оператор $\hat{U}$ называется оракулом и является подпрограммой алгоритма Гровера. При этом оракул содержит всю информацию о решаемой задаче, остальной алгоритм в зависимости от конкретной поставленной задачи не меняется.

Выражение (1) означает, что оператор $\hat{U}$ должен инвертировать фазу состояния $|x\rangle$, соответствующего искомому элементу, и оставлять неизменными все остальные состояния [16]. Это позволяет получить ясное представление об устройстве оракула, делающего алгоритм Гровера полезным в приложении задач криптоанализа.

Рассматривается задача атаки открытого текста: для заданного открытого текста и шифртекста необходимо определить ключ, которым было произведено зашифрование. Решение подобной задачи представляет интерес с практической точки зрения, поскольку тот же ключ мог быть использован для шифрования других данных. Утверждается, что не существует иного способа отыскания ключа по тексту и шифртексту, кроме перебора. Для ускорения перебора может быть использован алгоритм Гровера.

В результате выполнения алгоритма состояние $|x\rangle$ должно содержать единственную доминирующую амплитуду, индекс которой в битовом представлении соответствует предполагаемому ключу. Оракул $\hat{U}$ может содержать информацию о текстах, в том числе в дополнительных кубитах. Функцией $\hat{U}$ для задачи криптоанализа будет зашифрование открытого текста с помощью ключа $|x\rangle$ и сравнение результата с известным шифртекстом. Если полученный и заданный шифртексты совпадают, оператор $\hat{U}$ должен инвертировать фазу состояния $|x\rangle$. Блок PTXT обозначает инициализацию квантового регистра данными классического текста через классически-контролируемые гейты $\hat{X}$. Сравнение текстов может быть произведено путём добавления в квантовый регистр классических данных о зашифрованном тексте. На рис. 1 данная операция показана блоком !CTXT. Если бит шифртекста с некоторым индексом равен 0, то операция !CTXT подействует оператором $\hat{X}$ на кубит с тем же индексом. Таким образом, если на вход оракула подавался корректный ключ, после действия операции !CTXT все дополнительные кубиты (не кубиты текста) будут находиться в состоянии $|1\rangle$, и действующий на них оператор C16Z инвертирует фазу данного состояния (Здесь и далее как CnZ или CnNOT обозначаются условные операторы, контролируемые несколькими кубитами: C1Z – CZ, C1NOT – CNOT, C2NOT – оператор Тоффоли и т.д.). Дальнейшие обратные преобразования в оракуле приведут дополнительные кубиты к состоянию $|0\rangle$, а кубиты ключа – к состоянию $U|x\rangle$. Оракул для атаки AES-128 может быть построен аналогичным образом с точностью до числа кубитов и раундов.

Прямая атака S-AES с утечкой

Описанная выше атака требует 32 кубита. Симуляция алгоритма с регистром такого объёма даже при эмуляции идеальной унитарной динамики чистых состояний требует более 40 ГБ оперативной памяти, что делает практически невозможным симуляцию данной атаки на GPU. Возможный способ уменьшить количество требуемых кубитов — рассмотреть случай, когда часть битов ключа оказывается известна благодаря атаке по стороннему каналу.

Как можно видеть на рис. 1, в спецификации S-AES 16-битные ключи раунда делятся на два

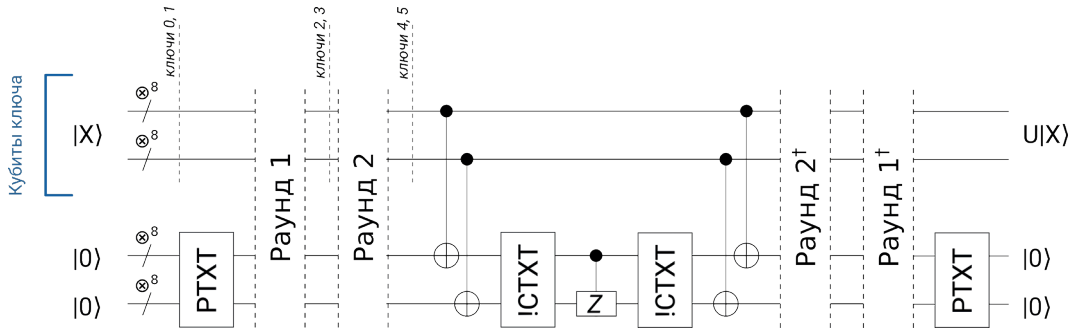


Рис. 1. Топологическая схема оракула для прямой 32-кубитной атаки Гровера на S-AES. AES может быть построен аналогичным образом с точностью до числа кубитов и раундов.

8-битных сегмента, обычно обозначаемых B. Текст делится на два 8-битных сегмента, обозначаемых $N_{1,2}$. Рассмотрим простой случай, когда ключ B_1 оказался известен. Для этого, во-первых, определим алгебраические выражения ключей раундов. Исходные ключи обозначаются как B_0 и B_1, ключи первого раунда – B_2 и B_3, второго – B_4 и B_5. Здесь и далее обозначение операций побитового сложения опускаются для краткости.

$$B_0 = B_0 \qquad B_3 = B_1B_2 = C_0B_0B_1B_1^{SR}$$
$$B_1 = B_1 \qquad B_4 = C_1B_2B_3^{SR} = C_0C_1B_0B_1^{SR}[C_0B_0B_1B_1^{SR}]^{SR} \quad (3)$$
$$B_2 = C_0B_0B_1^{SR} \qquad B_5 = B_3B_4 = C_1B_1B_2B_2B_3^{SR} = C_1B_1B_3^{SR}$$

Здесь C_0 и C_1 — специфицированные константы раундов, верхние индексы S и R обозначают действие операций подстановки (S-Box) и разворота полубайтов (RotateNibble). Интерес представляет вопрос, можно ли использовать дополнительные данные о битах ключа для модификации алгоритма и распутывания (факторизации) кубитов, соответствующих известным битам от состояния остального квантового регистра.

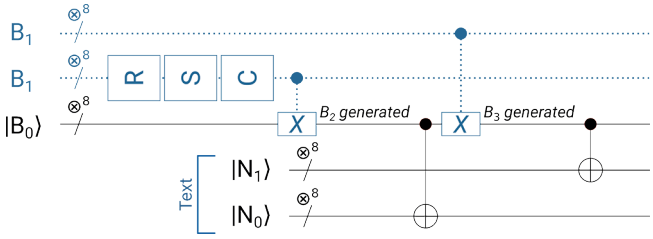


Рис. 2. Расширение ключа при частном случае утечки.

Блоки R, S и C обозначают операции RotateNibble, S-Box и AddConst соответственно.

На рис. 2 показан процесс расширения ключа при утечке исходного байта B_1. Данные B_1 находятся в классической памяти, что обозначено цветным пунктиром. Не представляет сложности генерация B_2 в кубитах, в которых исходно хранился байт B_0. Генерация B_3 затем может быть произведена после использования B_2, в тех же кубитах, с использованием классической копии B_1.

Определённую сложность представляет генерация B_4. Как видно из формул (3), выражение B_4 включает в себя битовую сумму B_0 со значением функции S-Box, аргумент которой также содержит B_0. Таким образом, данное выражение становится необратимым, процедура его генерации становится неунитарным преобразованием, соответственно, не может быть реализована в виде квантовой программы без привлечения дополнительных кубитов.

Обойти данную проблему можно путём перехода от генерации B_4 сразу к вычислению результатов раунда для регистра текста, добавляя слагаемые B_4 к тексту последовательно, как это показано на рис. 3.

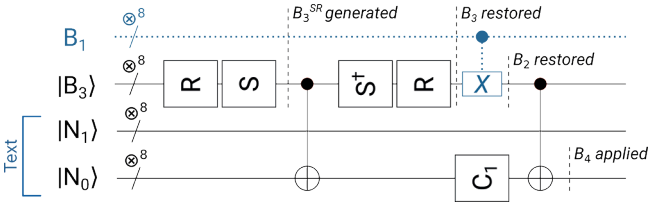


Рис. 3. Добавление ключа раунда B_4 к байту текста N_0 без непосредственного расчёта B_4 в кубитах регистра.

Генерация B_5 также не представляет сложностей и является обратимой. Таким образом при утечке B_1 возможна реализация атаки всего на 24 кубитах вместо 32, что уже доступно для численного моделирования на GPU. Однако описанный подход оказывается невозможен при утечке B_0. По этой причине для построения общей оптимизированной атаки требуется иной подход.

Атака S-AES разделением

В основе атаки разделением лежит идея повторного использования кубитов за счёт последовательной генерации полубайтов текста. Вместо хранения полного текста и полного ключа в 32 кубитах, выделяется 16 кубитов на работу с ключом и 4 кубита для работы с текстом. В регистре ключа происходит процедура генерации ключей раунда, в то время как в регистре текста генерируется зашифрованный полубайт. Далее происходит сравнение полученного полубайта с соответствующим полубайтом известного шифртекста. Результат записывается в 1 кубит-анциллу с помощью гейта C4NOT с четырьмя контрольными и одним целевым кубитом. Повторив данную процедуру для трёх полубайтов 16-битного текста, сохранив результаты сравнения в три кубита-анциллы и проведя сравнение для последнего полубайта в 4 кубитах регистра текста, необходимо подействовать на регистр текста и анциллы гейтом C7Z. В случае, если на вход оракула был подан корректный ключ, значение всех анцилл, а также кубитов регистра текста будет $|1\rangle$, и гейт C7Z инвертирует фазу данного состояния. Данные шаги изображены на рис. 4. Далее, аналогично схеме на рис. 1 необходимо произвести обратные преобразования для восстановления исходных значений кубитов в регистре ключа.

В общем случае для атаки разделением требуется 23 кубита. Верхний индекс операции !CTXT указывает, какой полубайт шифртекста сравнивается с содержимым регистра. Преобразование $Round\ A.B$ на рис. 4 генерирует один из четырёх полубайтов результата раунда. A обозначает номер раунда, а B обозначает номер полубайта результата.

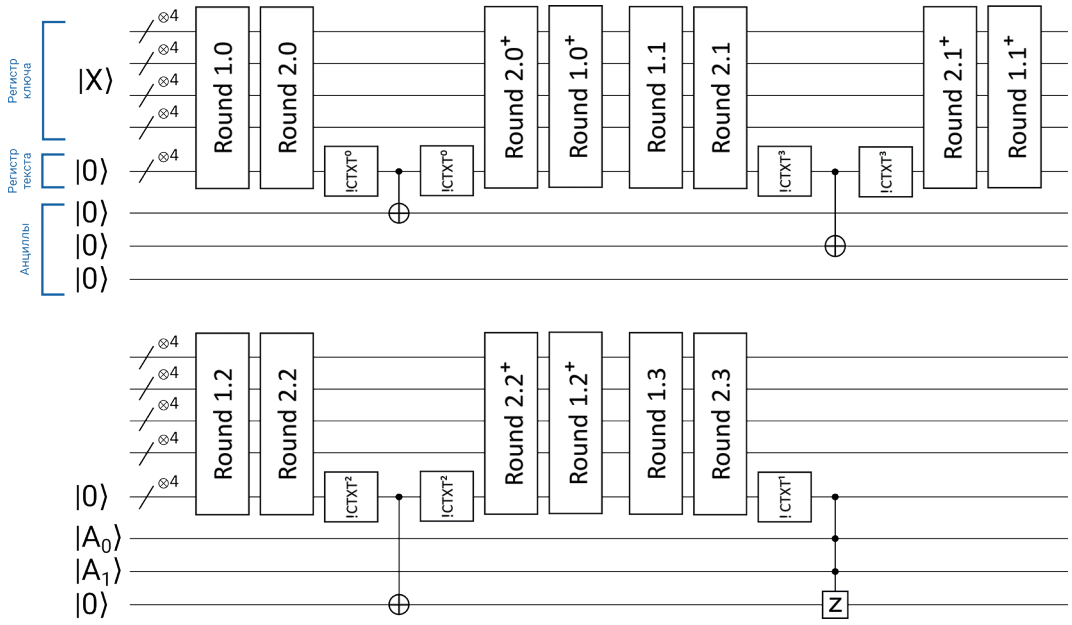


Рис. 4. Топологическая схема оракула атаки разделением.

Данная конфигурация оракула требует $N = 16$ (регистр ключа) + 4 (регистр текста) + 3 (анциллы) = = 23 кубита. Также данная атака естественным образом обрабатывает любую полубайтовую утечку, обеспечивая соответствующую дополнительную экономию кубитов.

Ключевым элементом при обработке утечки, а также в целом при пополубайной генерации шифтекста

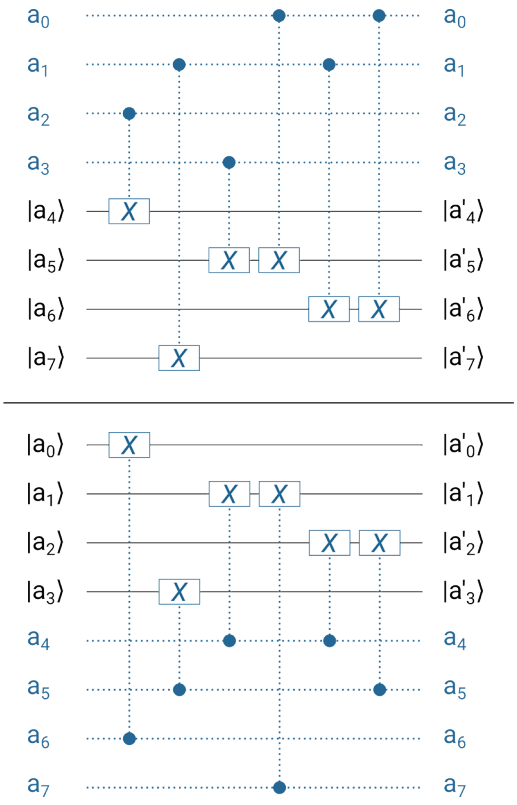


Рис. 5. Схемы гибридного преобразования MixColumn.

является схема частичного преобразования MixColumn (далее MC). Преобразование MC является одним из базовых в шифрах AES и S-AES, и применяется в ходе раунда. В случае S-AES оно действует на 8 битов и генерирует 8-битный результат. Поскольку для каждого байта результирующего шифртекста требуется сгенерировать сначала первый полубайт, а затем второй, необходимо сконструировать 8-кубитное преобразование, которое сохраняет состояние одного входного полубайта неизменным, а во втором способно генерировать как первый, так и второй полубайт результата. Для обеспечения возможности обработки утечки также необходимо избежать использования запутывающих гейтов CNOT, для которых кубиты, оставляемые в преобразовании неизменными, являлись бы целевыми. Схемы данных преобразований следуют из спецификации S-AES и представлены на рис. 5.

Преобразование действует на 8 кубитов, из которых 4 остаются неизменными, а на месте оставшихся четырёх генерируется один из двух полубайтов результата обычного преобразования MixColumns. Кубиты, которые остаются неизменными, обозначены на рис.5 цветным пунктиром. Поскольку данные кубиты выступают исключительно контрольными, в случае частичной утечки вместо них могут быть использованы классические биты. Данных преобразований достаточно для реализации атаки разделением с любой конфигурацией полубайтов утечки.

Моделирование оптимизированной атаки S-AES

В ходе работы было проведено моделирование полной атаки разделением, атаки разделением с утечкой и прямой атаки с утечкой B_1. Ресурсные

характеристики квантовых схем данных атак представлены в таблице 1.

Снижение ресурсных требований к моделированию на классических симуляторах позволило произвести анализ устойчивости атак к элементарным квантовым шумам: ошибке инвертирования значения бита (вероятностное применение оператора $\hat{X}$) и инвертирования фазы (вероятностное применение оператора $\hat{Z}$) при применении двухкубитного гейта в декомпозированной схеме. Полученные в результате зависимости вероятности определения корректного ключа от вероятности ошибки представлены на рис. 6 и рис. 7.

Получение подобных зависимостей без привлечения алгоритмов атаки с утечкой и атаки разделением было практически нереализуемо, поскольку однократное исполнение полной 32-кубитной атаки Гровера на S-AES с шумовой моделью на вычислительном кластере Центра квантовых технологий МГУ занимало более 480 часов. На представленных же графиках каждая точка получена усреднением по 50 запускам.

Данные графики позволяют сформировать представление о величине шумов, которым может быть подвержен квантовый компьютер для практического применения в задачах квантового криптоанализа. Очевидно, что влияние шумов на алгоритм атаки на полноценные шифры AES-128 и AES-256 будет ещё на порядок выше. При этом из графиков можно сделать вывод, что атака разделением более чувствительна к шумовому воздействию, очевидно, за счёт значительно большей глубины алгоритма. Однако необходимо помнить, что данная атака требует меньше кубитов, а при условно сопоставимом техническом исполнении аппаратного обеспечения, уровень ошибок в регистре меньшего объёма будет ниже. Убедиться в этом можно на примере дорожной карты квантовых вычислителей IBM [11]. Анализ возможности расширения представленных концепций экономии кубитов для AES-128 и построение подобных графиков шумовой устойчивости хотя бы для исключительных случаев с утечкой большей части ключа позволит расширить понимание подходов к перспективной задаче квантового криптоанализа и обеспечить большую степень готовности к реализации квантового превосходства для отрасли информационной безопасности.

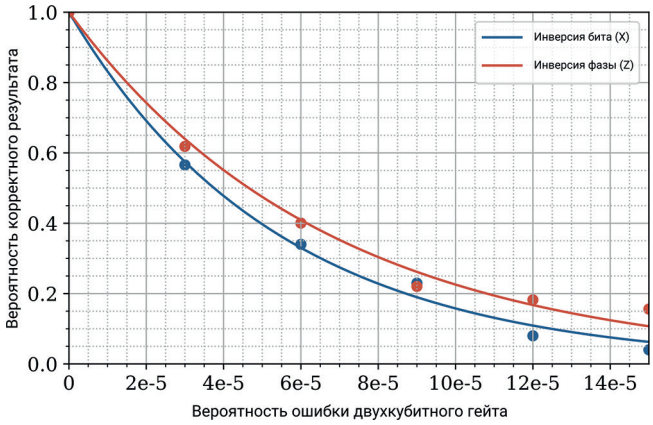


Рис. 6. Зависимость вероятности обнаружения корректного ключа от вероятности битовой и фазовой ошибки двухкубитного гейта для прямой атаки с утечкой (24 кубита). Аппроксимация $y = e^{-ax}$, Для ошибки фазы a = 18468, для ошибки бита a = 14893

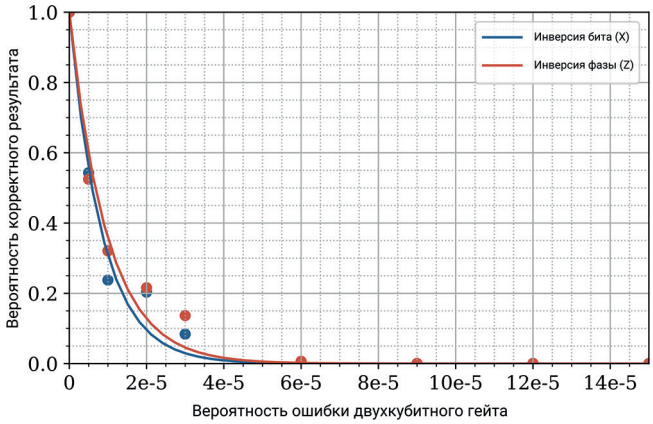


Рис. 7. Зависимость вероятности обнаружения корректного ключа от вероятности битовой и фазовой ошибки двухкубитного гейта для разделением атаки с утечкой (15 кубитов). Аппроксимация $y = e^{-ax}$. Для ошибки фазы a = 117545, для ошибки бита a = 102862

Литература

1. Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing. – 1996. – С. 212–219.
2. NIST. FAQ on Kyber512 // URL: csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/faq/Kyber-512-FAQ.pdf. – 2023.
3. Cai Z. et al. Quantum error mitigation //Reviews of Modern Physics. – 2023. – Т. 95. – №. 4. – С. 045005. DOI: 10.1103/RevModPhys.95.045005.
4. NIST. Advanced Encryption Standard (AES) // Federal Information Processing Standards Publication 197. - 2001. DOI: 10.6028/NIST.FIPS.197.
5. Moh'd A., Jararweh Y., Tawalbeh L. AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation. || In Information Assurance and Security (IAS) //2011 7th International Conference on. – С. 292–297. DOI: 10.1109/ISIAS.2011.6122835.
6. Ferraiolo H., Regenscheid A. Cryptographic algorithms and key sizes for personal identity verification // National Institute of Standards and Technology Special Publication 800. – 2024. DOI: 10.6028/NIST.SP.800-78-5.
7. Yan B. et al. Factoring integers with sublinear resources on a superconducting quantum processor //arXiv preprint arXiv:2212.12372. – 2022.

8. Khattar T., Yosri N. A comment on «Factoring integers with sublinear resources on a superconducting quantum processor» // arXiv preprint arXiv:2307.09651. – 2023.
9. Grebnev S. V. et al. Pitfalls of the sublinear QAOA-based factorization algorithm // IEEE Access. – 2023. – Т. 11. – С. 134760–134768. DOI: 10.1109/ACCESS.2023.3336989.
10. Atom Computing. Quantum startup Atom Computing first to exceed 1,000 qubits // URL: https://atom-computing.com/quantum-startup-atom-computing-first-to-exceed-1000-qubits/. – 2023.
11. IBM. IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility // URL: newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility. – 2023.
12. Li Z. et al. New record in the number of qubits for a quantum implementation of AES //Frontiers in Physics. – 2023. – Т. 11. – С. 1171753. DOI: 10.3389/fphy.2023.1171753.
13. Musa M. A., Schaefer E. F., Wedig S. A simplified AES algorithm and its linear and differential cryptanalyses // Cryptologia. – 2003. – Т. 27. – №. 2. – С. 148–177. DOI: 10.1080/0161-110391891838.
14. Jang K. B. et al. Grover on simplified aes //2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). – IEEE, 2021. – С. 1–4. DOI: 10.1109/ICCE-Asia53811.2021.9642017.
15. Almazrooie M. et al. Quantum Grover attack on the simplified-AES //Proceedings of the 2018 7th International Conference on Software and Computer Applications. – 2018. – С. 204–211. DOI: 10.1145/3185089.3185122.
16. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Перевод с английского под редакцией М. Н. Вялого и П. М. Островского с предисловием К. А. Валиева // Москва «МИР». – 2006. С. 311–320.

QUANTUM-ENHANCED SYMMETRICAL CRYPTOANALYSIS OF S-AES

Moiseevskiy A. D.[3], Manko S. D.[4]

Keywords: *quantum computing, quantum cryptanalysis, quantum threat, symmetric encryption, S-AES.*

Objective of the study: *to study the possibility of reducing quantum resource requirements for Grover's algorithm attack on block ciphers. Simplified-AES is considered as an example. To investigate the possibilities of using a partial key leakage. To estimate the required resources and to simulate a quantum attack on S-AES with reduced requirements.*

Research methods: *algebraic analysis, numerical simulation.*

Research results: *we have demonstrated the possibility of significantly reducing the number of qubits required to attack Simplified-AES by optimizing Grover's oracle. The resource requirements are reduced sufficiently, allowing to study quantum attack on Simplified-AES using numerical simulation on a PC with 400 MB of RAM in about 30 minutes (depending on the CPU configuration). A numerical simulation of a quantum attack on S-AES has been carried out for the case of an ideal leakage configuration, taking into account the elementary quantum noises.*

Scientific novelty: *a new quantum attack algorithm for Simplified-AES cipher with significantly reduced requirements for the qubits number is proposed. Numerical simulation of the attack using this algorithm is carried out, which was practically impossible for previously known approaches. The results illustrate that our ideas about the resource requirements for a quantum attack and, as a consequence, the possible time of its practical implementation can be significantly incorrect if an alternative method for implementing even an already known asymptotically unimprovable quantum attack algorithm is found.*

References

1. Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. – 1996. – S. 212–219.
2. NIST. FAQ on Kyber512 //URL: csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/faq/Kyber-512-FAQ.pdf. – 2023.
3. Cai Z. et al. Quantum error mitigation // Reviews of Modern Physics. – 2023. – Т. 95. – №. 4. – S. 045005. DOI: 10.1103/RevModPhys.95.045005.
4. NIST. Advanced Encryption Standard (AES) // Federal Information Processing Standards Publication 197. - 2001. DOI: 10.6028/NIST.FIPS.197.
5. Moh'd A., Jararweh Y., Tawalbeh L. AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation. || In Information Assurance and Security (IAS) //2011 7th International Conference on. – S. 292–297. DOI: 10.1109/ISIAS.2011.6122835.
6. Ferraiolo H., Regenscheid A. Cryptographic algorithms and key sizes for personal identity verification //National Institute of Standards and Technology Special Publication 800. – 2024. DOI: 10.6028/NIST.SP.800-78-5.
7. Yan B. et al. Factoring integers with sublinear resources on a superconducting quantum processor //arXiv preprint arXiv:2212.12372. – 2022.

3 Alexey D. Moiseevskiy, InfoTeCS JSC, S-Quantum LLC, MSU Quantum Technology Centre. Moscow, Russia. E-mail: Aleksey.Moiseevsky@infotecs.ru
4 Sofya D. Manko, InfoTeCS JSC. Moscow, Russia. E-mail: Sofia.Manko@infotecs.ru

8. Khattar T., Yosri N. A comment on «Factoring integers with sublinear resources on a superconducting quantum processor» //arXiv preprint arXiv:2307.09651. – 2023.
9. Grebnev S.V. et al. Pitfalls of the sublinear QAOA-based factorization algorithm // IEEE Access. – 2023. – T. 11. – S. 134760-134768. DOI: 10.1109/ACCESS.2023.3336989.
10. Atom Computing. Quantum startup Atom Computing first to exceed 1,000 qubits // URL: https://atom-computing.com/quantum-startup-atom-computing-first-to-exceed-1000-qubits/. – 2023.
11. IBM. IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility // URL: newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility. – 2023.
12. Li Z. et al. New record in the number of qubits for a quantum implementation of AES //Frontiers in Physics. – 2023. – T. 11. – S. 1171753. DOI: 10.3389/fphy.2023.1171753.
13. Musa M.A., Schaefer E.F., Wedig S. A simplified AES algorithm and its linear and differential cryptanalyses // Cryptologia. – 2003. – T. 27. – №. 2. – S. 148–177. DOI:10.1080/0161-110391891838.
14. Jang K.B. et al. Grover on simplified AES // 2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). – IEEE, 2021. – S. 1–4. DOI: 10.1109/ICCE-Asia53811.2021.9642017.
15. Almazrooie M. et al. Quantum Grover Attack on the Simplified-AES // Proceedings of the 2018 7th International Conference on Software and Computer Applications. – 2018. – S. 204–211. DOI: 10.1145/3185089.3185122.
16. Nielsen M., Chuang I. Quantum Computation and Quantum Information. Perevod s anglijskogo pod redakciej M.N. Vjalogo i P.M. Ostrovskogo s predisloviem K.A. Valieva // Moskva «MIR». – 2006. C. 311–320.

О ВЛИЯНИИ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ ФУНКЦИЙ ХЕШИРОВАНИЯ НА УСТОЙЧИВОСТЬ СОВРЕМЕННЫХ БЛОКЧЕЙН-ЭКОСИСТЕМ И ПЛАТФОРМ

Ищукова Е. А.[1]

DOI: 10.21681/2311-3456-2025-3-63-71

Целью настоящей работы *является систематизация знаний по функциям хеширования современных блокчейн-экосистем и платформ, а также определение криптографической стойкости упомянутых функций с точки зрения времени, затрачиваемого на проведение криптоанализа.*

Методы исследования *основываются на использовании теории информации, теории устойчивости, теории криптографии и криптоанализа, математического аппарата теории вероятностей и математической статистики, технологии блокчейн, технологиях обеспечения киберустойчивости и информационной безопасности.*

Результаты: *в работе рассмотрены основные бесключевые криптографические примитивы, применяемые в современных блокчейн-системах – функции хеширования. Для них рассмотрены подходы к определению криптографической стойкости с точки зрения вычислительных затрат по отношению ко времени применения тактики полного перебора. Рассмотрено пять различных кейсов применения функций хеширования в составе блокчейн-систем и возможные сценарии атак на них.*

Практическая ценность *заключается в рассмотрении ряда кейсов, связанных с применением функций хеширования в современных блокчейн-системах. Для каждого кейса сформулирована постановка задачи, приведено возможное решение и дана оценка его сложности. Показано, что при правильном использовании функций хеширования обеспечивается достаточная стойкость блокчейн-систем, построенных на их основе. Также показано, что большинство встречающихся уязвимостей связано с ошибками реализации или применения функций хеширования внутри блокчейн-систем, а не со слабостью конструкций используемых функций.*

Ключевые слова: *киберустойчивость, блокчейн, криптографическая стойкость, алгоритм шифрования, функция хеширования, криптография, криптоанализ.*

Введение

Блокчейн технологии являются частным случаем построения систем распределенного реестра. Отличительной особенностью блокчейн технологий является выстраивание единого связанного списка, в котором каждая следующая запись зависит от предыдущей, а значит невозможно изменить какую-то запись в базе данных, не изменив все остальные, связанные с ней записи [1, 2]. Выстраивание единого связанного списка становится возможным за счет использования механизмов криптографии. Как правило, в качестве основных элементов любой блокчейн системы используется асимметричная криптография на эллиптических кривых (для формирования адресов в сети, формирования подписи, а также подтверждения своего права совершать те или иные операции в сети) и функции хеширования (для проверки целостности отдельных записей в системе, проверки целостности блоков, упаковки транзакций в блок, а также в случае необходимости для выстраивания цепочки блоков в соответствии с консенсусом).

Именно поэтому функции хеширования являются объектом пристального внимания ученых, которые изучают их стойкость, моделируя процессы хеширования и пытаясь выявить возможные уязвимости, а также оценить влияние таких уязвимостей на стабильность работы блокчейн системы в целом.

Рассмотрим кратко мировой опыт по анализу наиболее известных функций хеширования. Наибольшее количество работ посвящено анализу функции хеширования SHA-1, которая является предшественницей семейства функций хеширования SHA-2. Так, в 2005 году группа китайских ученых предложила алгоритм поиска коллизий, который оказался в 2000 раз быстрее, чем полный перебор всех возможных комбинаций [3]. В работе [4] рассмотрена успешная атака на алгоритм SHA-1. Авторы нашли способ подделать два разных PDF-документа с одинаковым хешем SHA-1, которые отображают разное произвольно выбранное визуальное содержимое. При этом сами авторы отмечают, что смогли обнаружить эту коллизию, объединив множество специальных криптоаналитических методов сложными способами. Также имеются результаты по дифференциальному анализу функции SHA-1 [5] и ее упрощенных версий [6]. Для текущих используемых функций хеширования

1 Ищукова Евгения Александровна, кандидат технических наук, ведущий научный сотрудник Научного центра информационных технологий и искусственного интеллекта НТУ Сириус. Россия. E-mail: ischukova.ea@talantiuspeh.ru, ORCID 0000-0002-6818-1608.

семейств SHA-2 и SHA-3 в открытой публикации сведения об успешном применении анализа отсутствуют [2]. Наиболее успешной атакой на сегодняшний день является применение метода дифференциального криптоанализа к функции хеширования SHA-256, сокращенной до 46 раундов [7].

Наряду с исследованием структуры функций хеширования с применением различных крипто аналитических техник, изучаются и другие вопросы: скорость работы в зависимости от реализации и используемой аппаратной части, возможность применения в устройствах специального назначения (например, IoT), а также другие вопросы. Так, в работе [8] исследуется влияние выбора другой хэш-функции на общую производительность блокчейна на примере платформы Ethereum. Авторы показали, что производительности блокчейна могут существенно зависеть от используемой хэш-функции. В работе [9] авторы предлагают новое семейство легковесных хэш-функций, предназначенных для приложений IoT в здравоохранении. Похожее исследование представлено в статье [10], где в качестве хеш-функции для систем блокчейн-IoT используется функция HashLEA. Исследование различных аспектов применимости функций хеширования в составе блокчейн-систем также рассматривается в ряде других работ [11–19].

Проведенный анализ показывает, что вопрос надежности и безопасности использования функций хеширования в составе блокчейн-технологий является актуальным. В данной статье предлагается рассмотреть основные подходы к применению функций хеширования в составе блокчейн систем с точки зрения их надежности.

1. Постановка задачи

Целью работы является систематизация знаний о функциях хеширования, используемых в современных блокчейн платформах, в том числе определение их криптографической стойкости с точки зрения времени, затрачиваемого на проведение анализа.

Для достижения поставленной цели необходимо:

1. Дать краткую характеристику для современных функций хеширования и подходов к их анализу, определить назначение их применения внутри блокчейн-систем.
2. Рассмотреть подходы к определению криптографической стойкости для каждого из случаев применения с точки зрения вычислительных затрат по отношению ко времени применения тактики полного перебора.

2. Объект исследования

Под функцией хеширования h = H(M) мы понимаем некоторое необратимое легко вычислимое математическое преобразование H() из сообщения M произвольной длины в сообщение фиксированной длины h. В силу того, что пространство возможных входов в функцию хеширования бесконечно, а пространство выходных значений конечно и ограничено размерностью выходного хеш-сообщения, неизменно будет существовать бесконечное множество коллизий. То есть таких ситуаций, при которых два различных значения M и M1 на входе функции H() приведут к образованию одного и того же выходного значения h = H(M) = H(M1). Криптографически стойкой функцией хеширования считают такую функцию хеширования, для которой не существует эффективного поиска коллизий. При этом различают два вида стойкости при поиске коллизий. Стойкость в слабом смысле сводится к тому, что для заданного сообщения M вычислительно трудно подобрать второе сообщение M1, имеющего такое же хеш-значение h = H(M) = H(M1). Стойкость в сильном смысле сводится к тому, что вычислительно трудно подобрать два произвольных сообщения M и M1, обладающих одним и тем же хеш-значением h = H(M) = H(M1).

Различают ключевые и бесключевые функции хеширования. Как правило, ключевые функции хеширования строятся на основе какого-либо симметричного алгоритма шифрования. В блокчейн-системах обычно используются бесключевые алгоритмы хеширования преимущественно для контроля целостности транзакций и блоков, а также иногда для обеспечения корректной работы механизма выстраивания блоков в цепочку (например, в случае с механизмом консенсуса «доказательство работы» от англ. proof-of-work). Кроме того, используются надстройки над алгоритмами хеширования. Например, схема вычисления HMAC используется для вычисления секретного ключа шифрования из стартовой сид-фразы или вычисления дочерних ключей из мастер-ключа, а схема хеширования с использованием дерева Меркля используется для упаковки выбранных транзакций в блок [2].

3. Подходы к определению стойкости функций хеширования в составе блокчейн систем

Как уже было отмечено ранее, функции хеширования бывают двух видов – ключевые и бесключевые. С точки зрения их применимости в современных блокчейн-системах, будем рассматривать в первую очередь бесключевые функции хеширования. По принципу построения все функции хеширования можно разделить на две категории: построенные на основе структуры Меркля-Дамгарда или построенные по принципу впитывающей губки. К наиболее часто используемым в современных блокчейн-системах можно отнести функции хеширования семейства RIPEMD, функции хеширования семейств SHA-2 и SHA-3. Для российских блокчейн-систем, построенных на основе отечественной

криптографии, используется функция хеширования ГОСТ Р34.11-2012. Так как объем статьи ограничен, то в настоящей работе ограничимся лишь краткой характеристикой по каждой из функций хеширования, применительно к которой будем рассматривать подходы к анализу. Детальное описание работы функций хеширования для всех упоминаемых семейств хеширования можно найти в работе [2].

Функция хеширования RIPEMD-160 построена на основе структуры Меркля-Дамгарда. За один раз она обрабатывает блок данных размерностью 512 бит в течение 80 раундов преобразований. На выходе образуется хеш-значение размерностью 160 бит.

Функция хеширования SHA-256 построена на основе структуры Меркля-Дамгарда. Хеширование выполняется блоками данных по 512 бит с обязательным дополнением последнего блока. Преобразование одного блока выполняется в течение 64 раундов преобразований. На выходе образуется хеш-значение размерностью 256 бит.

Функция хеширования Keccak-256 построена по принципу впитывающей губки. Функция хеширования Keccak лежит в основе семейства хеширования SHA-3. Важно отметить, что по сравнению с семейством SHA-3 оригинальный алгоритм Keccak имеет множество настраиваемых параметров (в то время как в стандарте SHA-3 эти параметры зафиксированы), а также для функции Keccak имеются отличия в том, как выполняется дополнение последнего блока хешируемых данных.

Для того чтобы одно и то же значение хешировалось по-разному, зачастую применяют так называемое «подсаливание» – добавление к исходной информации ничего не значащей последовательности, которая полностью изменит результат хеширования. Так, например, криптокошельки подсаливают сид-фразу, для того чтобы даже одинаковые сид-фразы давали разные секретные ключи в разных криптокошельках. При этом то, как выполняется подсаливание, полностью зависит от разработчика системы. Это может быть уникальное значение соли для каждого пользователя, а может быть глобальная соль, одинаковая для всех пользователей сервиса.

Рассмотрим наиболее известные подходы к анализу криптографических функций хеширования. Для функций хеширования задача анализа сводится либо к нахождению коллизии, либо к нахождению прообраза (восстановлению исходного сообщения).

Атака по словарю. С помощью данной атаки можно осуществлять как поиск коллизии, так и поиск прообраза. Составляется словарь с наиболее вероятными значениями, которые могут поступать на вход функции хеширования. Анализ выполняется поиском по составленной таблице. Успех анализа зависит от объема составленного словаря.

Атака полным перебором. Аналогична атаке по словарю. Только поиск ведется по всем возможным комбинациям символов для входного сообщения. Здесь сложность анализа возрастает с ростом длины входного сообщения.

Радужные таблицы используются для построения цепочек хеш-значений и, как правило, используются для поиска паролей.

Парадокс «дней рождений» заключается в том, что для получения из множества, содержащего N видов элементов, двух элементов одинакового вида требуется сделать O ($\sqrt{N}$) попыток. Благодаря парадоксу «дней рождения» атака методом полного перебора для поиска коллизий требует в $2^{n/2}$ раз меньше операций, чем для поиска прообраза.

Метод дифференциального криптоанализа рассматривает разность двух сообщений (определяемую с помощью операции сложения по модулю 2) и используется для поиска коллизий. Задача сводится к тому, чтобы определить наиболее вероятную разность dM для двух текстов M и M1 (dM = M xor M1), которая после применения функции хеширования h = H(M) и h1 = H(M1) на выходе преобразуется в разность, равную 0: dh = h xor h1 = 0, что фактически означает вариант наличия коллизии:

$$h = h1 = H(M) = h(M1).$$

Метод алгебраического криптоанализа применяется путем построения системы линейных уравнений, связывающих между собой биты исходного сообщения и биты вырабатываемой хеш-последовательности. На сегодняшний день активно развивается направление применения SAT-решателей к решению задач нахождения прообраза и поиска коллизий [20]. Кроме того, известны атаки на упрощенные хеш-функции с применением комбинаций методов дифференциального и алгебраического анализа [2].

Атака на основе использования слабости функции дополнения сообщения используется тогда, когда в хеш-функции отсутствует дополнение сообщения или в силу каких-то причин (например, неправильная программная реализация или слабость самой функции дополнения) дополнение выполняется неправильным образом. Рассмотрим упрощенный пример. Пусть функция хеширования за один раз обрабатывает блок размерностью 8 байт. Допустим, на вход поступает сообщение M = ABCD, которое по размеру меньше, чем обрабатываемый блок на входе функции хеширования. Такое сообщение будет дополнено какой-то битовой последовательностью, например, нулями в младших значащих разрядах до полного размера блока ABCD0000. В этом случае мы легко получаем коллизию. Так как и сообщение M = ABCD, и сообщение M1 = ABCD0000 приведут к одному и тому же хеш-значению.

DOI: 10.21681/2311-3456-2025-3-63-71

Атака удлинением сообщения заключается в том, что для функций хеширования, построенных на основе структуры Меркля-Дамгарда, существует возможность изменить хеш-значение, добавив дополнительный блок информации в конец исходного сообщения. При этом пользователю даже не обязательно знать исходное сообщение. Достаточно иметь выходное хеш-значение, которое будет использовано для инициализации стартовых регистров.

Метод встречи посередине можно применить в том случае, когда процесс хеширования можно разбить на независимые итерации. Или, например, в случае, когда выполняется двойное хеширование друг за другом. В этом случае процессы хеширования можно разделить и выполнять параллельно, после чего производить поиск совпадений.

Рассмотрим несколько кейсов, связанных с применением функций хеширования в современных блокчейн-технологиях. Для каждого из случаев определим возможный сценарий атак и оценим сложность анализа.

Кейс № 1.

Описание задачи: В разных блокчейн-платформах транзакции упаковываются по-разному. Однако при этом, как правило, для упаковки транзакций используется принцип хеширования с использованием дерева Меркля. При вычислении хеш-значения блока используются не сами транзакции, а только корень созданного дерева Меркля. Рассмотрим пример такого блока в случае, когда используется механизм консенсуса, не связанный с вычислением хеш-значения (отличный от PoW).

Постановка задачи: Блок данных M состоит из заголовочной информации и корня дерева Меркля RM, образованного транзакциями блока T1, T2, T3 ...TN. Для вычисления корня дерева Меркля используется функция хеширования h = H(Ti). Необходимо заменить в блоке M одну транзакцию так, чтобы корень дерева Меркля остался неизменным. При этом должны быть соблюдены все правила составления транзакций и блока.

Решение:

Вход: Транзакции T1, T2, T3...TN. Функция хеширования h = H(T). Корень дерева Меркля RM.

Выход: Транзакции T1, T2, T3...TNew.

Пример построения дерева Меркля для различного количества входных транзакций показан на рис. 1. Отличительной особенностью алгоритма является удвоение последнего хеш-значения, если количество листьев в обрабатываемом уровне дерева является нечетным. В современных блокчейн платформах ведется проверка на дублирование транзакций в блоке, чтобы избежать уязвимости CVE-2012-2459. Из рис. 1 наглядно видно, что самым простым вариантом решения поставленной задачи является поиск коллизии для самого нижнего уровня дерева Меркля. Только в этом случае все дальнейшие преобразования будут выполняться одинаково.

В случае нечетного количества транзакций задача сводится к замене последней транзакции TN на транзакцию TNew таким образом, чтобы выполнялось соотношение H(TN||TN) = H(TNew||TNew).

В случае четного количества транзакций задача сводится к замене последней транзакции TN на транзакцию TNew таким образом, чтобы выполнялось соотношение H(TN – 1||TN) = H(TN – 1||TNew).

В обоих случаях перебору (подбору) подлежит одна из транзакций. Основная проблема заключается в том, что новая транзакция TNew должна быть построена по всем правилам, которые предъявляются данной блокчейн системой к построению транзакций. Это означает, что в данном случае нельзя перебирать все возможные двоичные комбинации для второй части хешируемого сообщения. В данном случае можно применить несколько техник анализа.

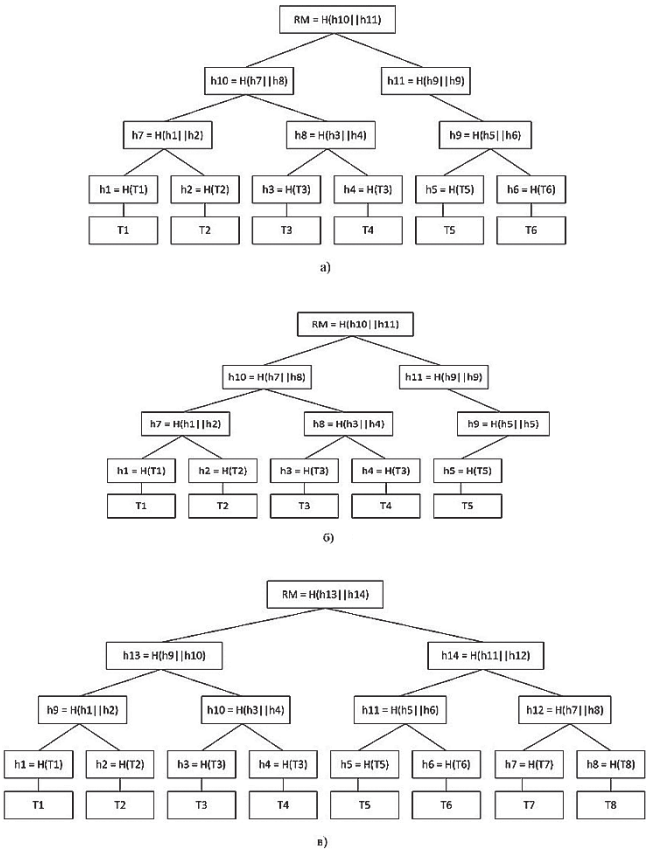


Рис. 1. Пример построения дерева Меркля

Вариант 1. Формирование новой транзакции TNew. Вычисление хеш-значения H(TNew||TNew) или H(TN – 1||TNew). Сравнение полученного хеш-значения с H(TN||TN) или H(TN – 1||TN) соответственно. Сложность анализа будет зависеть от длины n вырабатываемой хеш-последовательности и в среднем составит 2n/2 шагов.

Вариант 2. В случае четного количества транзакций можно попробовать применить метод дифференциального криптоанализа для случая, когда разность входов составляет dT = 0|| (TN xor TNew), а разность выходов dH = 0. Этот вариант, возможно, найдет решение в будущем, так как в настоящий момент сведений о применении метода дифференциального криптоанализа к полнораундовым алгоритмам SHA-1 и SHA-2 нет.

Кейс № 2.

Описание задачи: Для алгоритма консенсуса Proof-of-Work главным критерием выстраивания цепочки блоков является подбор такого значения nonce, при котором результат хеширования блока образует заданное количество нулевых бит в старших разрядах. Транзакции, как и в предыдущем случае, упаковываются с помощью дерева Меркля и при вычислении хеш-значения блока обычно учитывается только корень дерева Меркля. При этом изменение количества и состава транзакций может оказывать влияние на заголовочную информацию в блоке.

Постановка задачи: Блок данных M состоит из заголовочной информации IV, корня дерева Меркля RM и значения nonce. Для вычисления хеша блока используется функция хеширования h = H(M). Необходимо заменить блок M на блок M1 с соблюдением всех правил составления блока (в зависимости от блокчейн-платформы). Например, убрать или добавить одну или несколько транзакций, заменить в транзакции скрипт погашения и т.д. При этом хеш-значение нового блока M1 должно совпадать с хеш-значением блока M.

Решение:

Вход: Блок M = (IV||RM||nonce). Функция хеширования h = H(T).

Выход: Блок M1 = (IV1||RM1||nonce1), такой что h(M) = h(M1)

Данный кейс сводится к задаче поиска коллизии. В отличие от предыдущего кейса, здесь нет необходимости сохранять корень дерева Меркля неизменным. Достаточно переопределить набор транзакций в блоке и стартовую информацию блока (IV1||RM1). После чего необходимо перебирать значение nonce1 до тех пор, пока не будет получена коллизия h(IV||RM||nonce) = h(IV1||RM1||nonce1). Сложность анализа будет зависеть от длины n вырабатываемой хеш-последовательности и в среднем составит 2n/2 шагов.

Кейс № 3.

Описание задачи: В публичных блокчейн-сетях распространена практика, когда публичные ключи пользователей не хранят в системе в открытом виде. Считается, что публичный ключ можно использовать для вычисления приватного ключа, несмотря на то что это является вычислительно сложной задачей. Для платформы Эфириум адрес пользователя в сети составляет 20 байт и вычисляется как хеш от публичного ключа алгоритма ECDSA. В качестве функции хеширования используется алгоритм Keccak-256. Общая схема выработки адреса для сети Эфириум приведена на рис. 2.

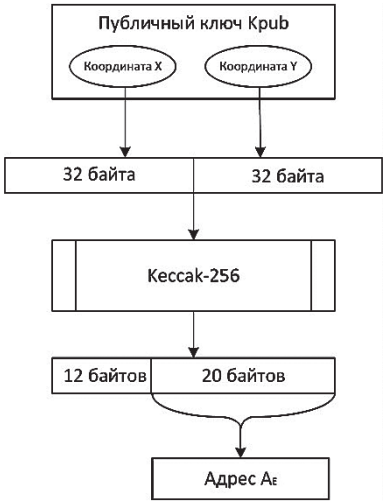


Рис. 2. Алгоритм выработки адреса в сети Эфириум

Постановка задачи: Известен адрес сети Эфириум AE. Определить публичный ключ пользователя.

Решение:

Вход: адрес сети Эфириум AE.

Выход: публичный ключ в виде координат точки Q = (x, y).

В данном случае задача сводится к поиску прообраза. Входными параметрами являются координаты точки Q = (x, y) для эллиптической кривой ECDSA. Забегая вперед (подробнее задачи, связанные с асимметричной криптографией на эллиптических кривых, будут рассмотрены в следующем разделе), отметим следующий факт. Не все возможные значения x в диапазоне от 1 до 2^{256} будут принадлежать заданной эллиптической кривой. Определить, является ли заданное квадратичное уравнение разрешимым для x можно с использованием символа Якоби. Для тех значений x, которые принадлежат заданной эллиптической кривой, всегда будут существовать два значения y. В общем случае алгоритм поиска публичного ключа будет выглядеть следующим образом.

Алгоритм 1:

Для всех x от 1 до $2^{256} - 1$:

1. Определить значение символа Якоби.
2. Если символ Якоби не равен 1, то вернуться к шагу 1.
3. Определить значения y_1 и y_2.
4. Вычислить h = Keccak-256(x||y_1).

DOI: 10.21681/2311-3456-2025-3-63-71

5. Если младшие 20 бит h равны AE, то решение точка (x||y_1).
6. Вычислить h = Keccak-256(x||y_2).
7. Если младшие 20 бит h равны AE, то решение точка (x||y_2).

В общей сложности потребуется 2^{257} операций хеширования для вычисления прообраза точки Q = (x, y).

Кейс № 4.

Описание задачи: Для платформы Биткоин адрес пользователя в сети составляет 25 байт и представляет собой кодировку Base58 от результата двойного хеширования публичного ключа алгоритма ECDSA с применением функций хеширования SHA-256 и RIPEMD-160 с добавлением 4 байтов контроля целостности, которые вырабатываются от старших 21 байта адреса путем двойного хеширования с использованием алгоритма SHA-256. Общая схема выработки адреса для сети Биткоин приведена на рис. 3.

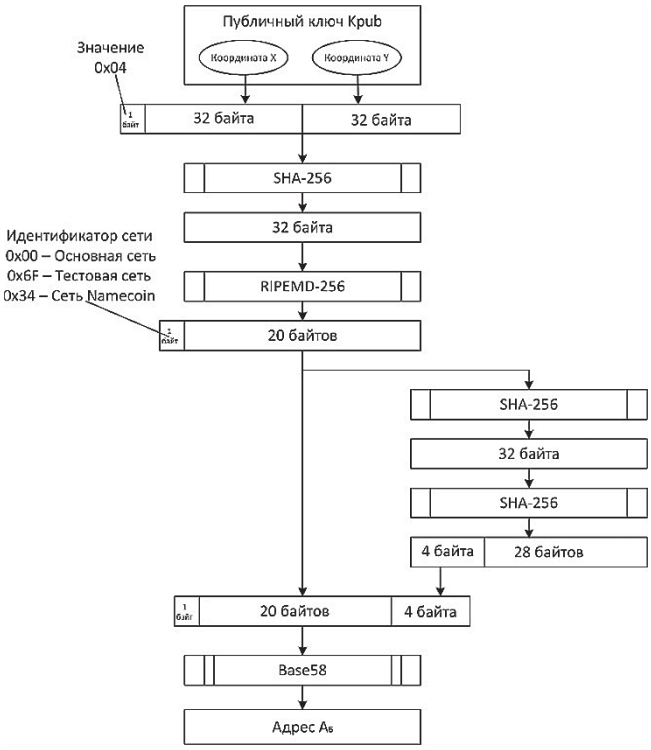


Рис. 3. Алгоритм выработки адреса в сети Биткоин

Постановка задачи: Известен адрес сети Биткоин АБ. Определить публичный ключ пользователя.

Решение:

Вход: адрес сети Биткоин $A_Б$.

Выход: публичный ключ в виде координат точки Q = (x, y).

В данном случае задача также сводится к поиску прообраза. Входными параметрами являются координаты точки Q = (x, y) для эллиптической кривой ECDSA. Первый байт устанавливается равным 0x04 всегда, что означает запись точки эллиптической кривой в развернутом виде. Аналогично предыдущему кейсу, не все возможные значения x в диапазоне от 1 до 2^{256} будут принадлежать заданной эллиптической кривой. Определить, является ли заданное квадратичное уравнение разрешимым для x можно с использованием символа Якоби. Для тех значений x, которые принадлежат заданной эллиптической кривой, всегда будет существовать два значения y. Прежде, чем приступать к поиску публичного ключа, необходимо преобразовать заданный адрес $A_Б$ в кодировку Base256. Обозначим старшие 21 байта адреса $A_Б$ как $MSB_{21}A_Б$, а младшие 4 байта адреса как $LSB_4A_Б$. Вычислить хеш-значение контрольной суммы: h = SHA-256(SHA-256($MSB_{21}A_Б$)). Сравнить младшие 4 байта полученного значения h с $LSB_4A_Б$. В случае совпадения этих значений, признать адрес правильным и приступить к поиску публичного ключа. В общем случае алгоритм поиска публичного ключа будет выглядеть следующим образом.

Алгоритм 2:

1. Для всех x от 1 до 2^{256} – 1:
   - 1.1. Определить значение символа Якоби.
   - 1.2. Если символ Якоби не равен 1, то вернуться к шагу 1.
   - 1.3. Определить значения y_1 и y_2.
   - 1.4. Вычислить h1 = SHA-256(x||y_1).
   - 1.5. Вычислить h2 = RIPEMD-160(h1).
   - 1.6. Если (00||h2) = $MSB_{21}A_Б$, то решение точка (x||y_1).
   - 1.7. Если (6F||h2) = $MSB_{21}A_Б$, то решение точка (x||y_1).
   - 1.8. Если (34||h2) = $MSB_{21}A_Б$, то решение точка (x||y_1).
   - 1.9. Вычислить h1 = SHA-256(x||y_2).
   - 1.10. Вычислить h2 = RIPEMD-160(h1).
   - 1.11. Если (00||h2) = $MSB_{21}A_Б$, то решение точка (x||y_2).
   - 1.12. Если (6F||h2) = $MSB_{21}A_Б$, то решение точка (x||y_2).
   - 1.13. Если (34||h2) = $MSB_{21}A_Б$, то решение точка (x||y_2).

В общей сложности потребуется 2^{258} операций хеширования для вычисления прообраза точки Q = (x, y).

Можно рассмотреть альтернативный вариант поиска на основе использования метода «встреча посередине». В этом случае необходимо создать базу предвычисленных значений, по которой будет осуществляется поиск. Сложность данному алгоритму будет добавлять необходимость хранения большой базы предвычисленных данных.

Алгоритм 3:

1. Для всех x от 1 до 2^{256} – 1:
   - 1.1. Определить значение символа Якоби.
   - 1.2. Если символ Якоби не равен 1, то вернуться к шагу 1.

1.3. Определить значения y_1 и y_2.
1.4. Вычислить h1 = SHA-256(x||y_1). Сохранить в Базе1 значения (x||y_1, h1).
1.5. Вычислить h2 = SHA-256(x||y_2). Сохранить в Базе1 значения (x||y_2, h2).
1.6. Вычислить h3 = RIPEMD-160(x).
1.7. Если (00||h3) = $MSB_{21}A_Б$, то сохранить в Базе2 значение x.
1.8. Если (6F||h3) = $MSB_{21}A_Б$, то сохранить в Базе2 значения x.
1.9. Если (34||h2) = $MSB_{21}A_Б$, то сохранить в Базе2 значения x.

2. Для всех x из Базы 2 провести сравнение со значениями h1 и h2 из Базы 1. В случае совпадения с h1 решением является точка (x||y_1) из советующей записи в Базе1. В случае совпадения с h2 решением является точка (x||y_2) из советующей записи в Базе1.

В случае использования Алгоритма 3 в общей сложности потребуется $3 * 2^{256}$ операций хеширования, а также около 2^{416} сравнений по базе. В худшем случае объем памяти, который потребуется для сохранения Базы 1 составит 2^{263}, что соответствует 10ПБ. Для сохранения Базы 2 потребуется еще дополнительно 2^{165} байт, что соответствует примерно 4ПБ. Исходя из конфигурации самого мощного суперкомпьютера мира по данным на ноябрь 2024 года (сайт top500.org), можно видеть, что в настоящее время задача поиска коллизий и прообразов является трудно вычислимой и практически не решаемой.

Выводы

В работе рассмотрен ряд кейсов, связанных с применением функций хеширования в современных блокчейн-системах. Для каждого кейса выполнено описание проблемы, сформулирована постановка задачи, приведено возможное решение и дана оценка его сложности. Показано, что при правильном использовании современных функций хеширования обеспечивается достаточная стойкость блокчейн-систем, построенных на их основе. Большинство встречающихся уязвимостей связано с ошибками реализации или ошибками применения функций хеширования внутри блокчейн-систем, а не со слабостью конструкций используемых примитивов.

Достоверность предлагаемого научного подхода подтверждается применением общенаучных методов исследования, достаточным информационным обеспечением, а также корректным применением методов криптографии, в том числе в построении формульных доказательств и выводов.

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение №23-03 от 27.09.2024 г.).

Литература

1. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System // https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf
2. Ищукова Е.А., Панасенко С.П., Романенко К.С., Салманов В.Д. Криптографические основы блокчейн-технологий. – М.: ДМК Пресс, 2022. – 300 с.
3. Er-Rajy Latifa, El Kiram My Ahemed, El Ghazouani Mohamed, Achbarou Omar Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures // Journal of Internet Banking and Commerce. – 2017. – V. 22. – n. 3.
4. Stevens, Marc & Bursztein, Elie & Karpman, Pierre & Albertini, Ange & Markov, Yarik. (2017). The First Collision for Full SHA-1. p. 570–596. DOI: 10.1007/978-3-319-63688-7_19.
5. A. Bakhtiyor, A. Orif, B. Ilkhom and K. Zarif, «Differential Collisions in SHA-1». In: 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2020, pp. 1–5, DOI: 10.1109/ICISCT50599.2020.9351441.
6. Л.К. Бабенко, Е.А. Ищукова, Дифференциальный криптоанализ упрощенной функции хэширования SHA // Известия Южного федерального университета. Технические науки, 2010. – № 11. – С. 203 – 220.
7. Lamberger, Mario & Mendel, Florian. (2011). Higher-Order Differential Attack on Reduced SHA-256. IACR Cryptology ePrint Archive. 2011. 37.
8. Wang, Fuqin & Chen, Yijiang & Wang, Ruochen & Francis, Olusegun & Bugingo, Emmanuel & Zheng, Wei & Chen, Jinjun. (2019). An Experimental Investigation Into the Hash Functions Used in Blockchains. IEEE Transactions on Engineering Management. Vol. 67. No. 4. P. 1404–1424. DOI: 10.1109/TEM.2019.2932202.
9. Ramadan, Rabie A. and khalifa, Hany. S. and Dessouky, Mohamed and Aboshosha, Bassam W., Blockchain Technology for Enhanced Security of Iot Healthcare Devices: A Novel Lightweight Hash Function Approach and Secure Management System. Available at SSRN. http://dx.doi.org/10.2139/ssrn.4680105.
10. Sevin, A.; Osman Mohammed, A.A. Comparative Study of Blockchain Hashing Algorithms with a Proposal for HashLEA. Appl. Sci. 2024, 14(24), 11967. https://doi.org/10.3390/app142411967.
11. Cojocaru, A., Garay, J., Song, F. (2025). Generalized Hybrid Search with Applications to Blockchains and Hash Function Security. In: Chung, KM., Sasaki, Y. (eds) Advances in Cryptology – ASIACRYPT 2024. ASIACRYPT 2024. Lecture Notes in Computer Science, vol 15492. Springer, Singapore. P. 65-93. https://doi.org/10.1007/978-981-96-0947-5_3.

12. Fei Teng and Yong-zhen Li, Research on application of efficient hash function in blockchain technology, International Conference on High Performance Computing and Communication (HPCCE 2021), 2022. P. 121620Y. DOI: 10.1117/12.2628073.
13. Gençoğlu, M.Tuncay. (2022). Mathematical Analysis of The Hash Functions as a Cryptographic Tools for Blockchain. Turkish Journal of Science and Technology. 2022. Vol 17. Issue 2. p. 187–201. DOI: 17. 10.55525/tjst.1140811.
14. Alfaidi A., Semwal S. (2022) Privacy Issues in mHealth Systems Using Blockchain. Advances in Information and Communication. Vol. 438. P. 877–891. DOI: 10.1007/978-3-030-98012-2_61.
15. Wang, Maoning & Duan, Meijiao & Zhu, Jianming. (2018). Research on the Security Criteria of Hash Functions in the Blockchain. 47–55. DOI: 10.1145/3205230.3205238.
16. Fu, Jinhua & Qiao, Sihai & Huang, Yongzhong & Si, Xueming & Li, Bin & Yuan, Chao. (2020). A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA. Security and Communication Networks. 2020. Vol. 8. P. 1–12. DOI: 10.1155/2020/8876317.
17. F. Jahan, M. Mostafa, S. Chowdhury. Sha-256 in parallel blockchain technology: Storing land related documents. International Journal of Computer Applications. 2020. Vol. 175. No. 35. pp. 33–38. DOI:10.5120/ijca2020920911.
18. Z.A. Kamal, R.F. Ghani, R.F. Ghani A proposed hash algorithm to use for blockchain base transaction flow system. Original Research. 2021. Vol. 9. No. 4. pp. 657–673. DOI:10.13140/RG.2.2.31831.14249.
19. A.A.M.A. Ali, M.J. Hazar, M. Mabrouk, M. Zrigui Proposal of a Modified Hash Algorithm to Increase blockchain Security Procedia Computer Science. 2023. Vol. 225. pp. 3265–3275.
20. O. Zaikin Inverting Step-Reduced SHA-1 and MD5 by Parameterized SAT Solvers // 30th International Conference on Principles and Practice of Constraint Programming. – Leibniz International Proceedings in Informatics. – 2024. Volume 307, pp. 31:1–31:19. DOI: 10.4230/LIPIcs.CP.2024.31.

ON THE INFLUENCE OF CRYPTOGRAPHIC STABILITY OF HASHING FUNCTIONS ON THE STABILITY OF MODERN BLOCKCHAIN ECOSYSTEMS AND PLATFORMS

Ishchukova E. A.[2]

Keywords: *cyber resilience, blockchain, cryptographic strength, encryption algorithm, hashing function, cryptography, cryptanalysis.*

Purpose: *the aim of this work is to systematize knowledge on hashing functions of modern blockchain ecosystems and platforms, as well as to determine the cryptographic strength of the mentioned functions in terms of the time spent on cryptanalysis.*

Method: *Методы исследования основываются на использовании теории информации, теории устойчивости, теории криптографии и криптоанализа, математического аппарата теории вероятностей и математической статистики, технологии блокчейн, технологиях обеспечения киберустойчивости и информационной безопасности.*

Results: *the paper considers the main keyless cryptographic primitives used in modern blockchain systems – hashing functions. For them, approaches to determining cryptographic resistance are considered in terms of computational costs in relation to the time of applying the exhaustive search tactic. Five different cases of using hashing functions in blockchain systems and possible attack scenarios on them are considered.*

The scientific novelty *lies in the consideration of a number of cases related to the use of hashing functions in modern blockchain systems. For each case, a description of the problem is provided, a statement of the task is formulated, a possible solution is given and an assessment of its complexity is given. It is shown that with the correct use of hashing functions, sufficient stability of blockchain systems built on their basis is ensured. Most of the vulnerabilities encountered are associated with errors in the implementation or application of hashing functions within blockchain systems, and not with the weakness of the designs of the functions used.*

References

1. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System // https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf
2. Ishchukova E.A., Panasenko S.P., Romanenko K.S., Salmanov V.D. Kriptograficheskie osnovy blokchejn-tehnologij. – M.: DMK Press, 2022. – 302 s.
3. Er-Rajy Latifa, El Kiram My Ahemed, El Ghazouani Mohamed, Achbarou Omar Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures // Journal of Internet Banking and Commerce. – 2017. – V. 22. – n. 3.
4. Stevens, Marc & Bursztein, Elie & Karpman, Pierre & Albertini, Ange & Markov, Yarik. (2017). The First Collision for Full SHA-1. p. 570–596. DOI: 10.1007/978-3-319-63688-7_19.

2 Evgeniya A. Ishchukova, Ph.D. (of Tech.), Leading researcher of the Scientific Center of Information Technologies and Artificial Intelligence of NTU Sirius. E-mail: ischukova.ea@talantiuspeh.ru, ORCID 0000-0002-6818-1608.

5. A. Bakhtiyor, A. Orif, B. Ilkhom and K. Zarif, «Differential Collisions in SHA-1», 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2020, pp. 1-5, doi: 10.1109/ICISCT50599.2020.9351441.
6. L. K. Babenko, E. A. Ishhukova, Differencial'nyj kriptoanaliz uproshhennoj funkcii hjeshirovanija SHA // Izvestija Juzhnogo federal'nogo universiteta. Tehnicheskie nauki, 2010. – № 11. – S. 203 – 220.
7. Lamberger, Mario & Mendel, Florian. (2011). Higher-Order Differential Attack on Reduced SHA-256. IACR Cryptology ePrint Archive. 2011. 37.
8. Wang, Fuqin & Chen, Yijiang & Wang, Ruochen & Francis, Olusegun & Bugingo, Emmanuel & Zheng, Wei & Chen, Jinjun. (2019). An Experimental Investigation Into the Hash Functions Used in Blockchains. IEEE Transactions on Engineering Management. PP. 1–21. DOI: 10.1109/TEM.2019.2932202.
9. Ramadan, Rabie A. and khalifa, Hany. S. and Dessouky, Mohamed and Aboshosha, Bassam W., Blockchain Technology for Enhanced Security of Iot Healthcare Devices: A Novel Lightweight Hash Function Approach and Secure Management System. Available at SSRN: https://ssrn.com/abstract=4680105 or http://dx.doi.org/10.2139/ssrn.4680105
10. Sevin, A.; Osman Mohammed, A. A. Comparative Study of Blockchain Hashing Algorithms with a Proposal for HashLEA. Appl. Sci. 2024, 14, 11967. https://doi.org/10.3390/app142411967.
11. Cojocaru, A., Garay, J., Song, F. (2025). Generalized Hybrid Search with Applications to Blockchains and Hash Function Security. In: Chung, KM., Sasaki, Y. (eds) Advances in Cryptology – ASIACRYPT 2024. ASIACRYPT 2024. Lecture Notes in Computer Science, vol 15492. Springer, Singapore. https://doi.org/10.1007/978-981-96-0947-5_3.
12. Fei Teng and Yong-zhen Li, Research on application of efficient hash function in blockchain technology, International Conference on High Performance Computing and Communication (HPCCE 2021), 2022 10.1117/12.2628073.
13. Gençoğlu, M.Tuncay. (2022). Mathematical Analysis of The Hash Functions as a Cryptographic Tools for Blockchain. Turkish Journal of Science and Technology. 17. 10.55525/tjst.1140811.
14. Alfaidi ASemwal S(2022)Privacy Issues in mHealth Systems Using BlockchainAdvances in Information and Communication. DOI: 10.1007/978-3-030-98012-2_61877-891 Online publication date: 8-Mar-2022 https://doi.org/10.1007/978-3-030-98012-2_61.
15. Wang, Maoning & Duan, Meijiao & Zhu, Jianming. (2018). Research on the Security Criteria of Hash Functions in the Blockchain. PP. 47–55. DOI: 10.1145/3205230.3205238.
16. Fu, Jinhua & Qiao, Sihai & Huang, Yongzhong & Si, Xueming & Li, Bin & Yuan, Chao. (2020). A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA. Security and Communication Networks. 2020. PP. 1–12. DOI: 10.1155/2020/8876317.
17. F. Jahan, M. Mostafa, S. Chowdhury. Sha-256 in parallel blockchain technology: Storing land related documents Int. J. Comput. Appl., 175 (35) (2020), pp. 33–38.
18. Z. A. Kamal, R. F. Ghani, R. F. Ghani. A proposed hash algorithm to use for blockchain base transaction flow system Original Research, 9 (4) (2021), pp. 657–673
19. A. A. M. A. Ali, M. J. Hazar, M. Mabrouk, M. Zrigui Proposal of a Modified Hash Algorithm to Increase blockchain Security Procedia Computer Science, 225 (2023), pp. 3265–3275.
20. O. Zaikin Inverting Step-Reduced SHA-1 and MD5 by Parameterized SAT Solvers // 30th International Conference on Principles and Practice of Constraint Programming. – Leibniz International Proceedings in Informatics. – 2024.

МОДЕЛЬ БЛОКЧЕЙН-ПЛАТФОРМЫ С КИБЕРИММУНИТЕТОМ В УСЛОВИЯХ КВАНТОВЫХ АТАК

Балябин А. А.[1], Петренко С. А.[2]

DOI: 10.21681/2311-3456-2025-3-72-82

Цель исследования: *разработка математической модели блокчейн-платформы с кибериммунитетом для исследования свойства киберустойчивости национальных блокчейн-экосистем и платформ «Экономики данных» Российской Федерации в условиях новой квантовой угрозы.*

Методы исследования: *методы системного анализа, методы теории вероятностей и математической статистики, методы теории устойчивости сложных систем.*

Полученные результаты: *проведено исследование текущего состояния технологий блокчейн; сформирована концептуальная четырехуровневая модель блокчейн-платформы, включающая уровни: криптографических алгоритмов, алгоритмов консенсуса, смарт-контрактов и децентрализованных приложений; сформулирована гипотеза об обеспечении киберустойчивости на различных уровнях блокчейн-платформы; разработана математическая модель блокчейн-платформы с кибериммунитетом для национальных блокчейн-экосистем и платформ «Экономики данных» Российской Федерации; проведена оценка киберустойчивости блокчейн-платформ с кибериммунитетом в условиях квантовых атак, результаты которой позволили подтвердить гипотезу исследования.*

Научная новизна: *предложенная модель отличается от существующих тем, что формализует процесс функционирования блокчейн-платформы как сложной многоуровневой системы с учетом нового фактора – наличия атакующего, обладающего квантовым вычислительным потенциалом, что обеспечивает возможность исследования свойства киберустойчивости блокчейн-платформ в условиях квантовых атак. К элементам новизны модели также относится введение в нее новых операций по обнаружению аномального состояния и по восстановлению штатного функционирования, которые в совокупности впервые реализуют механизмы кибериммунной защиты блокчейн-платформы.*

Ключевые слова: *угрозы безопасности информации, квантовые угрозы безопасности, блокчейн-экосистемы и платформы, кибербезопасность, киберустойчивость, методы анализа и синтеза квантово-устойчивого блокчейн.*

Введение

Активное развитие технологий блокчейн началось в 2008 году с публикации *Nakamoto S.* «*Bitcoin: A Peer-to-Peer Electronic Cash System*». В работе описывалась концепция цифровой валюты Bitcoin, использующая технологию распределенного реестра (DLT) для обеспечения безопасности транзакций без необходимости в доверенных центрах. В 2009 году был запущен первый блокчейн Bitcoin, что ознаменовало начало эры блокчейн-технологий.

В 2015 году с запуском платформы Ethereum, появились такие понятия, как смарт-контракты, токены, системы децентрализованных финансов (DeFi), децентрализованные автономные организации (DAO), децентрализованные приложения (dApps) и др. С развитием блокчейн-экосистем и платформ возникла потребность в интероперабельности – обеспечении возможности разных блокчейн-сетей обмениваться данными и активами между собой.

В работе [1] представлена схема эволюции технологий блокчейн, включающая 5 этапов. Данная схема, однако, не учитывает развитие искусственного интеллекта, квантовых вычислений, а также повышенные требования, предъявляемые к киберустойчивости значимых информационно-технических систем в условиях роста киберугроз. Авторская схема эволюции технологий блокчейн, учитывающая данные актуальные тенденции, представлена на рис. 1.

Современное состояние развития технологий блокчейн соответствует этапу «Блокчейн 4.0» и характеризуется активным внедрением данных технологий в объекты Индустрии 4.0 [2], системы интернета вещей (IoT) [3] и облачные платформы [4], а также исследованием перспектив создания децентрализованной сети Интернет (Web3) [5]. В Российской Федерации технологии блокчейн применяются в рамках реализации национального проекта «Экономика данных» с целью перевода экономики страны, социальной сферы и органов власти на новые принципы работы.

1 Балябин Артём Алексеевич, младший научный сотрудник, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Россия. E-mail: Balyabin.AA@talantiuspeh.ru

2 Петренко Сергей Анатольевич, доктор технических наук, профессор, руководитель группы, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Россия. Orcid.org/0000- 0003-0644-1731. E mail: Petrenko.SA@talantiuspeh.ru

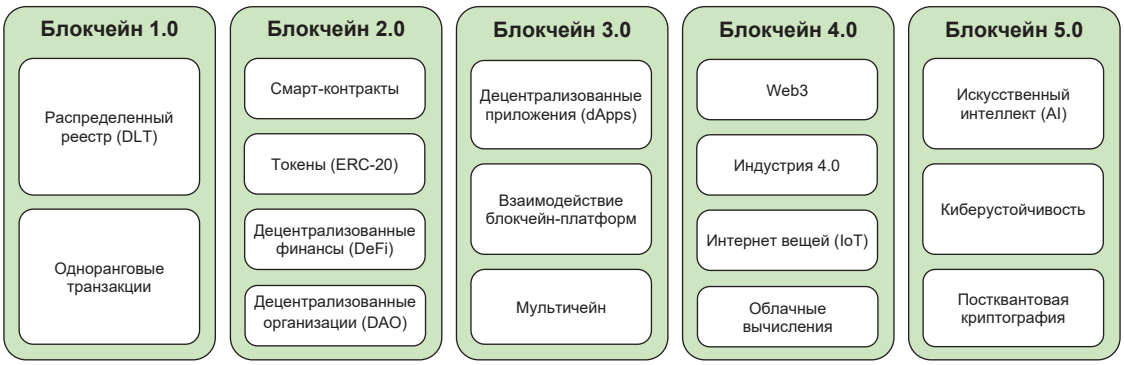


Рис. 1. Эволюция технологий блокчейн

В настоящем исследовании учитываются также и новейшие вызовы, такие как рост квантовых угроз, и предлагается модель блокчейн-платформы, отвечающей требованиям к киберустойчивости в условиях квантовых атак, в рамках следующего этапа развития технологий «Блокчейн 5.0».

1. Системный анализ блокчейн-платформ

Существует множество различных блокчейн-платформ (Bitcoin, Ethereum, Polkadot, Cardano, Solana, Tezos, EOS, Конфидент, InnoChain, Мастерчейн и др.), в каждой которых применяется свой стек технологий. Рассмотрим подробнее основные уровни блокчейн-платформ, значимые с точки зрения новой квантовой угрозы.

Фундаментом любой блокчейн-платформы являются криптографические алгоритмы хэширования (SHA-256, Ethash, Keccak, RIPEMD-160), шифрования (AES) и цифровой подписи (ECDSA). Ведутся исследования по применению в блокчейн постквантовых алгоритмов хэширования (NTRU, FrodoKEM), шифрования (FrodoKEM, Saber, BIKE, HQC, CRYSTALS-Kyber, SIKE) и цифровой подписи (CRYSTALS-Dilithium, SPHINCS+, FALCON, Picnic, Гиперикум, Шиповник, Крыжовник), устойчивых к атакам с применением квантового компьютера [6–9]. Данные криптоалгоритмы применяются для аутентификации узлов, формирования и проверки корректности транзакций и блоков и составляют основу алгоритмов консенсуса.

Следующий уровень блокчейн-платформ представлен алгоритмами консенсуса, которые необходимы для создания и проверки корректности блоков транзакций, а также согласования действий узлов. К наиболее распространенным из них относятся PoW, PoS, DPoS, BFT и PoA [10]. Алгоритмы консенсуса являются важнейшей частью блокчейн-платформы, позволяющей узлам принимать согласованное решение о добавлении в сеть нового блока.

Смарт-контракты активируются транзакциями и служат для автоматического исполнения последовательностей других транзакций (ERC-20, ERC-721, BEP-20). В своей работе они могут использовать сведения из внешнего мира, запрашиваемые у оракулов – программных или аппаратных источников данных (Chainlink, Band Protocol). Смарт-контракты служат основой для децентрализованных приложений и в то же время являются одним из самых уязвимых уровней блокчейн, поскольку подвержены, например, ошибкам численного переполнения, реентерантности и управления правами доступа [11, 12].

Уровень децентрализованных приложений (dApps) является надстройкой над смарт-контрактами, предназначенной для управления их совместным выполнением. Децентрализованные приложения также

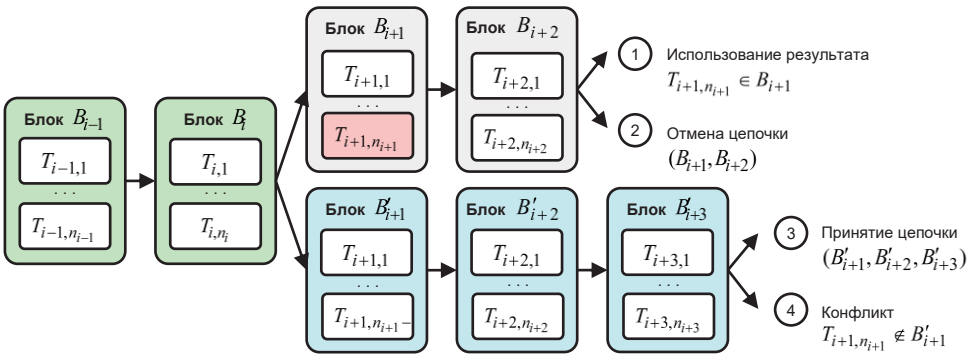


Рис. 2. Пример эмерджентного эффекта в блокчейн-платформе

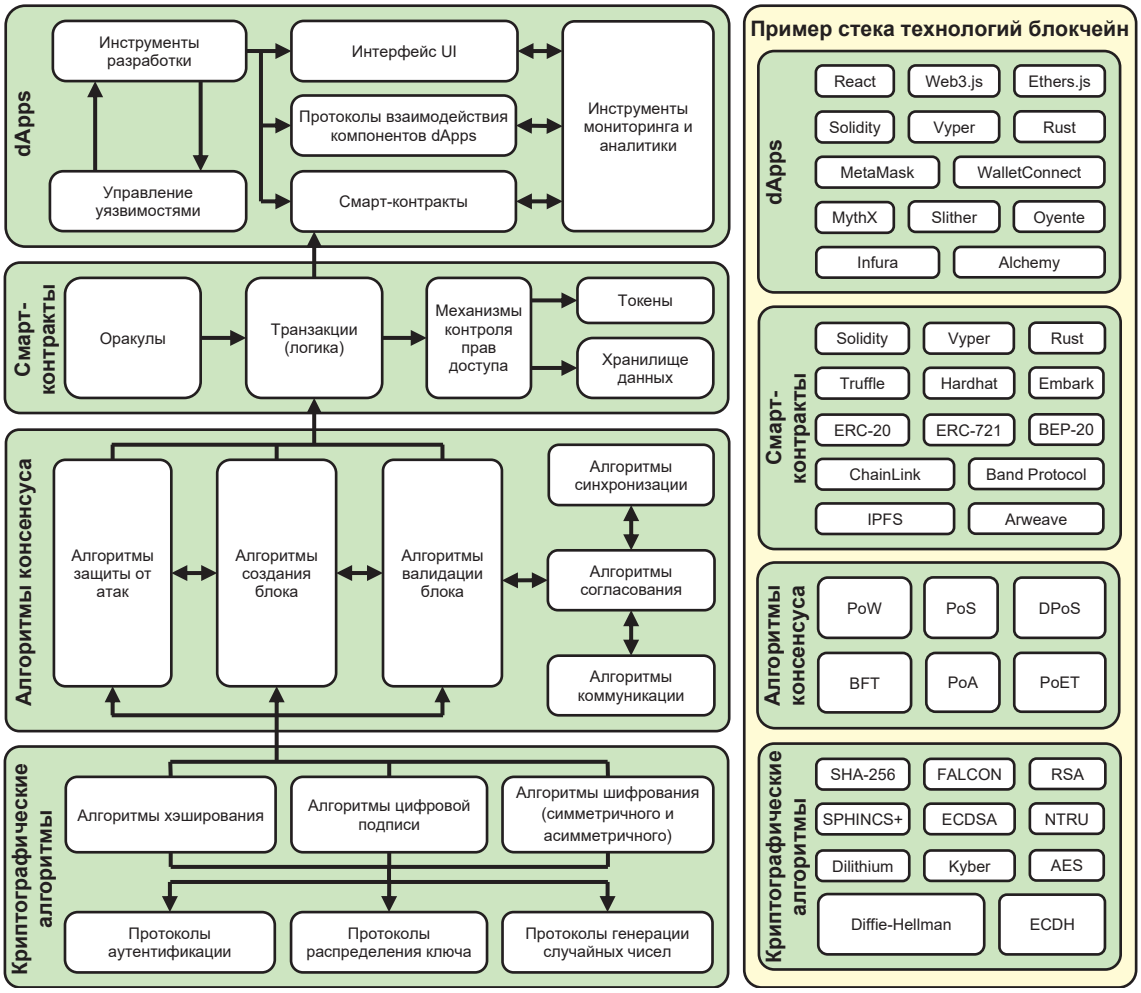


Рис. 3. Концептуальная модель блокчейн-платформы как сложной многоуровневой системы

подвержены ряду уязвимостей, в том числе уязвимостям вида «man-in-the-middle» [13, 14].

Совместное функционирование взаимосвязанных уровней блокчейн-платформы приводит к возникновению различных эмерджентных эффектов. Например, при штатном функционировании блокчейн может возникнуть следующая ситуация. Результат транзакции $T_{i+1,n_{i+1}}$, присутствующей в короткой цепочке блоков (B_{i+1}, B_{i+2}), используется для подтверждения некоторых операций. Транзакция отменяется при появлении более длинной цепочки $(B'_{i+1}, B'_{i+2}, B'_{i+3})$, в которой она отсутствует. При дальнейшем выполнении действий, опирающихся на ранее подтвержденный результат данной транзакции, возникает конфликтная ситуация, как показано на рис. 2.

Все это позволяет рассматривать блокчейн-платформу как сложную многоуровневую систему. Концептуальная четырехуровневая модель блокчейн-платформы представлена на рис. 3.

Далее необходимо определить понятие киберустойчивости блокчейн-платформ в условиях квантовых атак.

2. Квантовые атаки на блокчейн-платформы

Криптостойкость алгоритмов блокчейн, обеспечивается сложностью задач факторизации больших чисел и дискретного логарифмирования. Однако применение квантовых алгоритмов, таких как алгоритмы Шора и Гровера, позволяет значительно сократить время решения данных задач, что представляет новую угрозу для блокчейн-платформ [15].

Квантовый алгоритм Гровера предназначен для решения задачи поиска элемента в неупорядоченном множестве $\mathrm{f}:\{0,1\}^n \longrightarrow \{0,1\}$ и позволяет сократить вычислительную сложность поиска с $O(2^n)$ до $O(2^{n/2})$, где n – размерность пространства поиска в битах. Так, простой перебор 256-битной хэш-суммы SHA-256, используемой в алгоритме консенсуса PoW, будет иметь вычислительную сложность $O(2^{256})$, а с применением алгоритма Гровера – $O(2^{128})$.

Квантовый алгоритм Шора предназначен для решения задачи факторизации большого числа $N = 2^n$ и имеет полиномиальную вычислительную сложность $O(n^3)$, где n – количество бит числа. Это делает алгоритм ECDSA, основанный на сложности решения проблемы дискретного логарифмирования,

Таблица 1

Квантовые атаки на блокчейн-платформы

Уровень	Результат атаки	Последствие атаки
Децентрализованные приложения (dApps)	Обход аутентификации пользователя	Раскрытие защищенной информации (конфиденциальность) Появление в блокчейн вредоносного блока транзакций (целостность) Снижение или утрата работоспособности блокчейн-платформы (доступность)
	Фальсификация узла	
Смарт-контракты	Фальсификация данных о внешней среде (компрометация оракула)	
	Фальсификация токена	
	Нарушение логики смарт-контракта	
Алгоритмы консенсуса	Синтез произвольного блока транзакций, удовлетворяющего требованиям	
	Получение превосходства вычислительной мощности (установление контроля над сетью)	
Криптографические алгоритмы	Решение задачи факторизации большого числа	
	Решение задачи дискретного логарифмирования	
	Отыскание коллизии хэш-функции	

неустойчивым при наличии достаточного количества логических кубитов.

Квантовые атаки на блокчейн-платформу могут осуществляться на различных уровнях ее функционирования. Описание результатов и последствий квантовых атак на данных уровнях представлено в табл. 1.

Таким образом, с точки зрения нарушения свойства конфиденциальности конечная цель атаки на различные уровни блокчейн-платформы состоит в раскрытии защищенной информации, например, приватного ключа пользователя, с точки зрения нарушения свойства доступности – в снижении или нарушении работоспособности блокчейн-платформы, а с точки зрения нарушения свойства целостности – во внедрении вредоносного блока транзакций. Под вредоносным блоком, в частности, понимается блок с корректной хэш-суммой, содержащий транзакцию, противоречащую логике функционирования блокчейн-платформы, например транзакцию траты несуществующих средств. В дальнейшем в работе

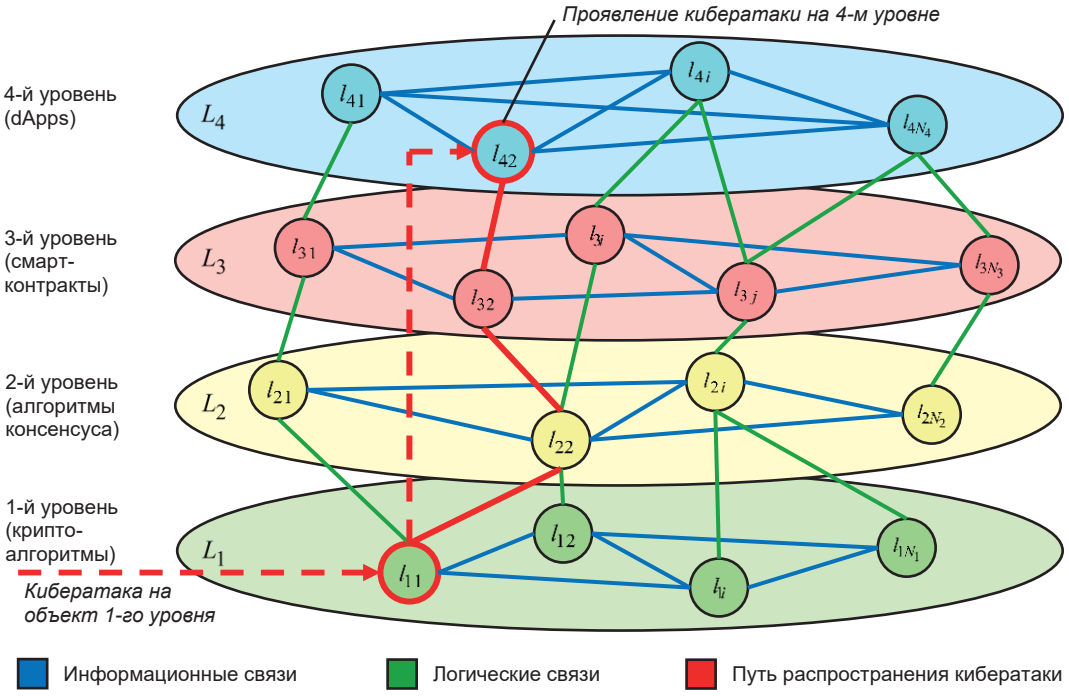


Рис. 4. Схема межуровневого отображения кибератаки на блокчейн-платформу

в основном будут подразумеваться атаки, направленные на нарушение свойства целостности.

Учитывая сложный, иерархический и децентрализованный характер блокчейн-платформы, дестабилизирующее воздействие, оказываемое на одном уровне, может проявляться на другом ее уровне, как показано на рис. 4.

Известно, что под киберустойчивостью информационно-технической системы понимается ее способность сохранять показатели своего функционирования в пределах допустимых значений в условиях дестабилизирующих воздействий (кибератак). Сформулируем определение для квантовой атаки и квантовой устойчивости блокчейн-платформы.

Определение 1. Под *квантовой атакой* на блокчейн-платформу будем понимать кибератаку, для достижения целей которой используется вычислительный потенциал квантового компьютера.

Определение 2. Под *квантовой устойчивостью блокчейн-платформы* (*киберустойчивостью в условиях квантовых атак*) будем понимать ее способность сохранять показатели своего функционирования в пределах допустимых значений в условиях дестабилизирующих воздействий (кибератак) с использованием квантового компьютера.

3. Постановка задачи исследования

Исследование возможностей обеспечения киберустойчивости блокчейн в условиях квантовых атак является перспективным научным направлением. Известны, например, работы [16, 17], посвященные организации квантово-устойчивого блокчейн с применением постквантовых криптографических алгоритмов. Одним из подходов к созданию киберустойчивых информационно-технических систем также является подход на основе кибериммунитета, заключающийся в наделении системы способностью обнаруживать аномалии и восстанавливать штатное функционирование [18–20].

Дано: L – блокчейн-платформа, функционирующая на четырех уровнях, так что $L = \{L_i | i \in [1,4]\}$; $X = \{X_i | i \in [1,4]\}$ – множество входных данных на каждом уровне; $Y = \{Y_i | i \in [1,4]\}$ – множество выходных данных на каждом уровне; $E = \{E_i | i \in [1,4]\}$ – множество параметров среды на каждом уровне; $A = \{A_i | i \in [1,4]\}$ – множество параметров дестабилизирующих воздействий на каждом уровне; $D = \{D_i | i \in [1,4]\}$ – множество параметров нейтрализующих воздействий на каждом уровне; $R = \{R_i | i \in [1,4]\}$ – множество показателей киберустойчивости функционирования блокчейн-платформы на каждом уровне.

Необходимо: разработать модель M блокчейн-платформы L с кибериммунитетом, устанавливающую закономерность изменения множества выходных данных Y и множества показателей киберустойчивости функционирования системы R от множества значений входных данных X, множества значений параметров среды E, множества значений параметров дестабилизирующих воздействий A и множества параметров нейтрализующих воздействий D. При этом на значения X, Y, E, A, D наложены условия допустимости: $X \subseteq X_{\text{доп}}$, $Y \subseteq Y_{\text{доп}}$, $E \subseteq E_{\text{доп}}$, $A \subseteq A_{\text{доп}}$, $D \subseteq D_{\text{доп}}$.

Формальная постановка научной задачи: найти

$$M: <L,X,E,A,D> \longrightarrow Y, R \mid \\ \mid X \subseteq X_{\text{доп}}, Y \subseteq Y_{\text{доп}}, E \subseteq E_{\text{доп}}, A \subseteq A_{\text{доп}}, D \subseteq D_{\text{доп}}. \quad (1)$$

Гипотеза исследования: киберустойчивость блокчейн-платформы на i-м уровне может быть эффективно обеспечена только при обеспечении ее на $(i-1)$-м уровне.

4. Модель блокчейн-платформы с кибериммунитетом

4.1. Уровень криптографических алгоритмов

Формализуем модель блокчейн-платформы на уровне криптографических алгоритмов (1-й уровень):

$X_1 = (x_1, \ldots, x_{n_1})$ – входные данные, представленные последовательностью транзакций x_i, $i \in [1,n_1]$ блока, где n_1 – количество транзакций;

$Y_1 = f_1(X_1)$ – выходные данные, представленные результатом применения функции хэширования f_1 к входным данным X_1;

$A_1 = \{(x_1, \ldots, x_{i-1}, a_i, x_{i+1}, \ldots, x_{n_1}), I_{\text{атак}_1}\}$ – параметры воздействия атакующего;

$(x_1, \ldots, x_{i-1}, a_i, x_{i+1}, \ldots, x_{n_1})$ – последовательность транзакций в блоке, включая вредоносную транзакцию a_i;

$I_{\text{атак}_1}$ – степень «влияния» атакующего на 1-й уровень блокчейн-платформы (например, $I_{\text{атак}_1} = H_{\text{атак}_1}$ – скорость перебора хэш-сумм (PoW), $I_{\text{атак}_1} = S_{\text{атак}_1}$ – доля владения активами (PoS));

$E_1 = \{I_{\text{сети}_1}, C, z_1\}$ – параметры среды функционирования;

$I_{\text{сети}_1}$ – степень «влияния» остальных участников, за исключением атакующего, на 1-й уровень блокчейн-платформы, $I_{\text{атак}_1} < I_{\text{сети}_1}$;

$C = 2^{z_1}$ – целевая сложность перебора хэш-сумм (PoW);

z_1 – количество требуемых нулевых бит в начале хэш-суммы блока;

$D_1 = \{w_1\}$ – параметры противодействия кибератакам, где w_1 – коэффициент доверия к узлу;

$E_2 = \{I_{\text{атак}_1}, I_{\text{сети}_1}\}$ – параметры среды функционирования для 2-го уровня блокчейн-платформы;

$U_1 = \{I_{\text{атак}_1}, I_{\text{сети}_1}\}$ – показатели функционирования блокчейн-платформы;

$q_1 = I_{\text{атак}_1} / (I_{\text{атак}_1} + I_{\text{сети}_1})$ – вероятность синтеза блока атакующим быстрее сети;

$R_1 = 1 - w_1 q_1$ – показатель киберустойчивости;

$\chi_1(Y_1) = \begin{cases} 1, \text{ если } \exists a_i \in X_1 : Y_1 = f_1(X_1),\ f(a_i, B) = 1; \\ 0, \text{ иначе.} \end{cases}$ – функция выявления аномалии, где f – функция проверки корректности транзакции a_i относительно всей имеющейся цепочки блоков B.

Утверждение 1. Показатель киберустойчивости блокчейн-платформы на 1-м уровне функционирования, вычисляемый с учетом вероятности синтеза и принятия блока атакующего в качестве основного, зависит только от степени «влияния» его на блокчейн-платформу и не зависит от целевой сложности перебора C.

Доказательство. Для блокчейн-платформ типа PoS это очевидно, поскольку узел, имеющий право синтеза блока, выбирается с вероятностью, пропорциональной доле владения ($S_{\text{атак}_1}$), и не зависит от сложности перебора хэш-суммы блока:

$$R_1 = 1 - w_1 q_1 = 1 - w_1 S_{\text{атак}_1} / (S_{\text{атак}_1} + S_{\text{сети}_1}). \quad (2)$$

Для блокчейн-платформ типа PoW вероятность синтеза и принятия блока атакующего быстрее сети можно определить как:

$$R_1 = 1 - w_1 T_{\text{общ}_1} / T_{\text{атак}_1}, \quad (3)$$

где $T_{\text{общ}_1} = C / (H_{\text{атак}_1} + H_{\text{сети}_1})$ – среднее время синтеза блока сетью, включая атакующего; $T_{\text{атак}_1} = C / H_{\text{атак}_1}$ – среднее время синтеза блока атакующим. То есть:

$$R_1 = 1 - w_1 q_1 = 1 - w_1 H_{\text{атак}_1} / (H_{\text{атак}_1} + H_{\text{сети}_1}). \quad (4)$$

Ч.т.д.

Таким образом, киберустойчивость блокчейн-платформы на 1-м уровне определяется ее способностью противодействовать принятию созданного атакующим вредоносного блока.

4.2. Уровень алгоритмов консенсуса

Формализуем модель блокчейн-платформы на уровне алгоритмов консенсуса (2-й уровень):

$X_2 = (x_1, \ldots, x_{n_2})$ – входные данные, представленные последовательностью блоков транзакций x_i, $i \in [1, n_2]$, где n_2 – количество блоков в цепочке;

$Y_2 = f_2(X_2)$ – выходные данные, представленные результатом согласования (консенсуса) узлами блокчейн цепочки блоков ;

$A_2 = \{(x_1, \ldots, x_{i-1}, a_i, x_{i+1}, \ldots, x_{n_2}), I_{\text{атак}_2}\}$ – параметры воздействия атакующего;

$(x_1, \ldots, x_{i-1}, a_i, x_{i+1}, \ldots, x_{n_2})$ – цепочка блоков, включая вредоносный блок a_i;

$I_{\text{атак}_2}$ – степень «влияния» атакующего на 2-й уровень блокчейн-платформы;

$E_2 = \{I_{\text{сети}_1}, z_2, R_1\}$ – параметры среды функционирования;

$I_{\text{сети}_2}$ – степень «влияния» остальных участников, за исключением атакующего, на 2-й уровень блокчейн-платформы, $I_{\text{атак}_2} < I_{\text{сети}_2}$;

z_2 – длина цепочки блоков для принятия ее в качестве основной;

$D_2 = \{w_2\}$ – параметры противодействия кибератакам, где w_2 – коэффициент доверия к узлу;

$E_3 = \{I_{\text{атак}_2}, I_{\text{сети}_2}, R_2\}$ – параметры среды функционирования для 3-го уровня блокчейн-платформы;

$U_2 = \{P_{\text{атак}_2}, P_{\text{сети}_2}, z_2, \lambda\}$ – показатели функционирования блокчейн-платформы;

$q_2 = I_{\text{атак}_2} / (I_{\text{атак}_2} + I_{\text{сети}_2})$ – вероятность синтеза блока атакующим быстрее сети;

$P_{\text{атак}_2} = w_2 q_2$ – вероятность синтеза и принятия блока атакующего;

$P_{\text{сети}_2} = 1 - P_{\text{атак}_2}$ – вероятность синтеза и принятия блока легитимных узлов сети, за исключением атакующего, $P_{\text{атак}_2} < P_{\text{сети}_2}$;

$\lambda = z_2 \frac{P_{\text{атак}_2}}{P_{\text{сети}_2}}$ – мат. ожидание длины цепочки блоков атакующего;

$R_2 = \varphi(U_2) = \sum_{k=0}^{z_2} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (P_{\text{атак}_2} / P_{\text{сети}_2})^{z_2 - k}\right)$ – показатель киберустойчивости;

$\chi_2(Y_2) = \begin{cases} 1, \text{ если } \exists a_i \in X_2 : Y_2 = f_2(X_2),\ f(a_i, B) = 1; \\ 0, \text{ иначе.} \end{cases}$ – функция выявления аномалии, где f – функция проверки корректности блока a_i относительно всей имеющейся цепочки блоков B, принимающая значение 1 в случае, если блок содержит некорректную транзакцию.

Таким образом, киберустойчивость блокчейн-платформы на 2-м уровне определяется ее способностью противодействовать принятию созданной атакующим вредоносной цепочки блоков.

4.3. Уровень смарт-контрактов

Формализуем модель блокчейн-платформы на уровне смарт-контрактов (3-й уровень):

$X_3 = \{X_{3i} | i \in [1, n_3]\}$ – множество входных данных, где $X_{3i} = \{x_{3ij} | j \in [1, \#X_{3i}]\}$, $i \in [1, n_3]$ – множество входных данных i-го смарт-контракта, n_3 – количество смарт-контрактов, при этом $X_{3i} = X_{3i}^{+} \cup X_{3i}^{-}$, где X_{3i}^{-} – подмножество вредоносных входных данных;

$Y_3 = f_3(X_3) = \{y_{3i} | y_{3i} = f_{3i}(x_{3i}),\ i \in [1, n_3]\}$ – выходные данные, представленные результатом выполнения смарт-контрактов с входными данными x_3, f_{3i} – функция i-го смарт-контракта;

$A_3 = (a_{31}, \ldots, a_{3n_3})$ – параметры воздействия, представленные вредоносными входными данными, передаваемыми атакующим в смарт-контракты, $a_{3i} \in X_{3i}^{-}$;

$E_3 = \{(\#X_{31}, \#X_{31}^{-}), \ldots, (\#X_{3n_3}, \#X_{3n_3}^{-}), R_2\}$ – параметры среды функционирования;

$D_3 = (D_{3i} | i \in [1, n_3])$ – параметры противодействия кибератакам, где $\{d_{3ij} | j \in [1, \#D_{3i}]\}$, $\#D_{3i} \in [0, \#X_{3i}^{-}]$, $i \in [1, n_3]$ – множество обнаруженных и заблокированных вредоносных входных данных i-го смарт-контракта;

$E_4 = \{\{P_{3i}^{a} | i \in [1, n_3]\}, R_3\}$ – параметры среды функционирования для 4-го уровня блокчейн-платформы;

$U_3 = \{P^a_{3i} | i \in [1,n_3]\}$ – показатели функционирования блокчейн-платформы;

$P^a_{3i} = P(S^a_{3i}) = (\#X^-_{3i} - \#D_{3i}) / \#X_{3i}$ – вероятность нарушения в i-м смарт-контракте (событие S^a_{3i});

$R_3 = \varphi(U_3) = R_2 \frac{1}{n_3} \sum_{i=1}^{n_3} (1 - P^a_{3i})$ – показатель киберустойчивости;

$\chi_3(Y_3) = \begin{cases} 1, \text{ если } \exists y'_{3i} \in Y_3 : f(x_{3i}, y'_{3i}) = 1; \\ 0, \text{ иначе.} \end{cases}$ – функция выявления аномалии, где f –функция проверки корректности результата выполнения смарт-контракта.

Таким образом, киберустойчивость блокчейн-платформы на 3-м уровне определяется ее способностью противодействовать выполнению смарт-контрактов с вредоносными входными данными.

4.4. Уровень децентрализованных приложений

Формализуем модель блокчейн-платформы на уровне децентрализованных приложений (dApps) (4-й уровень):

$X_4 = \{X_{4i} | i \in [1,n_4]\}$ – множество входных данных, где $X_{4i} = \{X_{4ij} | j \in [1,\#X_{4i}]\}$, $i \in [1,n_4]$ – множество входных данных i-го приложения, n_4 – количество приложений, при этом $X_{4i} = X^+_{4i} \cup X^-_{4i}$, где X^-_{4i} – подмножество вредоносных входных данных;

$Y_4 = f_4(X_4) = \{y_{4i} | y_{4i} = f_{4i}(x_{4i}),\ i \in [1,n_4]\}$ – выходные данные, представленные результатом выполнения приложений с входными данными X_4, f_{4i} – функция i-го приложения;

$A_4 = (a_{41}, ..., a_{4n_4})$ – параметры воздействия атакующего, представленные вредоносными входными данными, передаваемыми атакующим в приложения, $a_{4i} \in X^-_{4i}$;

$E_4 = \{\{P^a_{3i} | i \in [1,n_3]\}, R_3, (X_{41}, X^-_{41}), ..., (X_{4n_4}, X^-_{4n_4})\}$ – параметры среды функционирования блокчейн-платформы;

$D_4 = (D_{4i} | i \in [1,n_4])$ – параметры противодействия кибератакам, где $\{d_{4ij} | j \in [1,\#D_{4i}]\}$, $\#D_{4i} \in [0,\#X^-_{4i}]$, $i \in [1,n_4]$ – множество обнаруженных и заблокированных вредоносных входных данных i-го приложения;

$U_4 = \{P^a_{4i} | i \in [1,n_4]\}$ – показатели функционирования блокчейн-платформы на, где $P^a_{4i} = P(S^a_{4i})$ – вероятность нарушения в i-м приложении, вызванного обработкой вредоносных входных данных a (событие S^a_{4i});

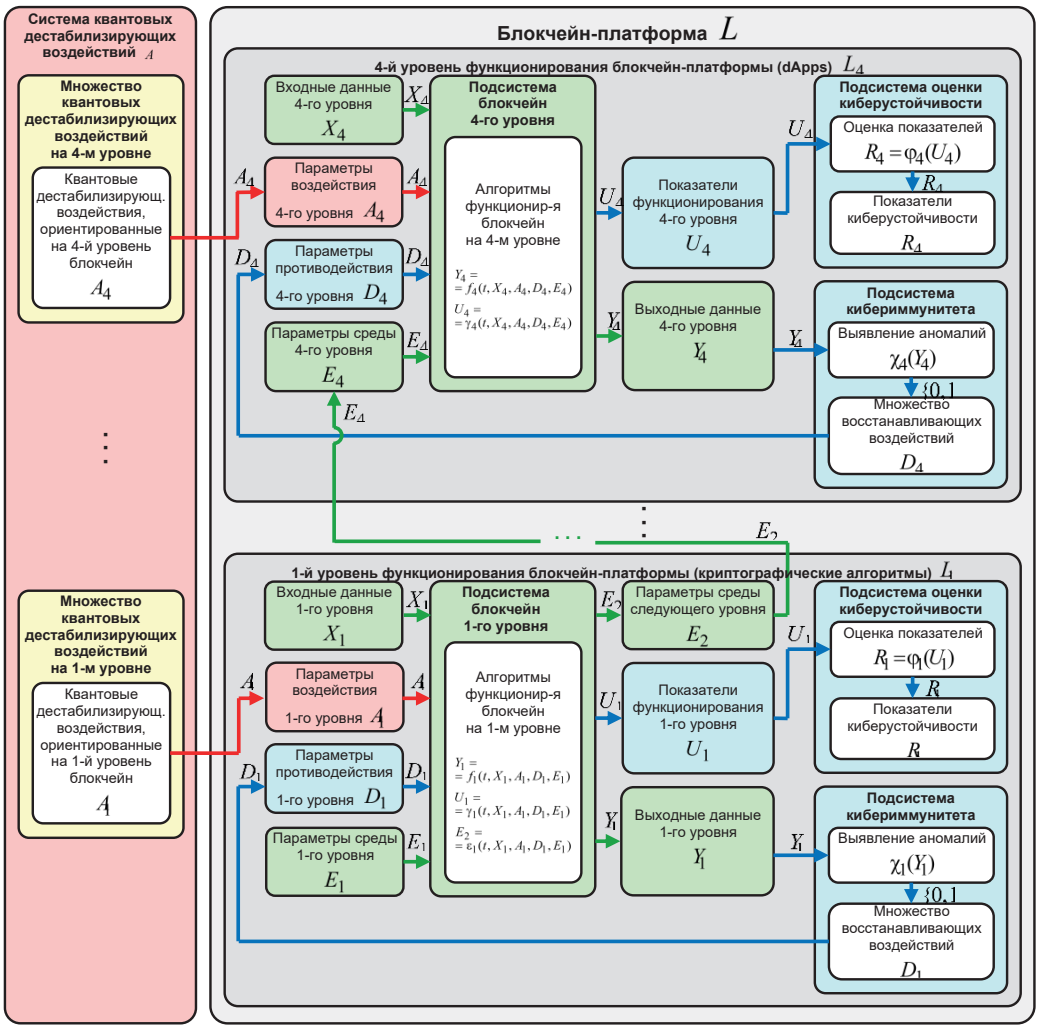


Рис. 5. Многоуровневая модель блокчейн-платформы в условиях квантовых атак

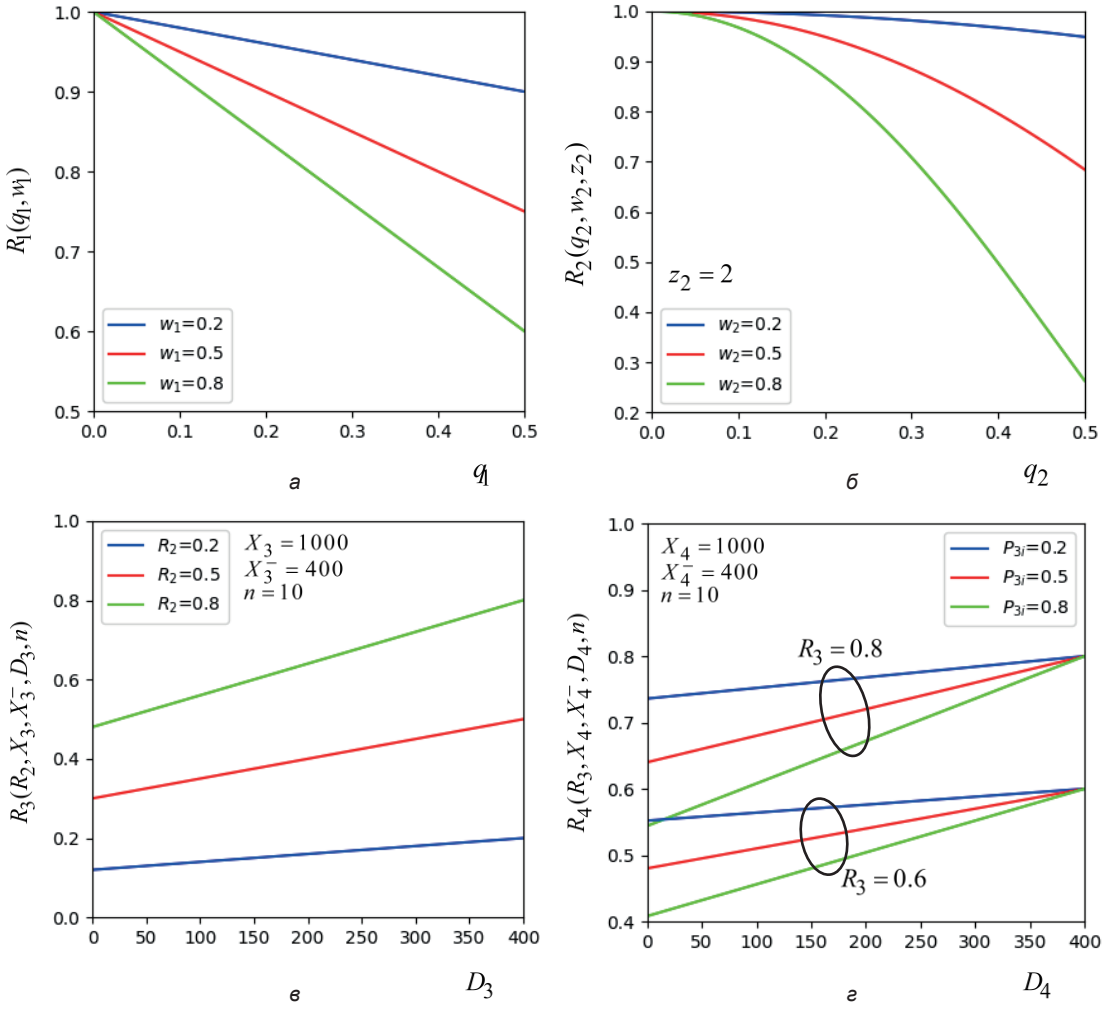


Рис. 6. Результаты экспериментальных исследований киберустойчивости: а – на 1-м уровне (криптоалгоритмов); б – на 2-м уровне (алгоритмов консенсуса); в – на 3-м уровне (смарт-контрактов); г – на 4-м уровне (децентрализованных приложений, dApps)

$P_{4i}^a = P(S_{4i}^a) = \frac{(\#X_{4i}^- - \#D_{4i})}{\#X_{4i}} \frac{1}{l_i} \sum_{r=1}^{l_i} P_{3ir}^a$ – вероятность нарушения в i-м приложении, состоящем из l_i смарт-контрактов, где P_{3ir}^a – вероятность нарушения в i-м смарт-контракте $r \in [1, l_i]$.

$R_4 = \varphi(U_4) = R_3 \frac{1}{n_4} \sum_{i=1}^{n_4} (1 - P_{4i}^a)$ – показатель киберустойчивости;

$\chi_4(Y_4) = \begin{cases} 1, \text{ если } \exists y'_{4i} \in Y_4 : f(x_{4i}, y'_{4i}) = 1; \\ 0, \text{ иначе.} \end{cases}$ – функция выявления аномалии, где f – функция проверки корректности результата выполнения децентрализованного приложения, принимающая значение 1 в случае, если результат некорректен, и 0 – иначе.

Таким образом, киберустойчивость блокчейн-платформы на 4-м уровне определяется ее способностью противодействовать выполнению децентрализованных приложений с вредоносными входными данными.

4.5. Многоуровневая модель блокчейн-платформы

Схема многоуровневой модели блокчейн-платформы в условиях квантовых атак представлена на рис. 5.

Учитывая сложный многоуровневый характер блокчейн-платформ, при выполнении практических расчетов можно оценивать лишь показатель киберустойчивости верхнего уровня, представляющий собой свертку: $R_1 \longrightarrow R_2 \longrightarrow R3_1 \longrightarrow R_4$.

5. Исследование квантовой устойчивости блокчейн-платформ с кибериммунитетом

Результаты экспериментальных исследований квантовой устойчивости блокчейн-платформы на различных уровнях функционирования приведены на рис. 6.

Киберустойчивость блокчейн-платформы в условиях квантовых атак на 1-м уровне снижается по мере увеличения вероятности q_1 того, что атакующий создаст вредоносный блок раньше остальной сети и этот блок будет принят в блокчейн. Противодействие принятию вредоносного блока оказывается с помощью снижения коэффициента доверия w_1 к атакующему узлу (рис. 6а).

На 2-м уровне киберустойчивость также зависит от вероятности принятия вредоносного блока q_2 и коэффициента доверия w_2, однако наблюдается нелинейная зависимость, поскольку атакующему необходимо синтезировать цепочку из z_2 блоков и «убедить» остальную сеть принять ее (рис. 6б).

На 3-м уровне киберустойчивость зависит от количества обнаруженных и нейтрализованных вредоносных входных данных D_3. Как видно, при нейтрализации все большего количества вредоносных входных данных значение показателя киберустойчивости уровня смарт-контрактов стремится к значению показателя предыдущего уровня R_2 (рис. 6в).

На 4-м уровне киберустойчивость оценивалась аналогично предыдущему уровню для двух различных значений R_3 с учетом вероятностей P_{3i} возникновения нарушений в смарт-контрактах, составляющих децентрализованные приложения. Показатель киберустойчивости R_4 при этом так же стремится к значению R_3 (рис. 6г).

Таким образом:

- в блокчейн-платформе существуют межуровневые связи, что характеризует ее как сложную многоуровневую систему;
- кибератака, осуществляемая на нижележащем уровне, оказывает влияние на все вышележащие уровни блокчейн-платформы;
- киберустойчивость на i-м уровне может быть эффективно обеспечена только при условии обеспечения ее на $(i-1)$-м уровне.

Результаты экспериментальных исследований позволяют подтвердить выдвинутую гипотезу.

Выводы

В настоящем исследовании поставлена задача синтеза математической модели блокчейн-платформы с кибериммунитетом в условиях квантовых атак. Проведен системный анализ и сформирована концептуальная четырехуровневая модель блокчейн-платформы, включающая уровни: криптографических алгоритмов, алгоритмов консенсуса, смарт-контрактов и децентрализованных приложений. Выдвинута гипотеза об обеспечении киберустойчивости на различных уровнях блокчейн-платформы. Разработана многоуровневая модель блокчейн-платформы с кибериммунитетом, отличающаяся от существующих учетом наличия атакующего, обладающего квантовым вычислительным потенциалом, и внедрением новых операций по обнаружению аномалий и восстановлению штатного функционирования системы.

В результате экспериментов выявлен ряд количественных закономерностей снижения киберустойчивости блокчейн-экосистем и платформ «Экономики данных» РФ в условиях атак злоумышленников с применением квантового компьютера, что позволило подтвердить выдвинутую гипотезу.

В дальнейшем результаты исследования будут использованы для синтеза методов и методик обеспечения киберустойчивости блокчейн-платформ в условиях квантовых атак на основе кибериммунитета.

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение №23-03 от 27.09.2024 г.).

Литература

1. Mourtzis D., Angelopoulos J., Panopoulos N. Blockchain Integration in the Era of Industrial Metaverse // Applied Sciences. 2023. Vol. 13. No. 3. P. 1353. DOI: 10.3390/app13031353.
2. Марков А.С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. 2023. № 1(53). С. 2–12. DOI: 10.21681/2311-3456-2023-1-2-12.
3. Nguyen D.C. et al. 6G Internet of Things: A Comprehensive Survey // IEEE Internet of Things Journal. 2022. Vol. 9. No. 1. Pp. 359–383. DOI: 10.1109/JIOT.2021.3103320.
4. Балябин А.А., Петренко С.А., Костюков А.Д. Модель угроз безопасности и киберустойчивости облачных платформ КИИ РФ // Защита информации. Инсайд. 2024. № 5 (119). С. 26–34.
5. Chen C. et al. When Digital Economy Meets Web3.0: Applications and Challenges // IEEE Open Journal of the Computer Society. 2022. Vol. 3. Pp. 233–245. DOI: 10.1109/OJCS.2022.3217565.
6. Петренко А.С., Ломако А.Г., Петренко С.А. Анализ современного состояния исследований проблемы квантовой устойчивости блокчейна. Часть 1 // Защита информации. Инсайд. 2023. № 3 (111). С. 38–46.
7. Петренко А.С., Петренко С.А., Костюков А.Д. Эталонная модель блокчейн-платформы // Защита информации. Инсайд. 2022. № 4 (106). С. 34–44.
8. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн-платформ // Вопросы кибербезопасности. 2022. № 3(49). С. 2–22. DOI: 10.21681/2311-3456-2022-3-2-22.
9. Петренко А.С., Петренко С.А. Basic Algorithms Quantum Cryptanalysis (Основные алгоритмы квантового криптоанализа) // Вопросы кибербезопасности. 2023. № 1(53). С. 100–115. DOI: 10.21681/2311-3456-2023-1-100-115.

10. Lashkari B., Musilek P. A Comprehensive Review of Blockchain Consensus Mechanisms // IEEE Access. 2021. Vol. 9. Pp. 43620–43652. DOI: 10.1109/ACCESS.2021.3065880.
11. Zou W. et al., Smart Contract Development: Challenges and Opportunities // IEEE Transactions on Software Engineering. 2021. Vol. 47. No. 10. Pp. 2084–2106. DOI: 10.1109/TSE.2019.2942301.
12. Kushwaha S.S., Joshi S., Singh D., Kaur M. Lee H.-N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract // IEEE Access. 2022. Vol. 10. Pp. 6605–6621. DOI: 10.1109/ACCESS.2021.3140091.
13. Маркова С.В. Выявления уязвимостей в децентрализованных информационных системах на основе смарт-контрактов с помощью методов обработки больших данных // Фундаментальные исследования. 2022. № 9. С. 47–53.
14. Zheng P., Jiang Z., Wu J., Zheng Z. Blockchain-Based Decentralized Application: A Survey // IEEE Open Journal of the Computer Society. 2023. Vol. 4. Pp. 121–133. DOI: 10.1109/OJCS.2023.3251854.
15. Петренко А.С., Романченко А.М. Перспективный метод криптоанализа на основе алгоритма Шора // Защита информации. Инсайд. 2020. № 2(92). С. 17–23.
16. Петренко А.С. Квантово-устойчивый блокчейн: научная монография // Санкт-Петербург: Питер, 2023. 384 с.
17. Fernandez-Carames T.M., Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks // IEEE Access. 2020. Vol. 8. Pp. 21091–21116. DOI: 10.1109/ACCESS.2020.2968985.
18. Петренко С.А. Киберустойчивость Индустрии 4.0: научная монография // «Издательский Дом «Афина». 2020. 256 с.
19. Балябин, А.А. Модель облачной платформы КИИ РФ с кибериммунитетом в условиях информационно-технических воздействий // Защита информации. Инсайд. 2024. № 5(119). С. 35–44.
20. Балябин А.А., Петренко С.А., Костюков А. Д. Метод восстановления облачных и пограничных вычислений на основе кибериммунитета // Защита информации. Инсайд. 2022. № 6(108). С. 26–31.

MODEL OF A BLOCKCHAIN PLATFORM WITH CYBER-IMMUNITY UNDER QUANTUM ATTACKS

Balyabin A.A.[3], Petrenko S.A.[4]

Keywords: *threats to information security, quantum threats to security, blockchain ecosystems and platforms, cybersecurity, cyber resilience, methods of analysis and synthesis of quantum-resistant blockchain.*

Purpose of work *is to review new aspects for the task of information extraction from ensembles of quantum states, dictated by practical tasks of quantum cryptography.*

Research methods: *mathematical methods of quantum information theory, in particular, unambiguous discrimination of quantum states.*

Results of the study: *the paper analyzes the literature on the topic of eavesdropper information bounds in quantum cryptography in the presence of channel attenuation, including in the absence of quantum memory. The features of application of the fundamental information bound to the eavesdropper information in the presence of attenuation, the threats of application of ad hoc countermeasures for unambiguous state discrimination attack are demonstrated. The problems of finding an effective postselective eavesdropping transformation, as well as measurement in the absence of eavesdropper's quantum memory, are formulated.*

Scientific novelty: *the scientific novelty consists in the integration of disparate approaches to the problem of eavesdropper information bounds in quantum cryptography and resisting attacks in case of lossy channel. The review describes the peculiarities of applying information bound to quantum cryptography problems and formalizes the challenges facing the eavesdropper under attenuation conditions.*

References

1. Mourtzis D., Angelopoulos J., Panopoulos N. Blockchain Integration in the Era of Industrial Metaverse // Applied Sciences. 2023. Vol. 13. No. 3. P. 1353. DOI: 10.3390/app13031353.
2. Markov A.S. Vazhnaya vekha v bezopasnosti otkrytogo programmnogo obespecheniya // Voprosy kiberbezopasnosti. 2023. № 1 (53). Pp. 2–12. DOI: 10.21681/2311-3456-2023-1-2-12.
3. Nguyen D.C. et al. 6G Internet of Things: A Comprehensive Survey // IEEE Internet of Things Journal. 2022. Vol. 9. No. 1. Pp. 359–383. DOI: 10.1109/JIOT.2021.3103320.
4. Balyabin A.A., Petrenko S.A., Kostyukov A.D. Model' ugroz bezopasnosti i kiberustoychivosti oblachnykh platform KII RF // Zashchita informatsii. Insayd. 2024. № 5 (119). Pp. 26–34.
5. Chen C. et al. When Digital Economy Meets Web3.0: Applications and Challenges // IEEE Open Journal of the Computer Society. 2022. Vol. 3. Pp. 233–245. DOI: 10.1109/OJCS.2022.3217565.

3 Artyom A. Balyabin, Junior Researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, E-mail: Balyabin.AA@talantiuspeh.ru

4 Sergei A. Petrenko, Dr.Sc. (in Tech.) (Grand Doctor, Full Professor), Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Orcid.org/0000- 0003-0644-1731, E-mail: Petrenko.SA@talantiuspeh.ru

6. Petrenko A. S., Lomako A. G., Petrenko S. A. Analiz sovremennogo sostoyaniya issledovaniy problemy kvantovoy ustoychivosti blokcheyna. Chast' 1. // Zashchita informatsii. Insayd. 2023. № 3(111). Pp. 38–46.
7. Petrenko A. S., Petrenko S. A., Kostyukov A. D. Etalonnaya model' blokcheyn-platformy // Zashchita informatsii. Insayd. 2022. № 4(106). Pp. 34–44.
8. Petrenko A. S., Petrenko S. A. Metod otsenivaniya kvantovoy ustoychivosti blokcheyn-platform // Voprosy kiberbezopasnosti. 2022. № 3(49). Pp. 2–22. DOI 10.21681/2311-3456-2022-3-2-22.
9. Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis // Voprosy Kiberbezopasnosti. 2023. No. 1 (53). Pp. 100–115. DOI 10.21681/2311-3456-2023-1-100-115.
10. Lashkari B., Musilek P. A Comprehensive Review of Blockchain Consensus Mechanisms // IEEE Access. 2021. Vol. 9. Pp. 43620–43652. DOI: 10.1109/ACCESS.2021.3065880.
11. Zou W. et al., Smart Contract Development: Challenges and Opportunities // IEEE Transactions on Software Engineering. 2021. Vol. 47. No. 10. Pp. 2084–2106. DOI: 10.1109/TSE.2019.2942301.
12. Kushwaha S. S., Joshi S., Singh D., Kaur M. Lee H.-N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract // IEEE Access. 2022. Vol. 10. Pp. 6605–6621. DOI: 10.1109/ACCESS.2021.3140091.
13. Markova S. V. Vyyavleniya uyazvimostey v detsentralizovannykh informatsionnykh sistemakh na osnove smart-kontraktov s pomoshch'yu metodov obrabotki bol'shikh dannykh // Fundamental'nye issledovaniya. 2022. № 9. Pp. 47–53.
14. Zheng P., Jiang Z., Wu J., Zheng Z. Blockchain-Based Decentralized Application: A Survey // IEEE Open Journal of the Computer Society. 2023. Vol. 4. Pp. 121–133. DOI: 10.1109/OJCS.2023.3251854.
15. Petrenko A. S., Romanchenko A. M. Perspektivnyy metod kriptoanaliza na osnove algoritma Shora // Zashchita informatsii. Insayd. 2020. № 2(92). Pp. 17–23.
16. Petrenko A. S. Kvantovo-ustoychivyy blokcheyn: nauchnaya monografiya. // Sankt-Peterburg : Piter, 2023. 384 p.
17. Fernandez-Carames T. M., Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks // IEEE Access. 2020. Vol. 8. Pp. 21091–21116. DOI: 10.1109/ACCESS.2020.2968985.
18. Petrenko S. A. Kiberustoychivost' Industrii 4.0: nauchnaya monografiya // «Izdatel'skiy Dom «Afina». 2020. 256 p.
19. Balyabin A. A. Model' oblachnoy platformy KII RF s kiberimmunitetom v usloviyakh informatsionno-tekhnicheskikh vozdeystviy // Zashchita informatsii. Insayd. 2024. № 5(119). Pp. 35–44.
20. Balyabin A. A., Petrenko S. A., Kostyukov A. D. Metod vosstanovleniya oblachnykh i pogranichnykh vychisleniy na osnove kiberimmuniteta // Zashchita informatsii. Insayd. 2022. № 6(108). Pp. 26–31.

ФУНКЦИОНАЛЬНАЯ УСТОЙЧИВОСТЬ РАСПРЕДЕЛЕННОГО РЕЕСТРА В УСЛОВИЯХ ПОЯВЛЕНИЯ НОВОЙ КВАНТОВОЙ УГРОЗЫ

Сундеев П. В.[1]

DOI: 10.21681/2311-3456-2025-3-83-89

Цель исследования: *предложить подход к формальному анализу функциональной устойчивости или стабильности систем распределенного реестра для критических приложений в условиях появления новой квантовой угрозы.*

Методы исследования: *объектно-ориентированный анализ и синтез сложных систем, системный анализ, теория модульно-кластерных сетей, теория графов, теория матриц, математическая логика.*

Результаты исследования: *показано влияние безопасности архитектуры и политики доступа на функциональную стабильность распределенного реестра в условиях квантовой угрозы, предложена концепция и постановка задачи анализа безопасности архитектуры распределенного реестра в терминах теории модульно-кластерных сетей, подход к синтезу архитектуры с доказанными свойствами безопасности.*

Научная новизна: *применение теории модульно-кластерных сетей к анализу функциональной стабильности систем распределенного реестра в аспекте безопасности с учетом влияния квантовой угрозы.*

Ключевые слова: *модульно-кластерная сеть, системный анализ, безопасность.*

Введение

Технология распределенного реестра (DLT – Distributed ledger technologies) имеет децентрализованную архитектуру и предназначена для безопасного взаимодействия недоверенных субъектов на основе процедуры консенсуса без участия посредников [1–4]. В частных случаях централизованной или гибридной архитектуры предусмотрены администраторы и посредники, что позволяет контролировать систему, но создает дополнительные риски для участников взаимодействия. Национальные распределенные реестры могут попадать под действие законодательства о критической информационной инфраструктуре [5]. В условиях конкурентной среды на функциональную стабильность критической системы, кроме свойств надежности, производительности, функциональности и т.д., влияет безопасность, нарушение которой может быть целью внешних нарушителей, взаимодействующих субъектов и администраторов. Особенность архитектуры DLT – конструктивная реализация принципа «Secure by Design» на основе криптографии. Однако перспектива резкого увеличения скорости вычислений при появлении промышленных квантовых компьютеров создает неприемлемый для критических приложений риск компрометации неидеальной криптографии [6]. Поэтому для обеспечения доверия к системам распределенного реестра (DLTS – DLT System) необходимо формально оценивать безопасность архитектуры с учетом стойкости криптографии к квантовой угрозе.

В статье предложен системный подход к анализу архитектуры DLTS с формальным доказательством безопасности в условиях квантовой угрозы на основе методов теории модульно-кластерных сетей (МК-сетей) [7].

Особенности защиты информации в DLT

Функциональную стабильность в аспекте безопасности обеспечивают:

- политика разграничения доступа (ACP – Access Control Policy);
- конструктивная безопасность архитектуры (SBD – Secure By Design);
- надежность средств реализации ACP (MAC – Means of Access Control);
- безопасная обработка данных (SDP – Secure Data Processing).

При анализе безопасности архитектуры существенны первые три фактора.

ACP должен установить «собственник информации» с учетом собственной оценки ущерба из-за нарушения безопасности информации. Однако в законодательстве отсутствует понятие «собственник информации». Легитимно более широкое понятие «обладатель информации» [8], которое включает иные категории субъектов информационных отношений, имеющих правомерный доступ к информации. В условиях конкурентной среды и критичности системы такие субъекты должны включаться в модель угроз как потенциальные нарушители. Архитектура систем реализующих ACP в парадигме «обладатель информации», опасна для собственника из-за доступа к информации посредников, администраторов

1 Сундеев Павел Викторович, доктор технических наук, главный инженер-исследователь Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Россия. E-mail: sundeev.pv@talantiuspeh.ru

и т.п. Архитектура DLT в «классическом» исполнении конструктивно включает функционал защиты, который не позволяет вносить изменения в данные, переданные и зарегистрированные в реестре, что обеспечивает доверие участников к их целостности в условиях отсутствия доверия друг к другу. При этом актуальна угроза конфиденциальности [9].

Безопасная архитектура предполагает наличие в ней МАС, реализующих АСР. Состав функций защиты в DLTS зависит от конфигурации архитектуры и организации процесса обработки данных с учетом актуальных угроз безопасности информации и может включать идентификацию и аутентификацию субъектов и объектов доступа, авторизацию, шифрование, физическую защиту носителей и т.д., наличие и надежность которых необходимо учитывать при формальном анализе [3,4]. При анализе безопасности архитектуры DLT необходимо учитывать надежность МАС, в частности, учитывать риск компрометации неидеальной криптографии, которая является основой конструктивной безопасности архитектуры, в условиях квантовой угрозы.

Концепция анализа безопасности архитектуры DLT методами МК-сетей

Для формального анализа архитектура DLT представляется в виде объектно-ориентированной информационной модели в терминах теории МК-сетей [7]. «Классическая» архитектура DLT [1] представляет собой МК-сеть в виде полного ациклического маркированного регулярного ориентированного мультиграфа $G^{FLS}(M_N,R_M^{FLS})$, вершины которого обозначают функциональные модули M_P (P – число модулей) и модули защиты M_D (D – число МАС), где $M_P \cup M_D = M_N$ и $M_P \cap M_D = \varnothing$, а дуги R_M^{FLS} обозначают физические (F), синтаксические (L) и семантические (S) FLS интерфейсы модулей, которые определяют возможность информационных отношений между модулями.

Определение 1. Модульно-кластерная сеть – это FLS мультиграф $G^{FLS}(M_N,R_Q^{FLS})$, вершинами которого являются функционально-информационные модули $M_N = \{m_1, m, \ldots, m_n\}$, где N – их число, а дуги $R_M^{FLS} = \{R^F \cup R^L \cup R^S\}$ (где $R^F = \{r_x^F\}$, $R^L = \{r_y^L\}$, $R^S = \{r_z^S\}$) определяются наличием у модулей FLS-интерфейсов, через которые устанавливаются функционально-информационные отношения.

Мультиграф $G^{FLS}(M_N,R_M^{FLS})$ состоит из F, L и S остовных подграфов (или просто FLS-подграфов), у которых вершины совпадают и соответствуют множеству $M_N = \{m_1, m, \ldots, m_n\}$, а инцидентные им дуги различаются и определяются соответственно множествами $R^F = \{r_x^F\}$, $R^L = \{r_y^L\}$, $R^S = \{r_z^S\}$, отражающими FLS отношения между модулями.

Упрощенный фрагмент мультиграфа $G^{FLS}(M_N,R_M^{FLS})$ и его декомпозиция на остовные FLS подграфы представлены на (рис. 1).

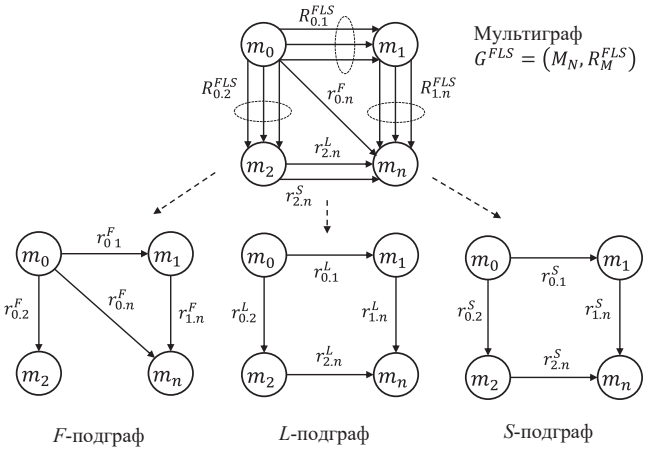


Рис. 1. Фрагмент мультиграфа $G^{FLS}(M_N,R_M^{FLS})$ МК-сети и его декомпозиция на остовные FLS-подграфы

Фрагмент мультиграфа на рис. 1 содержит два пути $P_{0.2}^{FLS} = \{R_{0,2}^{FLS}\}$ и $P_{0.n}^{FLS} = \{R_{0,1}^{FLS}, P_{1.n}^{FLS}\}$, по которым возможна реализация информационного процесса.

Декомпозиция элементов множества дуг $R_M \longrightarrow R_M^{FLS}$ расширяет классическое понятие «смежности» вершин мультиграфа.

Утверждение 1. Любые две вершины $\{m_i, m_j\}$ мультиграфа $G^{FLS}(M_N,R_M^{FLS})$ являются смежными, если и только если в FLS-подграфах между этими вершинами существует хотя бы одно подмножество кратных дуг вида $\{r_{i,j}^F, r_{i,j}^L, r_{i,j}^S\}$, которое называется полной FLS-дугой.

Утверждение 2. Информационное взаимодействие между любыми двумя модулями МК-сети возможно, если обозначающие их вершины $\{m_i, m_j\}$ графа $G^{FLS}(M_N,R_M^{FLS})$ смежные.

Утверждение 3. Путь P^{FLS} между произвольной парой вершин $\{m_i, m_j\}$ в FLS мультиграфе $G^{FLS}(M_N,R_M^{FLS})$ существует, если и только если существуют пути между этими вершинами в FLS-подграфах смежности.

Переход состояний МК-сети происходит только при наличии инцидентных дуг между смежными вершинами на всех трех уровнях взаимодействия (полная FLS дуга) активной траектории процесса при совпадении соответствующих индексов входных и выходных интерфейсов модулей. Семантика решающих правил определяется типовыми информационными примитивами [9] и может быть дополнена функционалом элементов DLT [1–4]. В децентрализованной «классической» схеме архитектуры DLT правила АСР являются однотипными для всех вершин.

В критических системах АСР и архитектура должны реализовать модель защиты с «полным перекрытием». Расширенный вариант модели защиты с полным перекрытием образует пятидольный ориентированный граф (рис. 2) на основе декомпозиции множества информационных взаимодействий

R_M на подмножества $\{R^F \cup R^L \cup R^S\}$ R_M^{FLS} *FLS*-отношений, реализующих фазы информационного взаимодействия в соответствии с парадигмой трехуровневого информационного взаимодействия [10], которые реализуются МАС из множества M_D.

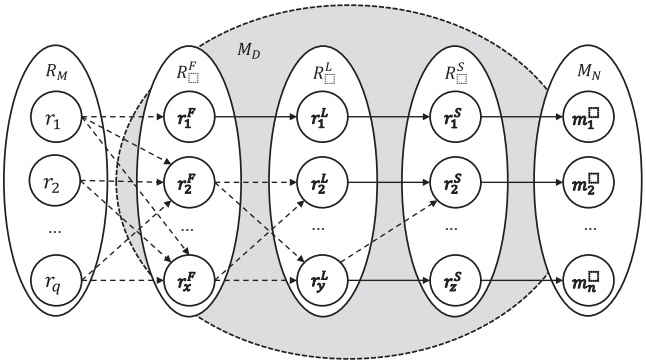


Рис. 2. Отображение множества информационных взаимодействий R_M на множество модулей M_N через множество M_D средств разграничения доступа и подмножества $\{R^F \cup R^L \cup R^S\}R_M^{FLS}$ FLS-отношений

В расширенной модели защиты с полным перекрытием множество вершин M_N, где N – число всех вершин мультиграфа G^{FLS}, разбивается правилами АСР на кластерные подмножества модулей обработки данных M_K (K – число кластеров), такие что $M_1 \cap M_2 \cap M_k = \emptyset$ и $M_1 \cup M_2 \cup M_k = M_K$, и M_D – подмножество МАС (D – число МАС), где $M_K \cap M_D = \emptyset$ и $M_K \cup M_D = M_N$. Кластерные ограничения отражаются на графе отсутствием полных *FLS* дуг между любыми элементами из разных подмножеств M_K. Мультиграф G^{FLS} является разновидностью цветной сети Петри [11], в которой *FLS*-маркеры имеют иерархическую зависимость и срабатывают в последовательности $R^F \longrightarrow R^L \longrightarrow R^S$ при совпадении согласованных выходных и входных индексов (цветов), которые определяют семантику переходов.

Задача анализа заключается в поиске состояний системы, нарушающих декларируемую политику, и в оценке уровня защиты для каждого пути по критерию отсутствия «слабого звена», т.е. вершин или дуг с весами ниже установленного значения. Статический анализ проводится на мультиграфе G^{FLS} проверкой гипотез о достижимости модулей при установленных кластерных ограничениях и позволяет оценить безопасность исходного состояния системы. Динамический анализ позволяет оценить безопасность состояний системы для всех траекторий информационной процесса при изменении состава вершин и дуг мультиграфа G^{FLS} в результате применения решающих правил управляемого логического вывода. Результаты проверки достижимости модулей отражаются в квадратной матрице достижимости модулей $A^Д = [a_{ij}]$ мультиграфа G^{FLS}, элементы которой строятся по правилу:

$$a_{ij} = \begin{cases} 1, \text{ если из вершины } i \text{ к вершине } j \text{ имеется путь } P_{ij}^{FLS}; \\ 0, \text{ если из вершины } i \text{ к вершине } j \text{ путь } P_{ij}^{FLS} \text{ отсутствует.} \end{cases} \quad (1)$$

Формальным критерием безопасности архитектуры является отсутствие пути P_{ij}^{FLS} между любыми произвольными вершинами из разных кластерных подмножеств M_K, который не содержит хотя бы одной вершины из подмножества M_D. Отсутствие пути доказывается сравнением значений каждой позиции кластерной матрицы $A^K = [a_{ij}]$, сформированной по правилам АСР с позицией в матрице достижимости $A^Д = [a_{ij}]$, которая формируется в результате логического вывода. Если матрицы равны, то формальные правила АСР выполняются и конфигурация архитектуры DLT безопасна. Для критических систем может быть установлен более строгий критерий безопасности – все полные *FLS*-дуги между любыми вершинами подмножества M_K должны быть инциденты хотя бы одной вершине из подмножества M_D. Этот случай актуален, например, для политики с «нулевым доверием» (Zero Trust), если каждое взаимодействие между любыми модулями осуществляется через процедуры безопасности.

Квантовая угроза для технологий распределенного реестра

Функции защиты могут быть реализованы МАС на физическом F, синтаксическом L или семантическом S уровнях информационного взаимодействия [7]. Для учета надежности МАС в оценке безопасности архитектуры DLT вершинам мультиграфа из множества M_D присваиваются нормированные весовые коэффициенты, характеризующие надежность защиты на основе внешних данных

$$V = |v_1^{(k)}, v_2^{(k)}, \ldots, v_n^{(k)}|. \quad (2)$$

Каждой v-ой вершине приписывается вес $V_v^{(k)}$, где k – функция веса.

Непрерывность уровня защиты оценивается сравнением значений весовых коэффициентов помеченных вершин графа для каждого пути относительно нормированного заданного значения, которое может быть установлено, например, классом защиты и уровнем доверия к средству защиты, или расчетным значением, например, стойкости криптографии к атакам с использованием квантового суперкомпьютера с высокой скоростью операций. Например, для функций шифрования и аутентификации, которые являются конструктивной основой безопасности архитектуры DLT, может быть задана оценка стойкости или вероятности компрометации криптографии. Для DLT оценка надежности криптографии является принципиальной. Публичные оценки скорости вычислений существующих квантовых компьютеров пока

не достигли области риска компрометации криптографии DLT, например, 13x106 кубит для взлома 256-битного ключа Bitcoin [6]. Однако анонсируется создание более производительных промышленных квантовых компьютеров, возможно скрытие информации об их наличии, разрабатываются эффективные методы атак на неидеальную криптографию при существующей скорости вычислений.

Снижение риска возможно, например, за счет использования постквантовой и идеальной криптографии, технологии квантового распределения ключей (QKD – Quantum Key Distribution). В частности, имеются рекомендации об использовании двойной длины ключа в симметричных блочных алгоритмах [6]. Усиление стойкости асимметричной криптографии за счет повышения сложности математических вычислений в предположении отсутствия эффективных методов обратного преобразования не дает гарантии конструктивной безопасности архитектуры DLT, что предполагает поиск альтернативной организации архитектуры для критических приложений.

Формальная постановка задачи анализа безопасности архитектуры DLTS

Пусть конечное множество элементов $M_N = \{m_1, m_2, ..., m_n\}$ (где N их число) составляет систему W, $M_K \cup M_D = M_N$ и $M_K \cap M_D = \emptyset$. Каждый элемент m обладает свойствами r_m^{FLS} из конечного множества свойств $R_M^{FLS} = \{R^F, R^L, R^S\}$, определенных на множестве M_N. Конкретный набор свойств всех элементов множества M_N, которые составляют подмножество $R_m^{FLS} \subset R_M^{FLS}$, определяет состояние ψ^t системы W в дискретный момент времени t. Множества M_N и R_M^{FLS} конечны, поэтому все состояния $\psi = f(M_N, R_M^{FLS}, t)$ принадлежат конечному множеству состояний Ψ системы W. Если в момент времени t между одной или несколькими парами модулей существуют бинарные отношения $\exists(m_i, m_j) \subset M_N$, которые на основании внешнего правила отнесены к подмножеству опасных, то состояние ψ^t относится к подмножеству опасных состояний $\bar{\Psi}$ системы W. Пусть задано множество Ψ объектов анализа и некоторое свойство r этого множества. Свойство r объекта анализа x может быть задано предикатом $P_r(x)$, определенным как функция на множестве Ψ со значениями «истина» (И) и «ложь» (Л)

$$P_r: \Psi \longrightarrow \{И, Л\}. \quad (3)$$

Если Ψ – множество состояний системы, ψ_i – безопасное состояние, ψ_j – опасное состояние, r – свойство «быть безопасным», то $P_r(\psi_i) = И$, $P_r(\psi_j) = Л$ для всех $\psi \in \Psi$. Множество Ψ разбивается предикатом P_r на два подмножества: $\Psi_r = \{\psi_1, \psi_2, ..., \psi_n\}$ – безопасные состояния системы, и $\bar{\Psi}_r = \{\psi_1, \psi_2, ..., \psi_e\}$ – опасные состояния системы. При этом справедливо

$$\Psi = \Psi_r \cup \bar{\Psi}_r, \Psi_r \cap \bar{\Psi}_r = \emptyset. \quad (4)$$

Вычислением значения истинности предиката $P_r(x)$ решается задача анализа безопасности некоторого объекта анализа x. Если свойство r рассматривать как сочетание других свойств объекта x, выраженных предикатами $P_{r_1}(x)$, $P_{r_2}(x)$, ..., то вычисление значения предиката $P_r(x)$ может быть проведено вычислением значения предикатов $P_{r_1}(x)$, $P_{r_2}(x)$, ... и затем определением истинности $P_r(x)$ путем приложения операции следования вида

$$F(P_{r_1}(x), P_{r_2}(x), ...) \longrightarrow P_r(x). \quad (5)$$

Применение некоторых операций логики к начальному множеству предложений, составляющему модель объекта x, и получение некоторого предложения этого же языка, являющегося формальным выражением свойства r, составляет процесс вычисления предиката $P_r(x)$. Каждое свойство r_j также может быть представлено через совокупность других свойств объекта. Задача анализа решается путем вычисления значения предиката $P_j(x)$, который принимает значение «истина», если объект x является j-ой модификацией ψ_j и значение «ложь» в противном случае. Представление логического компонента алгоритма анализа архитектуры DLTS в виде формальных операций логического следования на множестве предложений языка задания объекта анализа позволяет рассматривать процесс доказательства как многоуровневый управляемый логический вывод некоторого выражения этого языка, который отыскивается в ходе построения эксперимента.

Таким образом, в формальной постановке задача анализа безопасности архитектуры DLTS заключается в формировании множеств M_N и R_M^{FLS}, поиске элементов и доказательства полноты множества $\bar{\Psi}_r = \{\psi_1, \psi_2, ..., \psi_e\}$, где $\bar{\Psi}_r = f\{M_N, R_M^{FLS}\}$, для доказательства его пустоты ($\bar{\Psi}_r = \emptyset$), а также оценке соответствия весов $V_v^{(k)}$ элементов подмножества M_D установленному значению.

Доказательство безопасности состояний архитектуры DLTS

Для моделирования состояний системы FLS-подграфы задаются тремя взаимосвязанными квадратными бинарными FLS-матрицами

$$F = \|f_{i,j}\|; L = \|l_{i,j}\|; S = \|s_{i,j}\|, \quad (6)$$

где $i,j = 1, n$, n – максимальный номер вершины.

Свойства вершин и дуг мультиграфа задаются подматрицами FLS интерфейсов, которые полностью определяют функционально-структурные свойства модулей относительно других модулей архитектуры

$$F_{(ij)}^I = \|f_{(i^{вых.}\, j^{вх.})}^I\|; L_{(ij)}^I = \|l_{(i^{вых.}\, j^{вх.})}^I\|; S_{(ij)}^I = \|s_{(i^{вых.}\, j^{вх.})}^I\|, \quad (7)$$

где $F_{(ij)}^I$, $L_{(ij)}^I$, $S_{(ij)}^I$ – подматрицы смежных физических, синтаксических и семантических выходных для модулей m_i и входных для модулей m_j FLS интерфейсов.

Состояния системы являются результатом взаимодействия модулей на трех уровнях, поэтому необходимо генерировать согласованные FLS-матрицы смежности для каждого уровня информационного взаимодействия в соответствии с выражениями (6) и (7). Уровни взаимодействия представляются отдельными FLS-матрицами смежности, у которых строки и столбцы проиндексированы номерами модулей. Наличие значений, отличных от «0», в одинаковых позициях квадратных FLS-матриц указывает на то, что модули, номерами которых проиндексированы строки и столбцы, являются смежными вершинами.

Доказательство безопасности архитектуры обеспечивается управляемым перебором состояний в ходе построения FLS-мультиграфа состояний системы и определением на каждом шаге безопасности порожденного состояния. Проверка безопасности состояния заключается в установлении всех возможных отношений между модулями, которые изменялись на последнем шаге, и проверке их принадлежности подмножеству разрешенных отношений для этих модулей. Если отношения разрешены (присутствуют в кластерной FLS-модели), то состояние безопасное. Соответственно, если отношения запрещены (отсутствуют в кластерной FLS-модели), то состояние опасное. Строгость доказательства соответствует строгости математического аппарата логического вывода.

Подход к синтезу функционально стабильной архитектуры DLTS

Результаты оценки функционально-структурных свойств методами теории МК-сетей позволяют применять их для решения задачи структурно-функционального синтеза безопасной архитектуры DLTS, который заключается в итерационном процессе поиска опасных состояний и замыкании всех маршрутов между вершинами разных кластеров хотя бы на одну вершину подмножества M_D модулей MAC, а также замыкании всех входящих FLS-дуг на вершины со значением весового коэффициента не ниже установленного или замене модулей MAC из подмножества M_D.

Выводы

1. Применение методов теории МК-сетей, основанных на парадигме трехуровневого информационного FLS взаимодействия, позволяет моделировать и анализировать функционально-структурные свойства архитектуры DLT с формальным доказательством корректности результатов на основе управляемого логического вывода некоторого предложения формального языка математической логики.

2. Особенностью архитектуры DLT является однотипность FLS модулей, интерфейсов и кластеров ACP для всех (децентрализованная схема) или основного множества (централизованная и гибридная схемы) участников взаимодействия, что позволяет редуцировать граф состояний и аппроксимировать результаты на всю систему без потери достоверности оценок. Различия в схемах конфигурации архитектуры DLT могут учитываться в информационной модели, например, включением, кроме типовых модулей «потребитель» и «поставщик» данных, модулей «сервер хранения ключей», «сервер хранения данных», «управление обменом данными» и дополнительных FLS-интерфейсов [4]. В такой конфигурации возможен переход в опасное состояние через интерфейсы модулей, реализующих централизованные функции. При этом нарушается регулярность мультиграфа G^{FLS} и требуется корректировка исходной объектно-ориентированной информационной модели. Кроме того, в ACP с отсутствием доверия участников взаимодействия к централизованным модулям, их FLS интерфейсы формируют траектории процесса, которые всегда будут приводить систему в опасные состояния, например, из-за угрозы нарушения конфиденциальности транзакций и/или сведений об участниках взаимодействия. В этом случае для обеспечения корректности результатов логического вывода необходимо формировать ACP с исключением модулей с централизованными функциями из модели нарушителя безопасности и кластерных матриц. Целесообразно разработать модели угроз для типовых конфигураций архитектуры DLT с учетом особенностей ACP, архитектуры и квантовой угрозы.

3. Для оценки надежности криптографии DLT в условиях квантовой угрозы необходимы исследования с натурными экспериментами, в том числе с использованием квантовых коммуникаций и технологии квантового распределения ключей. Целесообразно провести оценку риска компрометации хранимых в DLT данных со сроком конфиденциальности более 5 лет в случае достижения «квантового превосходства», а также исследовать применение в DLT:

- более стойкой симметричной криптографии для снижения риска компрометации DLT при резком достижении «квантового превосходства» и/или появлении эффективных методов взлома неидеальной криптографии;
- технологии QKD для генерации криптографических ключей;
- «постквантовой» ассиметричной криптографии для защиты транзакций в некритических DLTS.

Для реализации формального анализа и синтеза функционально стабильной архитектуры DLTS на основе методов теории МК-сетей целесообразно провести дополнительные исследования и разработки, в частности:

- исследовать влияние ACP, децентрализованных, централизованных и гибридных конфигураций архитектуры на безопасность DLTS;

- разработать технологию построения модульно-кластерной модели DLTS с использованием технологии искусственного интеллекта, специально обученного для решения задач моделирования информационных процессов;
- разработать технологию автоматизированного синтеза безопасной архитектуры DLTS-P (Protection) на основе анализа модульно-кластерной модели.

В целях проведения натурного моделирования, проверки научных гипотез и синтеза безопасной архитектуры DLT в условиях квантовой угрозы перспективным является создание межотраслевого кластера квантовых коммуникаций и искусственного интеллекта в Научно-технологическом университете «Сириус» в рамках этапа II «Вторая очередь пилотного проекта – расширение межуниверситетской квантовой сети – с 01.01.2025 г. по 31.12.2025 г.» [11], что позволит решить научные задачи и достичь синергетического эффекта при взаимодействии с экспертами профильных организаций и ВУЗов.

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение №23–03 от 27.09.2024 г.).

Литература

1. Recommendation ITU-T X.1400 (10/2020), Distributed ledger technology security. Terms and definitions for distributed ledger technology.
2. Recommendation ITU-T X.1402 (07/2020), Distributed ledger technology security. Security framework for distributed ledger technology.
3. Recommendation ITU-T X.1408 (10/2021), Distributed ledger technology (DLT) security. Security threats and requirements for data access and sharing based on the distributed ledger technology.
4. Recommendation ITU-T X.1410 (03/2023), Distributed ledger technology (DLT) security. Security architecture of data sharing management based on the distributed ledger technology.
5. Федеральный закон РФ от 26.07.2017 № 187-ФЗ «О безопасности критической информационной структуры РФ».
6. Mark Webber, Vincent Elfving, Sebastian Weidt, Winfried K. Hensinger. The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime. AVS Quantum Sci. 4, 013801 (2022); doi: 10.1116/5.0073075.
7. Сундеев П. В. Модульно-кластерные сети: основы теории / П. В. Сундеев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2006. – № 22. – С. 31–52.
8. Федеральный закон РФ от 26.07.2007 № 149-ФЗ «Об информации, информационных технологиях и защите информации».
9. Запечников С. В. Системы распределенного реестра, обеспечивающие конфиденциальность транзакций / С. В. Запечников // Безопасность информационных технологий. – 2020. – Т. 27, № 4. – С. 108–123. – DOI 10.26583/bit.2020.4.09.
10. Системный анализ функциональной стабильности критичных информационных систем / Симанков В. С., Сундеев П. В. / под науч. ред. В. С. Симанкова. КубГТУ, ИСТЭк. – Краснодар, 2004. – 204 с.
11. K. Jensen Coloured Petri nets: A high-level language for system design and analysis // Advances in Petri Nets 1990, ICATPN 1989, Lecture Notes in Computer Science.– vol. 483, Berlin–Heidelberg: Springer.– 1991.– ISBN 978-3-540-53863-9.– Pp. 342–416. https://doi.org/10.1007/3-540-53863-1_31.
12. Концепция создания, развития и эксплуатации Межуниверситетской квантовой сети (МУКС) Национальной исследовательской квантовой сети (НИКС) на 2024–2030 годы (утв. заместителем министра науки и высшего образования РФ 02.02.2024 года).

FUNCTIONAL STABILITY OF A DISTRIBUTED REGISTRY IN THE CONTEXT OF A QUANTUM THREAT

Sundeev P. V.[2]

Keywords: *modular cluster network, system analysis, security.*

The purpose of the research: *to propose an approach to the formal analysis of the functional stability of distributed ledger systems for critical applications under conditions of quantum threat.*

Research methods: *object-oriented analysis and synthesis of complex systems, system analysis, theory of modular cluster networks, graph theory, matrix theory, mathematical logic.*

Research results: *the influence of architecture security and access policy on the functional stability of a distributed registry in the context of a quantum threat is shown, the concept and formulation of the problem of security analysis*

2 Pavel V. Sundeev, Doctor of Technical Sciences, Chief Research Engineer of the Scientific Center for Information Technologies and Artificial Intelligence of the Autonomous Educational Institution of Higher Education «Sirius University», Federal Territory «Sirius», Russia. E-mail: sundeev.pv@talantiuspeh.ru

of a distributed registry architecture in terms of the theory of modular cluster networks, an approach to the synthesis of architecture with proven security properties is proposed.

Scientific novelty: *application of the theory of modular cluster networks to the analysis of the functional stability of distributed registry systems in the aspect of security, taking into account the influence of the quantum threat.*

References

1. Recommendation ITU-T X.1400 (10/2020), Distributed ledger technology security. Terms and definitions for distributed ledger technology.
2. Recommendation ITU-T X.1402 (07/2020), Distributed ledger technology security. Security framework for distributed ledger technology.
3. Recommendation ITU-T X.1408 (10/2021), Distributed ledger technology (DLT) security. Security threats and requirements for data access and sharing based on the distributed ledger technology.
4. Recommendation ITU-T X.1410 (03/2023), Distributed ledger technology (DLT) security. Security architecture of data sharing management based on the distributed ledger technology.
5. Federal Law of the Russian Federation dated July 26, 2017 No. 187-ФЗ «On the security of the Critical Information Structure of the Russian Federation».
6. Mark Webber, Vincent Elfving, Sebastian Weidt, Winfried K. Hensinger. The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime. AVS Quantum Sci. 4, 013801 (2022); doi: 10.1116/5.0073075.
7. Sundeev P.V. Modular cluster networks: fundamentals of theory. KubGAU Scientific Journal [Electronic resource]. – Krasnodar: KubGAU, 2006. – № 22 (06). – The code of the Information Register is 0420600012\0132. Access mode: http://www.ej.kubagro.ru/2006/06/15.
8. Federal Law of the Russian Federation dated July 26, 2007 No. 149-ФЗ «On Information, Information Technologies and Information Protection».
9. Zapechnikov S.V. Distributed registry systems that ensure transaction confidentiality. Information Technology Security, [S.l.], v. 27, n. 4, pp. 108–123, 2020. ISSN 2074-7136.
10. System analysis of functional stability of critical information systems / Simankov V.S., Sundeev P.V. / under the scientific editorship of V.S. Simankov. KubSTU, ISTEk. Krasnodar, 2004. 204 p.
11. K. Jensen Coloured Petri nets: A high-level language for system design and analysis // Advances in Petri Nets 1990, ICATPN 1989, Lecture Notes in Computer Science. – vol. 483, Berlin – Heidelberg: Springer. – 1991. – ISBN 978-3-540-53863-9. – Pp.342–416. https://doi.org/10.1007/3-540-53863-1_31.
12. «The concept of creation, development and operation of the Interuniversity Quantum Network National Research Quantum Network (NICS) for 2024-2030» (approved by the Deputy Minister of Science and Higher Education of the Russian Federation on 02.02.2024).

КВАНТОВЫЕ СЕТИ: РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ ЧЕРЕЗ НЕДОВЕРЕННЫЕ УЗЛЫ

Кулик С.П.[1], Молотков С.Н.[2]

DOI: 10.21681/2311-3456-2025-3-90-98

Цель исследования: *анализ секретности квантового распределения ключей через недоверенные узлы в квантовых сетях.*

Метод исследования: *использование энтропийных соотношений неопределенностей.*

Результат(ы) исследования: *приведено доказательство секретности квантового распределения ключей через недоверенные узлы в квантовых сетях. Использование энтропийных соотношений неопределенностей позволяет получить точное решение для длины секретного ключа в однофотонном случае. Сделано сравнение с точным решением для протокола BB84 и явно показана принципиальная разница в логической структуре доказательств секретности ключей в этих протоколах, что, на наш взгляд, является важным для развития систем квантовой криптографии.*

Научная новизна: *приведено доказательство секретности квантового распределения ключей через недоверенные узлы в квантовых сетях.*

Ключевые слова: *квантовая криптография, фотоны, недоверенные узлы, энтропийные соотношения неопределенности.*

1. Введение

При построении волоконных систем квантовой криптографии важной задачей является увеличение дальности распределения секретных ключей. Неоднофотонность источника квантовых состояний и потери в линии связи приводят к тому, что длина линии связи оказывается ограниченной до величины, для которой гарантируется секретность распределяемых ключей. На сегодняшний день обсуждается несколько способов решения проблемы увеличения дальности:

1) использование квантовых повторителей;
2) распределение ключей по цепочке через промежуточные доверенные узлы;
3) передача ключей с использованием промежуточных недоверенных узлов;
4) использование специального протокола Measurement-Device-Independent (MDI-QKD) [1].

Первый способ требует пока отсутствующей долговременной квантовой памяти, поэтому практически не реализован.

Второй способ технически самый простой, но самый слабый с криптографической точки зрения, поскольку секретные ключи доступны на промежуточном доверенном узле, через который по цепочке происходит распределение секретных ключей. Использование доверенных узлов требует полной, в криптографическом смысле (технической и физической), защиты промежуточного узла; той же степени серьезности, как и защиты передающей и приемной станций.

В способе MDI-QKD промежуточные узлы выполняют измерения квантовых состояний, но не имеют доступа к самому ключу. Это позволяет снизить риск утечки информации через недоверенные узлы. Его преимущество – высокая безопасность и устойчивость к атакам на измерительные устройства. Однако существенным ограничением является сложная аппаратная реализация.

Третий способ привлекателен, поскольку не требует полной криптографической защиты промежуточного узла связи из-за того, что секретные ключи не возникают на данном узле. По этой причине такие промежуточные узлы называются недоверенными. Злоумышленник может видеть и знать всю работу аппаратуры на узле, но при этом не будет знать секретного ключа, который будет распределен между двумя легитимными пользователями через недоверенный узел. Такая удивительная, на первый взгляд, ситуация, кажется невозможной, тем не менее, может быть реализована с использованием квантовой криптографии.

Данная идея была сформулирована, по-видимому, впервые в работе [2], и основана на интерференции квантовых состояний от двух пространственно разделенных источников.

Идея квантового распределения ключей на основе квантового компаратора использует следующее свойство когерентных состояний – излучения лазера. При «сбивке» двух когерентных состояний $|\alpha\rangle$ и $|\beta\rangle$ на входах симметричного светоделителя,

1 Кулик Сергей Павлович, доктор физико-математических наук, профессор, Центр квантовых технологий, МГУ имени М.В. Ломоносова, Москва, Россия. E mail: sergei.kulik@physics.msu.ru

2 Молотков Сергей Николаевич, доктор физико-математических наук, профессор, Институт физики твердого тела имени Ю.А. Осипьяна РАН, г. Черноголовка Московской области, Россия. E-mail: molotkov@issp.ac.ru

на двух выходах светоделителя возникают состояния $\left|\frac{(\alpha+\beta)}{\sqrt{2}}\right\rangle$ и $\left|\frac{(\alpha-\beta)}{\sqrt{2}}\right\rangle$ (Рис. 1). Входные состояния «складываются» на одном выходе и «вычитаются» на другом выходе светоделителя – фактически сравниваются (именно с этим в работе [2] было связано название – квантовый компаратор). Иначе говоря, если фаза и амплитуда входных состояний одинаковы $\alpha = \beta = e^{i\varphi}|\alpha|$, то срабатывает детектор L (рис.1). Если фазы противоположны $\alpha = -\beta = e^{i\varphi}|\alpha|$, то срабатывает детектор R.

На такой идее может быть реализовано квантовое распределение ключей через недоверенные узлы, что потенциально может увеличить дальность распределения ключей в два раза. Отсчеты детектора публично известны Алисе, Бобу и злоумышленнику на узле, который знает работу всей аппаратуры[3].

В работе приведено точное доказательство секретности для квантового распределения ключей с недоверенным узлом.

2. Общая идея распределения ключей через недоверенные узлы

Протокол распределения ключей выглядит следующим образом. Алиса случайно и равновероятно посылает сильно ослабленные когерентные состояния, которые получаются ослаблением лазерного излучения, $0 \longrightarrow |\alpha\rangle_A$ или $1 \longrightarrow |-\alpha\rangle_A$. Аналогично, Боб посылает $0 \longrightarrow |\alpha\rangle_B$ или $1 \longrightarrow |-\alpha\rangle_B$.

Отсчеты детекторов на недоверенном узле публично известны. Алиса и Боб, зная отсчет детекторов, L или R, и зная бит, который они посылали, могут синхронизовать свои биты – получить общий одинаковый бит ключа (рис. 1). Причем, зная только отсчеты детекторов на недоверенном узле, узнать ключ невозможно.

Данный метод распределения ключей рассматривается как перспективная технология квантовой криптографии – квантового распределения секретных ключей [3].

Разумеется, техническая реализация метода достаточно сложна, поскольку требует реализации устойчивой интерференции квантовых состояний из двух пространственно разделенных лазеров. Принципиальная возможность интерференции состояний из разных источников в лабораторных условиях была продемонстрирована еще в 1967 г. в работе [4]. Перенос таких экспериментов на реальные волоконные линии связи, когда участники разделены линией в несколько сотен километров до недоверенного узла, представляет собой задачу с принципиально другим уровнем сложности по сравнению с лабораторными экспериментами. Важно отметить, что никаких принципиальных физических запретов на реализацию таких систем нет.

3 Разумеется, злоумышленник может вывести из строя саму аппаратуру, при этом ключи не будут распределены. Важно, что нарушитель может знать работу всей аппаратуры, но не будет знать секретных ключей.

Для распределения ключей достаточно посылать пакеты когерентных состояний, локализованные в одном временном окне (рис. 1). Однако, как будет видно ниже, для доказательства секретности удобнее использовать пару состояний, локализованных в двух временных окнах вида

$$|\alpha\rangle_{1A} \otimes |e^{i\varphi_A}\rangle_{2A}, |\alpha\rangle_{1B} \otimes |e^{i\varphi_B}\rangle_{2B}, \quad (1)$$

где фазы состояний

$$\text{базис} + \begin{cases} \varphi_A = 0,\pi \\ \varphi_B = 0,\pi \end{cases}, \text{базис} \times \begin{cases} \varphi_A = \frac{\pi}{2}, \frac{3\pi}{2} \\ \varphi_B = \frac{\pi}{2} \end{cases}. \quad (2)$$

Нижние индексы отвечают за временные окна, в которых локализованы пакеты когерентных состояний. Состояния, локализованные в первом временном окне, никакой информации о бите ключа не несут, т.к. информация содержится в фазе когерентного состояния, локализованного во втором временном окне. Поскольку подслушиватель знает работу аппаратуры на недоверенном узле, длину линии от Алисы и Боба до недоверенного узла, то считается, что он знает и фазу самого когерентного состояния – знает

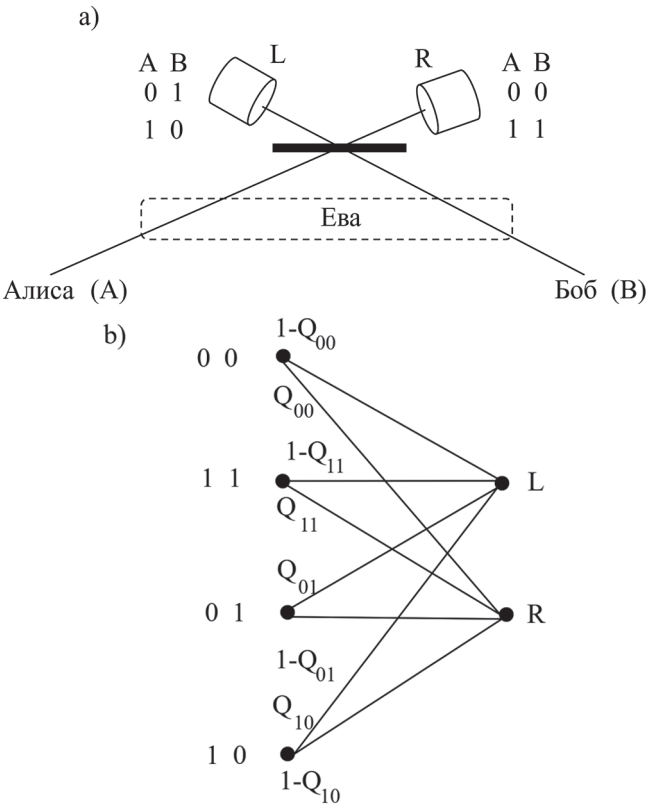


Рис. 1. a) Схематическое изображение квантового распределения ключей через недоверенный узел, и атака подслушивателя на два квантовых канала связи.

b) Структура классического канала (Алиса, Боб) – недоверенный узел. Показаны входной и выходной алфавит, а также переходные вероятности, описывающие канал связи.

комплексный параметр α, но не знает случайные в каждой посылке фазы φ_A и φ_B, несущие информацию о битах ключа.

Сбивка состояний на светоделителе приводит к состояниям на двух выходах, которые регистрируются детекторами L и R. Состояния на выходах светоделителя имеют вид

$$\text{Детектор } R\ |\frac{\alpha(e^{i\varphi_A}-e^{i\varphi_A})}{\sqrt{2}}\rangle_2 = |\sqrt{2}\bar{\alpha}\ \sin(\frac{\Delta\varphi}{2})\rangle_2,$$
$$\text{Детектор L}\ |\frac{\alpha(e^{i\varphi_A}+e^{i\varphi_A})}{\sqrt{2}}\rangle_2 = |\sqrt{2}\bar{\alpha}\ \cos(\frac{\Delta\varphi}{2})\rangle_2, \quad (3)$$

где

$$\Delta\varphi = \varphi_A - \varphi_B,\ \ .\bar{\alpha} = e^{i(\frac{\varphi_A+\varphi_B}{2})}. \quad (4)$$

Вероятность детектирования состояний детекторами L и R пропорциональна

$$Pr\{R,\Delta\varphi,\eta,l\} \propto 2\mu\sin^2(\frac{\Delta\varphi}{2})\eta_R\ T(l),$$
$$Pr\{L,\Delta\varphi,\eta,l\} \propto 2\mu\cos^2(\frac{\Delta\varphi}{2})\eta_L\ T(l), \quad (5)$$

где $T(l)$ – пропускание линии связи, l – длина линии связи, $\eta_{L,R}$ – квантовые эффективности детекторов.

В реальной ситуации в качестве информационных состояний используются сильно ослабленные когерентные состояния, которые имеют пуассоновскую статистику по числу фотонов. Т.е., кроме однофотонной компоненты, когерентные состояния содержат многофотонные составляющие фоковских состояний.

Первая задача состоит в получении доказательства секретности для однофотонных информационных состояний, поскольку секретный ключ формируется из однофотонной компоненты когерентных состояний.

Информация из многофотонных компонент, консервативно в пользу подслушивателя, считается полностью известной подслушивателю. Доля однофотонной компоненты на втором этапе доказательства секретности ключей может быть оценена, например, с использованием т.н. Decoy State метода [5].

Насколько нам известно, доказательство секретности ключей даже в однофотонном случае для квантового распределения ключей с недоверенным узлом не получено. Например, в работе [3], приводится длина секретного ключа для однофотонной компоненты, которая приведена без всякого вывода и, по сути, взята из работ, относящихся к протоколу BB84 [6]. Хотя сразу видно, что ситуация физически принципиально другая по сравнению с ситуацией, когда ключи распределяются непосредственно между Алисой и Бобом, поэтому и логика анализа секретности ключей также принципиально другая. Как будет видно ниже, длина секретного ключа будет зависеть от четырех параметров (ошибки в двух каналах связи Алиса – недоверенный узел, и Боб – недоверенный узел). Этот факт вносит принципиальное различие в анализ секретности, выполненный для протокола BB84 [6].

Ниже будет приведено точное доказательство секретности для квантового распределения ключей с недоверенным узлом. Под точным решением понимается решение, которое основано на фундаментальных энтропийных соотношениях неопределенностей, использование которых позволяет оценить верхнюю границу утечки информации к подслушивателю по наблюдаемому уровню ошибок при детектировании состояний детекторами L и R. Энтропийные соотношения, возникающие в данной задаче, по логике и структуре принципиально отличаются от соответствующих энтропийных соотношений при доказательстве секретности протокола BB84. Будет также проведено сравнение с доказательством секретности для протокола BB84, и явно показана принципиальная разница в логике и структуре доказательства, а также результатах по оценке длины секретного ключа.

3. Однофотонный случай, двойное запутанное квантовое состояние

При доказательстве секретности стандартного протокола BB84 используется сведение протокола, к так называемой, ЭПР-версии (запутанное состояние Эйнштейна-Подольского-Розена) [7–9].

Необходимость сведения протокола к ЭПР-версии связана с дальнейшим использованием энтропийных соотношений неопределенностей. Такое сведение является формальным математическим приемом. ЭПР-версия протокола эквивалентна исходной версии – приготовление, посыл состояний. ЭПР-пара нужна для использования энтропийных соотношений неопределенностей, поскольку в них фигурирует матрица плотности Алиса-Боб-Ева, которая происходит в разных базисах из одного и того же исходного состояния.

ЭПР-версия протокола выглядит следующим образом. Алиса генерирует ЭПР-пару, свою подсистему оставляет себе, а подсистему Боба отправляет на приемную станцию. Измерение Алисы над своей подсистемой в одном из базисов переводит ЭПР-пару в одно из базисных состояний для Алисы и Боба. Подсистема Боба подвержена атакам подслушивателя в канале связи.

При распределении с недоверенным узлом Алиса и Боб независимо посылают состояния, отвечающие 0 и 1. Посылки, где базисы Алисы и Боба не совпадали, отбрасываются. В каждом базисе возможны 4 комбинации состояний Алисы и Боба в канале связи, которые доступны для подслушивателя: (00), (11), (01), (10), отсчеты детекторов также известны.

Ниже протокол будет сведен к ЭПР-версии, при этом приходится использовать две независимые

ЭПР-пары. Уже на данном этапе возникает существенное отличие от доказательства секретности для протокола BB84.

Введем вспомогательные состояния Алисы (индекс $\bar{A}$) и Боба (индекс $\bar{B}$). Это состояния, которые остаются как эталонные на передающих станциях Алисы и Боба. Состояния, которые посылаются Алисой и Бобом в линию связи, имеют индексы A и B. Представления ЭПР-пары $\bar{A}A$) для канала (Алиса–недоверенный узел) в разных базисах имеет вид

$$|\Phi\rangle_{\bar{A}A} = \frac{1}{\sqrt{2}}\left(|\bar{0}^{+}\rangle_{\bar{A}} \otimes |\bar{0}^{+}\rangle_{A} + |\bar{1}^{+}\rangle_{\bar{A}} \otimes |\bar{1}^{+}\rangle_{A}\right) =$$

$$= \frac{1}{\sqrt{2}}\left(|\bar{0}^{\times}\rangle_{\bar{A}} \otimes |\bar{0}^{\times}\rangle_{A} + |\bar{1}^{\times}\rangle_{\bar{A}} \otimes |\bar{1}^{\times}\rangle_{A}\right). \quad (6)$$

Аналогично для ЭПР-пары $\bar{B}B$) для канала (Боб – недоверенный узел) имеем

$$|\Phi\rangle_{\bar{B}B} = \frac{1}{\sqrt{2}}\left(|\bar{0}^{+}\rangle_{\bar{B}} \otimes |\bar{0}^{+}\rangle_{B} + |\bar{1}^{+}\rangle_{\bar{B}} \otimes |\bar{1}^{+}\rangle_{B}\right) =$$

$$= \frac{1}{\sqrt{2}}\left(|\bar{0}^{\times}\rangle_{\bar{B}} \otimes |\bar{0}^{\times}\rangle_{B} + |\bar{1}^{\times}\rangle_{\bar{B}} \otimes |\bar{1}^{\times}\rangle_{B}\right). \quad (7)$$

Соответственно, двойная ЭПР-пара имеет вид

$$|\Phi\rangle_{\bar{A}\bar{B}AB} = |\Phi\rangle_{\bar{A}A} \otimes |\Phi\rangle_{\bar{B}B}. \quad (8)$$

Выбор состояния, которое посылается в каждый канал связи, осуществляется при помощи измерения в выбранном базисе над вспомогательными подсистемами $\bar{A}$ и $\bar{B}$. Измерения даются разложениями единицы

$$I_{\bar{A}} = |\bar{0}^{+}\rangle_{\bar{A}_{\bar{A}}}\langle\bar{0}^{+}| + |\bar{1}^{+}\rangle_{\bar{A}_{\bar{A}}}\langle\bar{1}^{+}| = |\bar{0}^{\times}\rangle_{\bar{A}_{\bar{A}}}\langle\bar{0}^{\times}| + |\bar{1}^{\times}\rangle_{\bar{A}_{\bar{A}}}\langle\bar{1}^{\times}|. \quad (9)$$

Аналогично для подсистемы $\bar{B}$

$$I_{\bar{B}} = |\bar{0}^{+}\rangle_{\bar{B}_{\bar{B}}}\langle\bar{0}^{+}| + |\bar{1}^{+}\rangle_{\bar{B}_{\bar{B}}}\langle\bar{1}^{+}| = |\bar{0}^{\times}\rangle_{\bar{B}_{\bar{B}}}\langle\bar{0}^{\times}| + |\bar{1}^{\times}\rangle_{\bar{B}_{\bar{B}}}\langle\bar{1}^{\times}|. \quad (10)$$

Измерение над двумя вспомогательными подсистемами для двух каналов дается разложением единицы

$$I_{\bar{A}\bar{B}} = I_{\bar{A}} \otimes I_{\bar{B}}. \quad (11)$$

4. Атака подслушивателя на квантовые состояния

После измерений подсистемы A и B переходят в одно из четырех состояний, которые подвержены атаке подслушивателя. Атака подслушивателя описывается супероператором T_{EAB}, явный вид которого, не потребуется. После атаки подслушивателя состояния в линиях связи даются следующими матрицами плотности в двух линиях связи

$$\rho_{ABE}(00) = T_{EAB}(|0^{+}0^{+}\rangle_{AB_{AB}}\langle 0^{+}0^{+}|),$$
$$\rho_{ABE}(01) = T_{EAB}(|0^{+}1^{+}\rangle_{AB_{AB}}\langle 0^{+}1^{+}|), \quad (12)$$
$$\rho_{ABE}(10) = T_{EAB}(|1^{+}0^{+}\rangle_{AB_{AB}}\langle 1^{+}0^{+}|),$$
$$\rho_{ABE}(11) = T_{EAB}(|1^{+}1^{+}\rangle_{AB_{AB}}\langle 1^{+}1^{+}|), \quad (13)$$

Для полной матрицы плотности в базисе + получаем

$$\rho_{\bar{A}\bar{B}AB} = (T_{EAB}(I_{\bar{A}\bar{B}}|\Phi\rangle_{\bar{A}\bar{B}AB_{\bar{A}\bar{B}AB}}\Phi|I_{\bar{A}\bar{B}}))=$$
$$= \frac{1}{4}\left(|\bar{0}^{+}\bar{0}^{+}\rangle_{\bar{A}\bar{B}_{\bar{A}\bar{B}}}\langle\bar{0}^{+}\bar{0}^{+}| \otimes \rho_{ABE}(00) + \right.$$
$$+ |\bar{0}^{+}\bar{1}^{+}\rangle_{\bar{A}\bar{B}_{\bar{A}\bar{B}}}\langle\bar{0}^{+}\bar{1}^{+}| \otimes \rho_{ABE}(01) +$$
$$+ |\bar{1}^{+}\bar{0}^{+}\rangle_{\bar{A}\bar{B}_{\bar{A}\bar{B}}}\langle\bar{1}^{+}\bar{0}^{+}| \otimes \rho_{ABE}(10) +$$
$$\left. + |\bar{1}^{+}\bar{1}^{+}\rangle_{\bar{A}\bar{B}_{\bar{A}\bar{B}}}\langle\bar{1}^{+}\bar{1}^{+}| \otimes \rho_{ABE}(11)\right), \quad (14)$$

В дальнейшем удобно ввести более компактные обозначения, заменив подсистемы $\bar{A}\bar{B}$ на случайную переменную X, которая имеет 4 значения. Для матрицы плотности в базисе + имеем

$$\rho_{X^{+}(AB)E} = \frac{1}{4}\sum_{x^{+}\in X^{+}}|x^{+}\rangle_{X_X}\langle x^{+}| \otimes \rho^{x^{+}}_{(AB)E}, \quad (15)$$

где

$$X^{+} = \{0^{+}0^{+},0^{+}1^{+},1^{+}0^{+},1^{+}1^{+}\}. \quad (16)$$

Аналогично в базисе ×

$$\rho_{X^{\times}(AB)E} = \frac{1}{4}\sum_{x^{\times}\in X^{\times}}|x^{\times}\rangle_{X_X}\langle x^{\times}| \otimes \rho^{x^{\times}}_{(AB)E}, \quad (17)$$

где значения случайной переменной X принадлежат алфавиту

$$X^{+} = \{0^{\times}0^{\times},0^{\times}1^{\times},1^{\times}0^{\times},1^{\times}1^{\times}\}. \quad (18)$$

5. Измерения на недоверенном узле

Рассмотрим измерения над состояниями в (15), поступающими из линий связи, на недоверенном узле. Преобразование состояний после измерений на недоверенном узле удобно описывать при помощи операторов Крауса, которые проектируют информационные состояния из обоих каналов. Поскольку результат детектирования известен, то удобно ввести формальные состояния $|L\rangle$ и $|R\rangle$, которые «привязаны» к отсчетам детекторов. В базисе + имеем

$$K^{+}_{(00),L} = |0^{+}0^{+}\rangle_{(AB)_Y}\langle L|,\ K_{(00),L} = |L\rangle_{Y_{(AB)}}\langle 0^{+}0^{+}|, \quad (19)$$
$$K^{+}_{(11),L} = |1^{+}1^{+}\rangle_{(AB)_Y}\langle L|,\ K_{(11),L} = |L\rangle_{Y_{(AB)}}\langle 1^{+}1^{+}|L|, \quad (20)$$
$$K^{+}_{(01),R} = |0^{+}1^{+}\rangle_{(AB)_Y}\langle R|,\ K_{(01),R} = |R\rangle_{Y_{(AB)}}\langle 0^{+}1^{+}|, \quad (21)$$
$$K^{+}_{(10),R} = |1^{+}0^{+}\rangle_{(AB)_Y}\langle R|,\ K_{(10),R} = |R\rangle_{Y_{(AB)}}\langle 1^{+}0^{+}|. \quad (22)$$

Аналогично предыдущему, операторы Крауса в базисе × имеют вид

$$K^{+}_{(00),L} = |0^{\times}0^{\times}\rangle_{(AB)_Y}\langle L|,\ K_{(00),L} = |L\rangle_{Y_{(AB)}}\langle 0^{\times}0^{\times}|, \quad (23)$$
$$K^{+}_{(11),L} = |1^{\times}1^{\times}\rangle_{(AB)_Y}\langle L|,\ K_{(11),L} = |L\rangle_{Y_{(AB)}}\langle 1^{\times}1^{\times}|, \quad (24)$$
$$K^{+}_{(01),R} = |0^{\times}1^{\times}\rangle_{(AB)_Y}\langle R|,\ K_{(01),R} = |R\rangle_{Y_{(AB)}}\langle 0^{\times}1^{\times}|, \quad (25)$$
$$K^{+}_{(10),R} = |1^{\times}0^{\times}\rangle_{(AB)_Y}\langle R|,\ K_{(10),R} = |R\rangle_{Y_{(AB)}}\langle 1^{\times}0^{\times}|, \quad (26)$$

где состояния $|R\rangle_Y$ и $|L\rangle_Y$ описывают отсчеты в одном из детекторов.

Результат измерений описывается случайной переменной Y, значения которой (y) принадлежат выходному алфавиту – отсчету в L или R детекторе,

$$y \in Y = \{L,R\}. \quad (27)$$

После измерений отсчета детектора на недове-

ренном узде, матрица плотности всех участников протокола Алиса-Боб-Ева в базисе + принимает вид

$$\rho_{X^+YE} = \frac{1}{4}\sum_{x^+\in X^+}\sum_{y\in Y}|x^+\rangle_{X_X}\langle x^+| \otimes |y\rangle_{Y_Y}\langle y| \otimes \rho_E^{x^+y}, \quad (28)$$

где

$$\rho_E^{x^+y} = \sum_{i=0,1}\sum_{j=0,1} K_{(ij),y}\, \rho^{x^+}_{(AB)E}\, K^+_{(ij),y}. \quad (29)$$

Аналогично для матрицы плотности в базисе × находим

$$\rho_{X^\times YE} = \frac{1}{4}\sum_{x^\times\in X^\times}\sum_{y\in Y}|x^\times\rangle_{X_X}\langle x^\times| \otimes |y\rangle_{Y_Y}\langle y| \otimes \rho_E^{x^\times y}, \quad (30)$$

где

$$\rho_E^{x^\times y} = \sum_{i=0,1}\sum_{j=0,1} K_{(ij),y}\, \rho^{x^\times}_{(AB)E}\, K^+_{(ij),y}. \quad (31)$$

Перейдем теперь к энтропийным соотношениям неопределенностей, в которых фигурируют матрицы плотности (15, 28, 30) и которые позволяют получить фундаментальную верхнюю границу утечки информации к подслушивателю.

6. Энтропийные соотношения неопределенностей

Для стандартного протокола BB84 энтропийные соотношения неопределенностей представляют собой «закон сохранения суммы двух условных энтропий – информаций Алиса-Евы и Алиса-Боб» (см. детали в [8, 10]). Данные соотношения позволяют найти верхнюю границу нехватки информации Евы относительно информационной строки Алисы через нехватку информации Боба относительно информационной строки Алисы. Нехватка информации Боба, классическая условная энтропия Шеннона Алиса-Боб, после измерений Боба оценивается через открытый классический канал связи по наблюдаемому числу ошибок.

В рассматриваемом случае энтропийные соотношения неопределенностей представляют собой закон сохранения суммы двух условных энтропий – $H(X^\times|E)$ условная энтропия между случайной величиной $X^\times$, находящейся у Алисы и Боба (см. (15, 17)) и Евой, и условной энтропией $H(X^+|Y)$ между X^+ (Алиса-Боб в сопряженном базисе) и Y – недоверенным узлом.

В асимптотическом пределе энтропийные соотношения неопределенностей [7,8] принимают вид

$$H(X^\times|E) + H(X^+|Y) \geq -\log|c|^2 = 2,$$
$$|c|^2 = \max_{i,j,i',j'=0,1} |_{\bar{A}\bar{B}}\langle i^+ j^+|i'^\times\, j'^\times\rangle_{\bar{A}\bar{B}}|^2 = \frac{1}{4}, \quad (32)$$

где

$$H(X^\times|E) = H(\rho_{X^\times E}) - H(\rho_E),\ H(X^+|Y) = H(\rho_{X^+Y}) - H(\rho_Y). \quad (33)$$

Частичная матрица плотности подслушивателя ρ_E в (33) относится к базису +. Матрица плотности (Алиса, Боб) – недоверенный узел $\rho_{X^+Y} = Tr_E\{\rho_{X^+YE}\}$ выражается через наблюдаемые параметры классического канала (Алиса, Боб) – недоверенный узел. Структура канала изображена на рис. 1. Для матрицы плотности находим

$$\rho_{X^+Y} =$$
$$= \frac{1}{4}|0^+0^+\rangle_{X_X}\langle 0^+0^+| \otimes \{(1-Q_{00})|L\rangle_{Y_Y}\langle L| + Q_{00}\,|R\rangle_{Y_Y}\langle R|\} +$$
$$+ \frac{1}{4}|0^+1^+\rangle_{X_X}\langle 0^+1^+| \otimes \{(1-Q_{01})|R\rangle_{Y_Y}\langle R| + Q_{01}|L\rangle_{Y_Y}\langle L|\} +$$
$$+ \frac{1}{4}|1^+0^+\rangle_{X_X}\langle 1^+0^+| \otimes \{(1-Q_{10})|R\rangle_{Y_Y}\langle R| + Q_{10}|L\rangle_{Y_Y}\langle L|\} +$$
$$+ \frac{1}{4}|1^+1^+\rangle_{X_X}\langle 1^+1^+| \otimes \{(1-Q_{11})|L\rangle_{Y_Y}\langle L| + Q_{10}|R\rangle_{Y_Y}\langle R|\}. \quad (34)$$

Переходные вероятности Q_{ij}, задающие классический канал связи (рис. 1) относятся к базису +, индекс базиса + для краткости опускаем. Для однофотонной компоненты для дальнейшего удобно обозначить так

$$P_{X|Y}(y|X=(ij)) = Q_{ij}, \quad (35)$$

где $y = L,R$. Например, $P_{X|Y}(L|X=(00))$ – условная вероятность того, что Алиса и Боб послали (00), и сработал детектор L, и т.д. Индекс базиса для краткости опускаем.

С учетом (33, 34) (см. также рис.) для условной энтропии находим

$$H(\rho_{X^+Y}) = 2 + \frac{1}{4}\sum_{i,j=0,1} h(Q_{ij}). \quad (36)$$

где $h(x) = -x\log(x) - (1-x)\log(1-x)$ – бинарная энтропийная функция Шеннона.

В симметричном случае, когда $Q_{ij} = Q$, получаем

$$H(\rho_{X^+Y}) = 2 + h(Q). \quad (37)$$

Далее для частичной матрицы плотности, описывающей состояния на недоверенном узле, с учетом (34), находим

$$\rho_Y = Tr_{X^+}\{\rho_{X^+Y}\} =$$
$$= \frac{1}{4}\{[2 - Q_{00} - Q_{11} + Q_{01} + Q_{10}]|L\rangle_{Y_Y}\langle L| +$$
$$+ [2 - Q_{01} - Q_{10} + Q_{00} + Q_{11}]|R\rangle_{Y_Y}\langle R|\}. \quad (38)$$

$$H(\rho_Y) = 1 - \bar{h}(q), \quad (39)$$

$$\bar{h}(q) = -(1-q)\log(1-q) - (1+q)\log(1+q),$$
$$q = \frac{1}{2}(Q_{00} + Q_{11} - Q_{01} - Q_{10}). \quad (40)$$

В итоге для условной энтропии находим с учетом (37) и (39)

$$H(X^+|Y) = 1 + \frac{1}{4}\sum_{i,j=0,1} h(Q_{ij}) - \bar{h}(q). \quad (41)$$

В симметричном случае ф-ла (41) принимает простой вид

$$H(X^+|Y) = 1 + h(q). \quad (42)$$

Интерпретация (42) имеет простой смысл. Канал на рис. 2 имеет четыре равновероятных состояний на входе (00), (11), (01), (10) и два состояния на выходе L и R. Уловная энтропия $H(X^+|Y)$ выхода

относительно входа имеет смысл нехватки информации выхода относительно входа, точнее говоря, нехватка информации в битах о входе при условии, что известен выход. На входе в канал поступает два бита информации – (00), (11), (01), (10). Если нет ошибок $Q = 0$, то знание того, какой детектор сработал L или R дает один бит информации. Условная энтропия при этом $H(X^+|Y) = 1$, т.е. не хватает одного бита, чтобы полностью знать информацию – два бита на входе в канал. Если подслушиватель вторгается в оба канала от Алисы и Боба к недоверенному узлу и получает информацию о передаваемых состояниях, то при этом возмущает их, что приводит к ошибкам в отсчетах детекторов.

7. Сравнение с точным решением для протокола BB84

В протоколе BB84 при доказательстве секретности используется одна ЭПР-пара Алиса-Боб

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0^+\rangle_A \otimes |\bar{0}^+\rangle_B + |1^+\rangle_A \otimes |1^+\rangle_B\right) =$$

$$= \frac{1}{\sqrt{2}}\left(|0^\times\rangle_A \otimes |0^\times\rangle_B + |1^\times\rangle_A \otimes |1^\times\rangle_B\right). \quad (43)$$

В асимптотическом пределе вместо (32, 33) возникают следующие энтропийные соотношения неопределенностей

$$H(X^\times|E) + H(X^+|Y) \geq -\log|c|^2 = 1,$$

$$|c|^2 = \max_{i,j,=0,1}|A\langle i + |j^\times\rangle A|^2 = \frac{1}{2}. \quad (43)$$

Соответственно, матрица плотности в базисе +, вместо (34), принимает вид

$$\rho_{X^+Y} = \frac{1}{2}|0^+\rangle_{X_X}\langle 0^+| \otimes \{(1 - Q_0)|0\rangle_{Y_Y}\langle 0| + Q_0|1\rangle_{Y_Y}\langle 1|\} +$$

$$+ \frac{1}{2}|1^+\rangle_{X_X}\langle 1^+| \otimes \{(1 - Q_1)|1^+\rangle_{Y_Y}\langle 1^+| + Q_1|0^+\rangle_{Y_Y}\langle 0^+|\}. \quad (45)$$

С учетом (45) , находим

$$H(\rho_{X^+Y}) = 1 + \frac{1}{2}\left(h(Q_0) + h(Q_1)\right). \quad (44)$$

В симметричном случае, когда $Q_0 = Q_1 = Q$, получаем

$$H(\rho_{X^+Y}) = 1 + h(Q). \quad (45)$$

Далее для частичной матрицы плотности Боба, с учетом (45), находим

$$\rho Y = Tr_{X^+}\{\rho_{X^+Y}\} = \frac{1}{2}\{|0^+\rangle_{Y_Y}\langle 0^+| + |1^+\rangle_{Y_Y}\langle 1^+|\}. \quad (46)$$

$$H(\rho_Y) = 1. \quad (47)$$

Напомним, что матрица плотности ρ_Y в ф-лах выше относится к базису +.

В итоге для условной энтропии, с учетом (46) и (49), получаем

$$H(X^+|Y) = \frac{1}{2}\left(h(Q_0) + h(Q_1)\right). \quad (48)$$

В симметричном случае ф-ла (50) принимает простой вид

$$H(X^+|Y) = h(Q), \quad (49)$$

которая дает нехватку информации выхода дискретного классического бинарного канала связи относительно входа [10]. В общем случае канал несимметричен.

8. Утечка информации при коррекции ошибок

После передачи квантовых состояний и измерений – отсчетов L и R детекторами, Алиса и Боб связаны бинарным (не обязательно симметричным) классическим каналом связи. Ситуация поясняется на рис. 2. Поскольку цель Алисы и Боба – получить идентичную битовую последовательность, то необходимо «привязаться», пусть для определенности, Бобу к битовой строке Алисы.

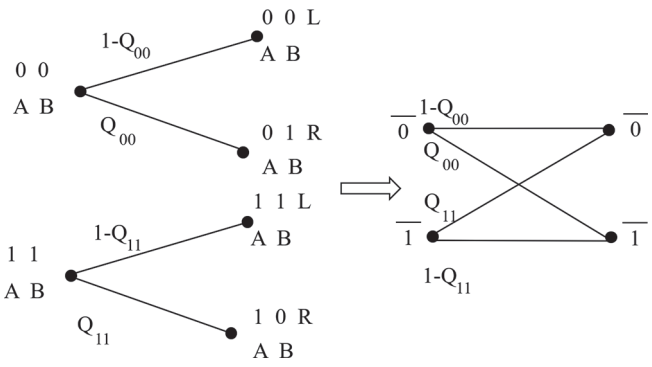


Рис. 2. Пояснения к процедуре коррекции ошибок Алисой и Бобом. Привязка происходит к биту Алисы (левая половина рис.). Правая половина – структура бинарного классического канала связи, в котором происходит коррекция ошибок – общего бита $\bar{0}$ или $\bar{1}$. Показаны также переходные вероятности бинарного канала связи в котором происходит коррекция ошибок.

Пусть привязка общих бит ($\bar{0}$, $\bar{1}$) идет к битам Алисы (см. рис. 2). Алиса всегда считает общим битом тот бит, который она послала. Алиса послала 0, тогда отсчет детектора L считает общим битом $\bar{0}$. Послала 1 – отсчет детектора L считает общим бит $\bar{1}$.

Далее Алиса послала 0 – отсчет детектора R считает общим бит $\bar{0}$, послала 1 – отсчет детектора R считает общим бит $\bar{1}$.

Пусть Алиса и Боб посылали 0 и 0 (уже в совпадающем базисе.) Пусть произошел отсчет в детекторе L – правильный отсчет. Тогда Алиса и Боб будут иметь одинаковый бит. Вероятность такого события есть $1 - Q_{00}$.

Если произошел отсчет в детекторе R, то Алиса будет считать общим битом свой бит 0 – привязка идет к ее битам, а Боб будет считать общим битом 1, что будет ошибкой. Вероятность такого события есть Q_{00}.

Аналогично, если Алиса посылала 1 и Боб посылал 1. Вероятность правильного отсчета есть $1 - Q_{11}$ – совпадение бита Алисы и Боба. Соответственно, вероятность ошибки есть Q_{11}.

Аналогично проводятся рассуждения, когда Алиса и Боб посылали противоположные значения бит.

С учетом сказанного, приходим к задаче исправления ошибок в бинарном классическом канале связи, точнее в двух независимых каналах связи с переходными вероятностями $\{1-Q_{00}, Q_{00}, 1-Q_{11}, Q_{11}\}$ и $\{1-Q_{01}, Q_{01}, 1-Q_{10}, Q_{10}\}$.

Далее, пусть передана и зарегистрирована серия длины n в асимптотическом пределе длинных последовательностей, в $\frac{1}{4}n$ посылок посылались состояния (00), $\frac{1}{4}n$ – (11), $\frac{1}{4}n$ – (01), $\frac{1}{4}n$ – (10). Утечка информации leak на одну посылку, которая требуется для исправления ошибок во всей последовательности в асимптотическом пределе

$$n\cdot leak = n[\frac{1}{2}\frac{(h(Q_{00})+h(Q_{11}))}{2}+\frac{1}{2}\frac{(h(Q_{01})+h(Q_{10}))}{2}. \quad (50)$$

Соответственно, в симметричном случае получаем

$$n\cdot leak = n[\frac{1}{2}\frac{(h(Q)+h(Q))}{2}+\frac{1}{2}\frac{(h(Q)+h(Q))}{2}. \quad (51)$$

Для сравнения, в протоколе BB84 ситуация между Алисой и Бобом после передачи и измерения квантовых состояний описывается одним классическим бинарным (в общем случае несимметричным) каналом связи, поэтому утечка информации при коррекции ошибок в асимптотическом пределе есть

$$n\cdot leak = n\frac{(h(Q_0)+h(Q_1))}{2}. \quad (52)$$

Для бинарного симметричного классического канала связи имеем

$$n\cdot leak = nh(Q). \quad (53)$$

Теперь можем перейти к вычислению длины секретного ключа.

9. Оценка длины секретного ключа

Для оценки длины секретного ключа (l) в пределе асимптотически длинных последовательностей ($n\longrightarrow\infty$) имеет место (см. детали в [7–9])

$$l=\lim_{n\to\infty}\frac{ln}{n}=H(X^{\times}|E)-leak, \quad (54)$$

здесь $leak$ – количество бит в пересчете на одну зарегистрированную посылку n, расходуемых на коррекцию ошибок. Ф-ла (56) имеет простую интерпретацию. Неформально, условная энтропия $H(X^{\times}|E)$ есть нехватка информации подслушивателя на одну посылку, которой не хватает до полного знания значения случайной переменной $X^{\times}$ при условии, что подслушиватель имеет в своем распоряжении квантовую систему E. Условная энтропия $H(X^{\times}|E)$ содержит в себе всю информацию об атаках подслушивателя. Энтропийные соотношения неопределенностей (32) позволяют найти фундаментальную нижнюю границу $H(X^{\times}|E)$ в базисе ×, не перебирая различные атаки, а получить оценку этой границы через наблюдаемые параметры классического канала (Алиса, Боб) – (детекторы L,R) в сопряженном базисе +.

Выражая $H(X^{\times}|E)$ через энтропийные соотношения неопределенностей (32), с учетом (41), получаем

$$H(X^{\times}|E)\geq 2-H(X^{+}|Y)=$$
$$=2-(1+\frac{1}{2}\sum_{i,j=0,1}h(Q_{ij})-\bar{h}(q)), \quad (55)$$

и

$$l=(X^{\times}|E)-leak=2-H(X^{+}|Y)-leak=$$
$$=1-(\frac{1}{2}\sum_{i,j=0,1}h(Q_{ij})-\bar{h}(q)). \quad (56)$$

В случае симметричного канала связи, когда $Q_{ij}=Q$ из (58), получаем

$$l=1-2h(Q), \quad (57)$$

Для сравнения приведем оценку длины секретного ключа для протокола BB84, с учетом (50,54) и (56), получаем

$$l=1-(h(Q_0)+h(Q_1)), \quad (58)$$

соответственно, в симметричном случае $Q_0=Q_1=Q$ находим

$$l=1-2h(Q). \quad (59)$$

В симметричном случае критическая ошибка Q, до которой можно распределять секретные ключи в протоколе распределения ключей через недоверенные узлы, такая же как в симметричном случае в протоколе BB84, и дается корнем уравнений (59) и (61), и оказывается равной $Q\approx 11\ \%$.

10. Заключение

На сегодняшний день передачу данных между узлами квантовой сети выполняют так называемые доверенные промежуточные узлы связи. При этом владелец сети контролирует все оборудование, которое генерирует, передает и принимает фотоны – носители информации. Такое решение проблемы позволяет исключить подключение к ним злоумышленников – за счет архитектуры сети. Однако такое построение систем связи не позволяет подключать большое число абонентов к инфраструктуре.

Для масштабирования квантовых коммуникаций предстоит создать технологию «недоверенных промежуточных узлов связи», то есть разработать такие устройства и системы, которые обеспечивали бы необходимый уровень безопасности, требуемую пропускную способность и гарантировали надежность коммуникаций. В теории это возможно, остается найти технологическое решение.

В данной работе обсуждается реализация квантового распределения ключей на основе квантового компаратора при помощи когерентных состояний, локализованных в определенных временных окнах.

Показано, что, хотя критическая ошибка в симметричном случае для протоколов совпадает, протоколы структурно совершенно различны. В общем несимметричном случае оценка для длины секретного ключа оказывается разной. Более того, в протоколе с недоверенным узлом длина секретного ключа в каждом базисе определяется в общем случае четырьмя параметрами $Q_{ij}(i,j = 0,1)$. В протоколе BB84 длина секретного ключа в каждом базисе в общем случае зависит от двух параметров Q_0 и Q_1. В обоих протоколах различные ошибки – переходные вероятности в классических каналах связи могут быть связаны как с разными характеристиками детекторов, так и неточностью приготовления информационных состояний. Важно, что в обоих протоколах в формулу для длины секретного ключа входят только наблюдаемые параметры. При этом характеристики детекторов – квантовые эффективности, темновые шумы, которые разумеется влияют на ошибки – сами явно не входят в формулу для длины секретного ключа.

Интерпретируем полученные результаты. Для удобства будем рассматривать симметричный случай. В протоколе BB84, как следует из энтропийных соотношений неопределенностей (44), нехватка информации подслушивателя $H(X|E) \geq 1 - h(Q)$, первое слагаемое 1 в правой части неравенства говорит о том, что без вторжения в линию связи, подслушиватель не знает 1 бит информации. Вторжение в линию связи приводит к ошибкам на приемной стороне. Чем больше ошибка Q, тем больше информации подслушиватель может получить. За это отвечает второе слагаемое в неравенстве (44). Таким образом, полная нехватка информации подслушивателя, которую он получает из квантового канала связи, производя при этом ошибку Q на приемной стороне, есть $1 - h(Q)$. Для исправления ошибок Q легитимные пользователи должны передать через открытый классический канал связи не менее $h(Q)$ бит информации в пересчете на одну посылку. Данная дополнительная информация доступна подслушивателю. При передаче квантовых состояний каждая посылка несет один бит секретной информации. Подслушиватель получает $h(Q)$ бит из квантового канала, и еще $h(Q)$ бит из классического канала при коррекции ошибок. В итоге полная нехватка информации подслушивателя, которая и является секретным ключом, есть $1 - h(Q) - h(Q)$ (см. ф-лу (61)).

В протоколе с недоверенным узлом в квантовый канал поступает пара квантовых состояний от Алисы и Боба, которые несут два бита секретной информации. Если подслушиватель не вторгается в квантовые каналы, а имеет доступ только к детекторам, то после отсчета одного из двух детекторов подслушиватель получает один бит информации. Как следует из энтропийных соотношений неопределенностей (32), нехватка информации подслушивателя есть $H(X|E) \geq 2 - (1 + h(Q)) = 1 - h(Q)$. Данное неравенство можно интерпретировать следующим образом. Исходная нехватка информации подслушивателя до отсчетов детекторов и без вторжения в каналы связи составляет два бита. Отсчет одного из детекторов уменьшает нехватку на один бит, слагаемое 1 в $(1 + h(Q))$ выше. Слагаемое $h(Q)$ отвечает за уменьшение нехватки информации за счет вторжения в каналы связи, что приводит к ошибке Q в отсчетах детекторов. Исправление ошибок требует публичного раскрытия не менее $leak = h(Q)$ бит информации при коррекции ошибок, что также уменьшает нехватку информации подслушивателя. В итоге полная нехватка информации подслушивателя (уже после коррекции ошибок) есть

$$H(X|E) - leak \geq 2 - (1 + h(Q)) - h(Q) = 1 - 2h(Q).$$

В заключение еще раз отметим, что, хотя формулы для длины секретного ключа в обоих протоколах и совпадают в симметричном случае, структурно и логически протоколы принципиально разные. В общем несимметричном случае длина секретного ключа оказывается разной.

Выше был рассмотрен случай однофотонных состояний, учет многофотонных компонент можно произвести, используя, например, Decoy State метод [5]. Изложение результатов такого анализа требует отдельного рассмотрения.

Выражаем благодарность В. Л. Елисееву, А. В. Уривскому, сотрудникам ИнфоТекс и СФБ Лаборатории за интерес к работе, обсужденние, сотрудничество и поддержку.

Исследования выполнены в рамках государственного задания МГУ имени М. В. Ломоносова.

Литература

1. Lo, H.-K., Curty, M., & Qi, B. Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503 (2012).
2. Молотков С. Н. Квантовая криптография на когерентных состояниях на основе квантового компаратора // Письма в Журнал экспериментальной и теоретической физики, 66, 736 (1997).

3 M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters, Nature, 557, 400 (2018).
4. R. L. Pfleegor, L. Mandel, Interference of Independent Photon Beams, Phys. Rev., 159, 1084 (1967).
5. Hoi-Kwong Lo, Xiongfeng Ma, Kai Chen, Decoy States Quantum Key Distribution, Phys. Rev. Lett., 94, 230504 (2005).
6. C. H. Bennett and G.Brassard, Quantum cryptography: Public key distribution and coin tossing, In Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process., pages 175–179, Bangalore, India (1984).
7. R. Renner, Security of Quantum Key Distribution, PhD thesis, ETH Zürich, arXiv:0512258 (2005).
8. M. Tomamichel, R. Renner, Uncertainty Relation for Smooth Entropies, Phys. Rev. Lett., 106, 110506 (2011).
9. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, R. Renner, Tight Finite-Key Analysis for Quantum Cryptography, arXiv:1103.4130 v2 (2011); Nature Communications, 3, 1 (2012).
10. T. M. Cover, J. A. Thomas. Elements of Information Theory. Wiley, (1991).

QUANTUM NETWORKS: KEY DISTRIBUTION VIA UNTRUSTED NODES

Kulik S. P.[4], Molotkov S. N.[5]

Keywords: *quantum cryptography, photons, untrusted nodes, entropy uncertainty relations.*

The aim of the research *is to analyze the secrecy of quantum key distribution through untrusted nodes in quantum networks.*

Research method: *the use of entropy uncertainty relations.*

Result(s) of the study: *the secrecy of quantum key distribution through untrusted nodes in quantum networks is proved. The use of entropy uncertainty relations makes it possible to obtain an accurate solution for the length of the secret key in the single-photon case. A comparison with the exact solution for the BB84 protocol is made and the fundamental difference in the logical structure of proof of the secrecy of keys in these protocols is clearly shown, which, in our opinion, is important for the development of quantum cryptography systems.*

Scientific novelty: *the article proves the secrecy of quantum key distribution through untrusted nodes in quantum networks.*

References

1. Lo, H.-K., Curty, M., & Qi, B. Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503 (2012).
2. S. N.Molotkov, Quantum cryptography on coherent states based on a quantum comparator, Letters to the Journal of Experimental and Theoretical Physics, 66, 736 (1997).
3 M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. Overcoming the rate-distance barrier of quantum key distribution without using quantum repeaters, Nature, 557, 400 (2018).
4. R. L. Pfleegor, L. Mandel, Interference of Independent Photon Beams, Phys. Rev., 159, 1084 (1967).
5. Hoi-Kwong Lo, Xiongfeng Ma, Kai Chen, Decoy States Quantum Key Distribution, Phys. Rev. Lett., 94, 230504 (2005).
6. C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, In Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process., pages 175–179, Bangalore, India (1984).
7. R. Renner, Security of Quantum Key Distribution, PhD thesis, ETH Zürich, arXiv:0512258 (2005).
8. M. Tomamichel, R. Renner, Uncertainty Relation for Smooth Entropies, Phys. Rev. Lett., 106, 110506 (2011).
9. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, R. Renner, Tight Finite-Key Analysis for Quantum Cryptography, arXiv:1103.4130 v2 (2011); Nature Communications, 3, 1 (2012).
10. T. M. Cover, J. A. Thomas. Elements of Information Theory. Wiley, (1991).

4 Sergey P. Kulik, Doctor of Physics and Mathematics. Doctor of Science, Professor, Center for Quantum Technologies, Lomonosov Moscow State University, Moscow, Russia. E-mail: sergei.kulik@physics.msu.ru
5 Sergey N. Molotkov, Doctor of Physics and Mathematics. Doctor of Medicine, Professor, Institute of Solid State Physics named after Y. A. Osipyan of the Russian Academy of Sciences, Chernogolovka, Moscow. Region, Russia. E-mail: molotkov@issp.ac.ru

КВАНТОВЫЙ КРИПТОАНКЛАВ ДЛЯ РЕАЛИЗАЦИИ НЕКОМПРОМЕТИРУЕМЫХ ДОВЕРЕННЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Елисеев В. Л.[1]

DOI: 10.21681/2311-3456-2025-3-99-104

Цель исследования: *разработка и обоснование архитектуры квантово-криптографической системы защиты доступа в центр обработки данных с высокими требованиями к конфиденциальности обрабатываемой информации, принадлежащей различным субъектам, на примере задачи федеративного обучения.*

Метод(ы) исследования: *системный анализ.*

Результат(ы) исследования: *рассматривается задача обеспечения конфиденциальности данных, принадлежащих различным субъектам, при их совместной обработке. Исследуется концепция криптоанклава как эффективного подхода для реализации поставленной задачи. Проводится анализ современных и перспективных угроз для криптографических методов защиты информации. Предлагается концепция квантового криптоанклава, сочетающего технологии криптографической защиты информации и квантового распределения ключей. Приводится пример возможной реализации квантового криптоанклава для решения задачи федеративного обучения.*

Научная новизна: *предложена архитектура квантового криптоанклава – центра обработки данных с криптографической защитой доступа с помощью сети квантового распределения ключей с доверенными промежуточными узлами.*

Ключевые слова: *криптоанклав, доверенные вычисления, федеративное обучение, квантовое распределение ключей, сеть квантового распределения ключей.*

Введение

Одним из следствий значительного развития информационных и коммуникационных технологий, наблюдающегося на протяжении нескольких десятков лет, стал существенный рост ценности информации, представленной в форме, доступной для цифровой обработки. Обладание информацией на протяжении всей истории человечества давало приоритет, однако только в наше время стало возможным конвертировать большие данные в коммерческий успех. Множество интернет-компаний, от поисковиков до социальных сетей, существуют исключительно благодаря возможности анализировать и продавать агрегированные данные о своих пользователях в форме рекомендательных и статистических моделей, обеспечивающих другим компаниям рост продаж их товаров и услуг. Феномен успеха интернет-магазинов связан не только с удобством выбора товаров и доставки, но и с возможностью точного таргетирования рекламы. Традиционные экономические субъекты, такие как банки и страховые компании, также повышают эффективность своей работы за счёт анализа больших данных. Весьма характерным выражением этой тенденции является крылатая фраза «данные – это новая нефть».

Развитие производительных вычислительных средств обеспечивает гигантский прогресс в обработке больших данных. Например, феномен больших языковых моделей является синергетическим эффектом больших данных (текстов и других видов информации), эффективных алгоритмов глубокого обучения и быстродействующих вычислительных платформ. Можно смело сказать, что чем больше данных удаётся собрать для обучения глубокой модели, тем более эффективной, мощной и полезной окажется такая модель.

Одним из ярких примеров понимания важности накопления, актуализации и использования больших данных во благо экономики государства является национальный проект «Экономика данных», объединяющий несколько прорывных направлений, каждое из которых в той или иной степени связано с обработкой информации.

Подобно любой ценности, данные тщательно охраняются. Для их защиты разработаны различные технические и криптографические методы, а также развитая правовая и регуляторно-нормативная база. Однако никакая защита не может считаться абсолютно надёжной, особенно в условиях постоянного прогресса в сфере высоких технологий обработки информации. Также под влиянием изменений в технологиях меняется и оценка рисков, связанных с перспективными и традиционными угрозами.

Рассмотрим задачу совместной обработки конфиденциальных данных, принадлежащих различным субъектам, с целью получения агрегированных моделей, полезных для субъектов-владельцев данных.

1 Елисеев Владимир Леонидович, кандидат технических наук, АО «ИнфоТеКС», ФГБОУ ВО Национальный исследовательский университет «Московский энергетический институт», Москва, E-mail: vlad-eliseev@mail.ru, ORCID: 0000-0002-9341-7475.

При этом важным условием является сохранение конфиденциальности данных в процессе их обработки, поскольку взаимное доверие субъектов друг к другу является ограниченным. Практически важным примером такой задачи является федеративное обучение глубоких моделей, которые вбирают в себя зависимости, выявленные в данных, и могут использоваться субъектами-владельцами данных в своей деятельности.

Обзор литературы

В обычных центрах обработки данных (ЦОД) реализуются политики организации доступа, обеспечивающие разделение потоков данных, хранилищ и вычислительных средств, арендованных или принадлежащих различным субъектам, которые будем называть *пользователями*. Фактически, для каждого из пользователей в ЦОД организуется изолированная от всех других пользователей среда – *виртуальный ЦОД* [1], состоящий из ресурсов, выделенных пользователю из общего пула физического ЦОД. Меры изоляции обычно определяются на организационно-техническом уровне, что означает наличие рисков, связанных с нарушением регламентов и характеристик системы защиты, к которым относятся ошибки и злонамеренные действия персонала ЦОД, а также сбои в работе оборудования и программного обеспечения системы защиты.

Криптографические методы защиты информации обычно применяются для организации доступа в виртуальный ЦОД и рассчитаны на защиту от внешнего нарушителя в телекоммуникационных каналах. В частности, трафик виртуального ЦОД шифруется при передаче наружу, в отрытую сеть. С точки зрения внешнего нарушителя, такая система представляет собой криптографически и организационно-технически защищенную сущность, которую обычно называют криптоанклавом.

Криптоанклав (англ. security enclave) получает и выдаёт данные исключительно в зашифрованном виде, расшифровывая их только внутри для обработки. Название этой концепции образовано словами «крипто» (от греч. kryptós – тайный, скрытый) и «анклав» (от фр. enclave, от лат. inclavatus – заключенный, запертый). С понятием криптоанклава тесно связаны технологии доверенных вычислений – Trusted Execution Environment (TEE).

Хорошо известным примером криптоанклава являются технологии Intel Software Guard Extensions (SGX) [2]. Она позволяет обрабатывать зашифрованные данные с помощью специального механизма центрального процессора, изолирующего программу от изменений (для предотвращения злонамеренного внедрения кода), а расшифрованные в процессе обработки данные – от инспекции другими программами. Реализация криптоанклава в виде механизма центрального процессора обладает тем недостатком, что существенно ограничивает производительность защищенной обработки данных выделенными страницами оперативной памяти. По этой причине SGX обычно используется только для хранения криптографических ключей и работы с ними, например, в процессе выполнения криптографических протоколов [3]. Для защищенной обработки больших данных SGX и другие подобные технологии не подходят.

Концепция криптоанклава может быть расширена на уровень вычислительной системы, кластера или даже всего ЦОД. В частности, виртуальный ЦОД может использоваться для реализации криптоанклава, однако в этом случае организационно-технических методов изоляции может оказаться недостаточно и для снижения рисков целесообразно использовать шифрование данных при их передаче по каналам внутри физического ЦОД.

Альтернативой криптоанклаву могли бы стать методы гомоморфной криптографии [4], которые обещают непосредственное выполнение вычислений над зашифрованными данными без их расшифрования. В 2009 году была предложена первая схема, обеспечивающая выполнение произвольных операций над зашифрованными данными [5], так называемое полное гомоморфное шифрование. Однако в настоящее время оно реализуется вычислительно чрезвычайно неэффективно, что на несколько порядков замедляет вычисления по сравнению с операциями над незашифрованными данными. Таким образом, гомоморфное шифрование в настоящее время не может использоваться для обработки больших данных.

Анализ показывает, что приемлемым подходом для обработки больших данных с сохранением их конфиденциальности является концепция криптоанклава, реализуемая в масштабе ЦОД при условии использования подходящих средств шифрования. Однако при совместной обработке конфиденциальных данных нескольких субъектов в одном криптоанклаве возникает проблема обеспечения доверия субъектов друг к другу, поскольку каждый из них равноправно обладает доступом в криптоанклав для загрузки своих данных и выгрузки результатов из него. Некоторые примеры совместной обработки конфиденциальных данных перечислены ниже:

- банковские модели оценки кредитоспособности клиентов (банковский скоринг);
- модели оценки риска страхования клиентов (страховой скоринг – страхование жизни, КАСКО и пр.);
- модели машинного обучения на объединенных выборках конфиденциальных данных;
- обработка любых конфиденциальных данных конфиденциальными же алгоритмами (например, экспертные системы диагностики заболеваний).

Федеративное обучение [6] является концепцией машинного обучения общей модели на основе использования данных нескольких субъектов без их прямого объединения. Задача федеративного обучения возникает в случае невозможности открытого соединения нескольких наборов обучающих данных в один. В частности, эта ситуация может возникать из-за ограничений на конфиденциальность отдельных наборов данных.

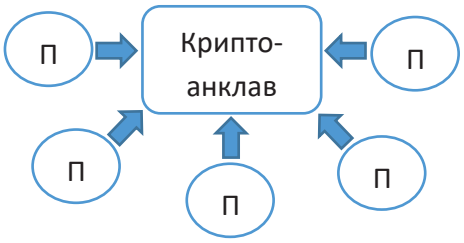
При использовании методов различных методов шифрования следует иметь в виду условия обеспечения конфиденциальности перед лицом тех или иных угроз. Например, одной из угроз для симметричного, асимметричного и постквантового шифрования являются действия внутреннего нарушителя. Если он обладает доступом к секретным ключам шифрования, то это нарушает конфиденциальность данных. В то же время в технологии квантового распределения ключей влияние внутреннего нарушителя минимизировано [7].

Рассмотрим архитектуру криптоанклава с защитой конфиденциальности данных от компрометации внутренним нарушителем на основе технологии квантового распределения ключей (КРК).

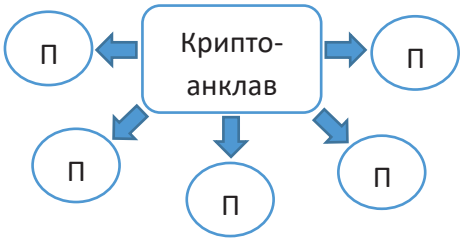
Криптоанклав для федеративного обучения

Целью функционирования криптоанклава обычно является создание каких-то обобщений данных для последующего использования этих обобщений для принятия решений. В рамках концепции федеративного обучения удобно назвать эти обобщения моделями.

Назовём *пользователями* криптоанклава (П) субъекты, загружающие свои данные в криптоанклав и получающие в результате обработки данных модели, которые, с одной стороны, созданы на основе данных, загруженных всеми пользователями, с другой – не содержащие эти данные в явном виде, допускающих их компрометацию. Таким образом, основные сценарии использования криптоанклава можно представить на рис. 1.



а) загрузка данных



б) выгрузка модели

Рис. 1. Сценарии использования криптоанклава

От обычного ЦОД криптоанклав отличается специальной политикой обеспечения безопасности данных, которая обусловлена тем, что, как правило, пользователи загружают свои данные в криптоанклав в расчёте, что эти данные не будут доступны другим пользователям. При этом все пользователи криптоанклава получают выгоду от того, что создаваемые в криптоанклаве модели создаются на основе объединенных данных всех пользователей.

Задачи, решаемые в криптоанклаве сродни задачам безопасных многосторонних вычислений (например, задача о миллионерах) и гомоморфной криптографии (вычисления над зашифрованными данными). В случае криптоанклава прикладные задачи можно решать классическим образом, но при этом сама политика работы с данными в криптоанклаве техническими мерами обеспечивает конфиденциальность этих данных.

На практике пользователи взаимодействуют с криптоанклавом через каналы коммуникаций, используемые как для передачи данных, являющихся конфиденциальными, так и для получения моделей, ценность которых также должна быть защищена от несанкционированного доступа. При этом пользователи криптоанклава не обязаны доверять друг другу, однако необходимо снизить риск компрометации данных вследствие реализации угрозы внутреннего нарушителя пользователя.

Анализ угроз конфиденциальности

Конфиденциальность данных при передаче по каналам коммуникаций может быть обеспечена как организационно-техническими (охрана линий связи), так и криптографическими мерами. При передаче данных через неконтролируемую среду (Интернет) обеспечить конфиденциальность организационно-техническими мерами невозможно, поэтому широко используются криптографические протоколы защиты передаваемых данных.

Все криптографические протоколы используют симметричные криптографические алгоритмы для шифрования данных в канале. Содержательные отличия касаются только способа распределения или выработки общего секретного ключа. Существуют следующие варианты решения этой задачи:

- доверенный курьер;
- протокол Диффи-Хеллмана;
- постквантовые протоколы (PQ-KEM);
- квантовое распределение ключей.

Таблица 1.

Уязвимость технологий распределения ключей

Технологии распределения ключей	Угрозы			
	Рост производительности классических компьютеров	**Квантовая атака Шора**	**Побочные каналы утечки**	**Внутренний нарушитель**
Доверенный курьер	–	–	–	Высокая уязвимость
Протокол Диффи-Хеллмана	Увеличение длины асимметричных ключей согласно закону Мура	Полностью компрометируется	Необходимо защищаться от утечек	Уязвим в любой момент времени
Постквантовые протоколы	– (предположительно неуязвимы)	–	Необходимо защищаться от утечек	Уязвим в любой момент времени
Квантовое распределение ключей	–	–	Необходимо защищаться от утечек	Уязвим только в моменты выработки первого квантового ключа

Каждый из вариантов имеет свои достоинства и недостатки. Перечислим общие угрозы, которые будем рассматривать, как влияющие на конфиденциальность криптографически защищенных данных:

- рост производительности классических компьютеров;
- квантовые атаки Шора и Гровера;
- побочные каналы утечки;
- внутренний нарушитель.

Квантовая атака Гровера одинаково влияет на конфиденциальность данных при любом способе распределения ключей, понижая стойкость симметричных криптографических алгоритмов до квадратного корня от числа возможных секретных ключей. То есть, при квантовой атаке Гровера симметричный ключ длиной 256 бит (число возможных ключей 2^{256}) будет обеспечивать стойкость, как если бы это был ключ длиной 128 бит без атаки Гровера (число возможных ключей $2^{128} = \sqrt{2^{256}}$. Данное снижение стойкости может быть легко компенсировано увеличением длины ключа в 2 раза, поэтому в настоящее время квантовая атака Гровера не считается приводящей к полной компрометации.

Уязвимость технологий распределения ключей к перечисленным выше угрозам сведена в таблицу 1.

Отметим одну важную особенность криптоанклава с точки зрения обеспечения криптографической защиты данных – пользователей, являющихся независимыми субъектами, при работе с криптоанклавами должны быть уверенными, что их данные не будут скомпрометированы вследствие реализации значимых угроз. При этом пользователи не могут влиять на защищенность каналов доступа других пользователей. В частности, внутренний нарушитель одного из субъектов доступа к криптоанклаву может нарушить конфиденциальность всей системы, если от него не будет создана адекватная защита.

Как видно из таблицы 1, единственным теоретически обоснованным способом почти полной защиты от внутреннего нарушителя является квантовое распределение ключей. Защита каналов доступа с помощью квантовых ключей гарантирует некомпрометируемость коммуникаций с криптоанклавом и обеспечивает доверие пользователей ко всей системе. Такую систему можно назвать *квантовым криптоанклавом*. Примером проекта, реализующего концепцию квантового криптоанклава, является Quantumacy [8]. В этом проекте, реализованном в рамках европейской инициативы OpenQKD в 2021-2022 годах, была рассмотрена модель проведения доверенных вычислений в криптоанклаве, доступ к которому обеспечивался с помощью КРК. В качестве модельных прикладных задач рассматривалось машинное обучение для диагностики заболеваний с наборами данных, получаемыми из различных источников. Доступ к источникам данных, согласно предложенной архитектуре, криптографически защищался с помощью технологии КРК.

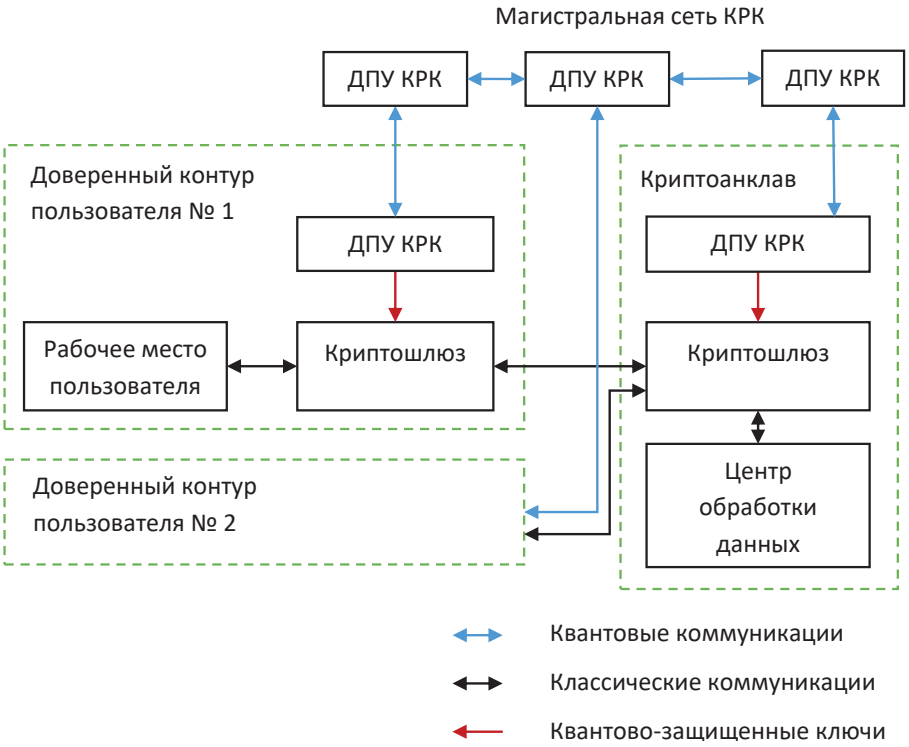


Рис. 2. Архитектура квантового криптоанклава

Архитектура квантового криптоанклава

В состав квантового криптоанклава (рис. 2) входят:

- доверенный промежуточный узел сети квантового распределения ключей (ДПУ КРК);
- криптошлюз, осуществляющий шифрование квантово-защищенными ключами данных между ЦОД и пользователями;
- центр обработки данных, в котором реализуются криптографические и организационно-технические меры защиты и производится совместная обработка данных, полученных от пользователей.

Для подключения к криптоанклаву в состав доверенного контура пользователя должны входить:

- доверенный промежуточный узел сети квантового распределения ключей (ДПУ КРК);
- криптошлюз, осуществляющий шифрование квантово-защищенными ключами данных между ЦОД и пользователями;
- рабочее место пользователя, посредством которого пользователь передаёт свой конфиденциальный набор данных в ЦОД и загружает полученную модель, а также осуществляет необходимые служебные операции при работе с криптоанклавом.

Магистральная сеть КРК [9] состоит из ДПУ КРК, соединённых каналами квантовых коммуникаций, обеспечивающих передачу квантово-защищенных ключей между криптошлюзами. Такой способ распределения криптографических ключей обеспечивает защиту от компрометации внутренним нарушителем.

Выводы

Предложенная архитектура квантового криптоанклава обеспечивает реализацию некомпрометируемого криптографически защищенного доступа в среду доверенных вычислений, реализуемую в ЦОД. По сравнению с концепцией криптоанклава новая архитектура снижает риски компрометации внутренним нарушителем. Технология квантового распределения ключей для обеспечения некомпрометируемости применяется в рамках современной концепции магистральных сетей КРК.

Литература

1. Bari M. F. et al. Data center network virtualization: A survey // IEEE communications surveys & tutorials. – 2012. – Т. 15. – №. 2. – С. 909–928.
2. Costan V., Devadas S. Intel SGX explained //IACR Cryptol, EPrint Arch. – 2016.
3. Park J., Kang B. B. EnclaveVPN: Toward Optimized Utilization of Enclave Page Cache and Practical Performance of Data Plane for Security-Enhanced Cloud VPN // Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses. – 2023. – С. 397–411. DOI: 10.1145/3607199.360721.
4. Fontaine C., Galand F. A survey of homomorphic encryption for nonspecialists // EURASIP Journal on Information Security. – 2007. – Т. 2007. – С. 1–10.

5. Gentry C. Fully homomorphic encryption using ideal lattices // Proceedings of the forty-first annual ACM symposium on Theory of computing. – 2009. – С. 169–178.
6. Bharati S. et al. Federated learning: Applications, challenges and future directions //International Journal of Hybrid Intelligent Systems. – 2022. – Т. 18. – №. 1–2. – С. 19-35. DOI: 10.3233/HIS-22000.
7. Прикладные квантовые технологии для защиты информации / Андрущенко А.С., Борисова А.В., Елисеев В.Л., Жиляев А.Е., Иванов О.А., Кармазиков Ю.В., Козлов С.К., Криштоп В.Г., Курнакова А.Д., Моисеевский А.Д., Попов В.Г., Рыбкин А.С. / под редакцией Втюриной А.Г., Елисеева В.Л. – 2-е изд., испр. – М: Медиа Группа «Авангард», 2024. 144 с.
8. «Quantumacy» project – investigating privacy-preserving forms of quantum communication – comes to a close | CERN QTI // URL: https://quantum.cern/news/announcement/quantumacy-project-investigating-privacy-preserving-forms-quantum-communication (дата обращения: 01.02.2025)
9. Елисеев В. Сети квантового распределения ключей – новый уровень сервисов информационной безопасности национальной сети Интернет / В. Елисеев // Интернет изнутри. – 2024. – № 20. – С. 10–15.

QUANTUM CRYPTO ENCLAVE FOR IMPLEMENTING UNCOMPROMISED TRUSTED DATA CENTERS

Eliseev V.L.[2]

Keywords: *crypto enclave, trusted computing, federated learning, quantum key distribution, quantum key distribution network.*

Purpose of the study: *development and justification of the architecture of a quantum-cryptographic system for protecting access to a data center with high requirements for the confidentiality of processed information belonging to various entities, using federated learning problem as the example.*

Methods of research: *systems analysis.*

Result(s): *the problem of ensuring the confidentiality of data belonging to different subjects during their joint processing is considered. The concept of a cryptoenclave is studied as an effective approach to implementing the task. An analysis of modern and prospective threats to cryptographic methods of information protection is carried out. The concept of a quantum cryptoenclave is proposed, combining technologies of cryptographic information protection and quantum key distribution. An example of a possible implementation of a quantum cryptoenclave for solving the problem of federated learning is given.*

Scientific novelty: *an architecture of a quantum cryptoenclave is proposed – a data center with cryptographic access protection using a quantum key distribution network with trusted intermediate nodes.*

References

1. Bari, M.F., Boutaba, R., Esteves, R., Granville, L.Z., Podlesny, M., Rabbani, M.G., ... & Zhani, M.F. (2012). Data center network virtualization: A survey. IEEE communications surveys & tutorials, 15(2), 909–928.
2. Costan, V. (2016). Intel SGX explained. IACR Cryptol, EPrint Arch.
3. Park, J., & Kang, B.B. (2023, October). EnclaveVPN: Toward Optimized Utilization of Enclave Page Cache and Practical Performance of Data Plane for Security-Enhanced Cloud VPN. In Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses (pp. 397–411).
4. Fontaine, C., & Galand, F. (2007). A survey of homomorphic encryption for nonspecialists. EURASIP Journal on Information Security, 2007, 1–10.
5. Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In Proceedings of the forty-first annual ACM symposium on Theory of computing (pp. 169–178).
6. Bharati, S., Mondal, M.R.H., Podder, P., & Prasath, V.S. (2022). Federated learning: Applications, challenges and future directions. International Journal of Hybrid Intelligent Systems, 18(1-2), 19–35.
7. Andrushhenko A.S., Borisova A.V., Eliseev V.L., Zhilyaev A.E., Ivanov O.A., Karmazikov Yu.V., Kozlov S.K., Krishtop V.G., Kurnakova A.D., Moiseevskij A.D., Popov V.G., & Rybkin A.S. (2024). Prikladnye kvantovye texnologii dlya zashhity informacii / ed. Vtyurinoj A.G., Eliseeva V.L. – 2nd edition. – M: Media Gruppa «Avangard», 2024. 144 p.
8. «Quantumacy» Project – Investigating Privacy-Preserving Forms of Quantum Communication – Comes to a Close | CERN QTI. (2022). https://quantum.cern/news/announcement/quantumacy-project-investigating-privacy-preserving-forms-quantum-communication.
9. Eliseev V. (2024). Seti kvantovogo raspredeleniya klyuchej – novyj uroven' servisov informacionnoj bezopasnosti nacional'noj seti Internet. Internet iznutri, 20, 10–15.

2 Vladimir L. Eliseev, Ph.D., JSC «InfoTeCS», National research university «Moscow power engineering institute», Moscow. E-mail: vlad-eliseev@mail.ru, ORCID: 0000-0002-9341-7475.

ОПРЕДЕЛЕНИЕ ДОСТОВЕРНОСТИ ОДНОКУБИТНЫХ ОПЕРАЦИЙ МЕТОДОМ РАНДОМИЗИРОВАННОГО БЕНЧМАРКИНГА

Бантыш Б. И.[1], Заливако И. В.[2], Колачевский Н. Н.[3], Федоров А. К.[4]

DOI: 10.21681/2311-3456-2025-3-105-109

Цель исследования: *определить эффективный и устойчивый к ошибкам метод оценки достоверности однокубитных квантовых операций, сформулировать и экспериментально реализовать алгоритм определения средней точности однокубитного квантового преобразования.*

Методы исследования: *теория зашумленных квантовых операций; рандомизация однокубитных квантовых схем, составленных из преобразований группы Клиффорда; теория унитарного 2-дизайна; экспериментальная апробация на квантовом вычислителе на базе ионов иттербия-171 в ловушке.*

Результаты исследования: *описан алгоритм оценки средней достоверности однокубитных операций и её статистической погрешности; экспериментальная апробация показала корректность модели экспоненциального спада вероятности получить целевое состояние при измерении с увеличением глубины квантовой схемы; результирующая экспериментальная средняя достоверность однокубитной квантовой операции равняется 99.94%.*

Научная новизна: *применение метода рандомизированного бенчмаркинга для определения средней достоверности однокубитных квантовых операций в квантовых вычислениях, в частности, для ионного квантового процессора на базе ионов иттербия-171.*

Ключевые слова: *квантовые вычисления, кубиты, ионы, однокубитные операции.*

Введение

Вычислительные возможности цифровых квантовых устройств определяются как количеством кубитов (элементарных информационных единиц в квантовом случае), так и точностью операций [1]. При этом даже в случае элементарных однокубитных операций определение точности (достоверности) требует специальных процедур [2–6]. Благодаря своей простоте и устойчивости к ошибкам приготовления и измерения одним из лидирующих подходов является определение достоверности однокубитной операции с помощью процедуры рандомизированного бенчмаркинга (randomized benchmarking) [2]. В настоящей работе мы детально описываем данный подход и представляем результаты его применения для определения достоверности однокубитных операций в ионном квантовом процессоре на базе ионов иттербия-171: полученная средняя точность клиффордовской однокубитной операции равняется $F = (99{,}944 \pm 0{,}002)$ %.

Рандомизированный бенчмаркинг

Процедура однокубитного рандомизированного бенчмаркинга представляет собой измерение случайных однокубитных квантовых схем, состоящих из 24 элементов однокубитной группы Клиффорда [2]. Поскольку группа Клиффорда обладает свойством 2-дизайна, в результате усреднения по случайным квантовым схемам каждый неидеальный случайный гейт эффективно ведёт себя как деполяризующий канал $E\gamma(\rho) = \gamma\rho + (1 - \gamma)\, I/2$, где γ – параметр канала, ρ – произвольная входная матрица плотности, а $I/2$ описывает полностью смешанное состояние кубита. Средняя достоверность клиффордовской операции при этом связана с параметром γ канала по формуле

$$F = \frac{1}{2} + (1 - \frac{1}{2})\gamma = \frac{1 + \gamma}{2}. \quad (1)$$

Для измерения параметра γ случайные схемы генерируются для различных глубин d. В конец каждой схемы добавляется специальный гейт таким образом, чтобы результат измерения в вычислительном базисе в идеальном случае всегда равнялся наперёд заданному значению («0» или «1»). Тогда можно показать, что для неидеальных гейтов вероятность получения целевого ответа есть

$$p(d) = A\gamma^d + B. \quad (2)$$

Параметры A и B зависят от величины ошибок приготовления и измерения. Таким образом, процедура рандомизированного бенчмаркинга заключается в экспериментальном измерении величины $\hat{p}$ для некоторого набора глубин d, аппроксимации

1 Бантыш Борис Игоревич, кандидат физико-математических наук, научный сотрудник НИТУ «МИСИС», Москва, Россия. E-mail: bbantysh60000@gmail.com
2 Заливако Илья Владимирович, кандидат физико-математических наук, высококвалифицированный научный сотрудник ФИАН им. П. Н. Лебедева, Москва, Россия. E-mail: zalivakoiv@lebedev.ru
3 Колачевский Николай Николаевич, д.ф.-м.н., профессор, член-корреспондент РАН, директор ФИАН им. П. Н. Лебедева, Москв, Россия. E-mail: kolachevsky@lebedev.ru
4 Федоров Алексей Константинович, директор Института физики и квантовой инженерии НИТУ «МИСИС», Москва, Россия. E-mail: lex1026@gmail.com

полученных значений функцией (2), и расчёта средней достоверности $\hat{F}$ клиффордовской операции по полученному значению $\hat{y}$.

Однокубитная группа Клиффорда

Однокубитная группа Клиффорда содержит 24 унитарных операции, включая единичную. Любая однокубитная унитарная матрица может быть представлена в виде следующего разложения:

$$U = Z(c)X(b)Z(a), \quad (3)$$

где $a,b,c = [0,2\pi)$ – независимые параметры,

$$X(\varphi) = \begin{pmatrix} \cos\varphi/2 & -i\sin\varphi/2 \\ -i\sin\varphi/2 & \cos\varphi/2 \end{pmatrix} \quad (4)$$

соответствует вращению вокруг оси x на угол φ,

$$Z(\varphi) = \begin{pmatrix} e^{-i\varphi/2} & 0 \\ 0 & e^{+i\varphi/2} \end{pmatrix} \quad (5)$$

соответствует вращению вокруг оси z на угол φ. В таблице 1 приведён список всех 24 преобразований группы Клиффорда и соответствующие параметры разложения (3). Такое разложение не является обязательным. При выполнении преобразований на физическом устройстве допускается произвольное разложение, реализующее заданную унитарную матрицу, однако разложение по формуле (3) минимизирует число физических операций на ионном квантовом вычислителе, так как преобразование $Z(\varphi)$ может быть выполнено виртуально со 100 % точностью.

Выбор целевого состояния

В результате выполнения случайной квантовой схемы может получиться одно из следующих 6 состояний:

$$|\varphi_1\rangle = |0\rangle,\ |\varphi_2\rangle = |1\rangle,\ |\varphi_3\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$
$$|\varphi_4\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},\ |\varphi_5\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}},\ |\varphi_6\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}.$$

В конец такой схемы необходимо добавить одно из преобразований из таблицы 1, чтобы привести состояние к целевому. В таблице 2 приведен возможный список таких преобразований.

Для каждого значения глубины схемы d рекомендуется в половине случаев выбирать целевое состояние $|0\rangle$, а в другой половине – целевое состояние $|1\rangle$. Это позволяет зафиксировать константу $B = 1/2$ в формуле (2), что повышает точность оценки $\hat{F}$ [7].

Выбор количества измерений

Пусть M_d есть число случайных схем для глубины d, а $N \geq M_d$ – общее число измерений для каждого d. Рекомендуется брать как можно более высокие значения данных параметров. В условиях, когда переключение к новой схеме требует относительно длительного времени, допускается брать меньшее значение M_d, но не менее 30. Число повторений каждой случайной схемы есть $n = [N/M_d]$. Остаток от деления распределяется поровну между произвольными

Таблица 1.

Список однокубитных преобразований из группы Клиффорда и соответствующие параметры разложения (3) с точностью до глобальной фазы

Преобразование	Матрица	a	b	c
U_1	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	0	π	0
U_2	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ -i & -i \end{pmatrix}$	3π/2	π/2	0
U_3	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	0	0	0
U_4	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -i & i \end{pmatrix}$	π/2	π/2	0
U_5	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}$	0	π/2	π/2
U_6	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$	π	π/2	π/2
U_7	$\begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}$	3π/2	π	0
U_8	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$	3π/2	π/2	π/2
U_9	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	π/2	0	0
U_{10}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	π/2	π/2	π/2
U_{11}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ i & -1 \end{pmatrix}$	0	π/2	π
U_{12}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$	π	π/2	π
U_{13}	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	π	π	0
U_{14}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ i & i \end{pmatrix}$	3π/2	π/2	π
U_{15}	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	π	0	0
U_{16}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$	π/2	π/2	π
U_{17}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -1 & -i \end{pmatrix}$	0	π/2	3π/2
U_{18}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ -1 & i \end{pmatrix}$	π	π/2	3π/2
U_{19}	$\begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix}$	π/2	π	0
U_{20}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$	3π/2	π/2	3π/2
U_{21}	$\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$	3π/2	0	0
U_{22}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$	π/2	π/2	3π/2
U_{23}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$	0	π/2	0
U_{24}	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix}$	π	π/2	0

Таблица 2.

Преобразования для приведения выходного состояния случайной схемы к целевому

Выходное состояние случайной схемы	$\|\varphi_1\rangle$	$\|\varphi_2\rangle$	$\|\varphi_3\rangle$	$\|\varphi_4\rangle$	$\|\varphi_5\rangle$	$\|\varphi_6\rangle$
Преобразование для приведения к состоянию $\|0\rangle$	U_3	U_1	U_4	U_2	U_5	U_6
Преобразование для приведения к состоянию $\|1\rangle$	U_1	U_3	U_2	U_4	U_6	U_5

$N \mathrm{mod} M_d$ схемами. Каждая схема реализуется в двух версиях: когда целевыми состояниями являются $|0\rangle$ или $|1\rangle$. На каждую из них приходится по $[n/2]$ повторений. Остаток от деления поочередно присваивается первой или второй версии схемы. Рекомендуется брать общее число измерений N не менее 1000.

При фиксированном максимальном числе M_{max} случайных схем для каждой глубины следует обратить внимание на следующее. При $M_{max} \geq 24^d$, вместо случайного выбора схем можно перебрать все комбинации из 24 гейтов. Для таких значений глубин требуется меньшее число квантовых схем. Если $24^{d-1} \leq M_{max} < 24^d$, для повышения точности усреднения рекомендуется сэмплировать случайные схемы без возвращения. При $M_{max} < 24^{d-1}$ квантовые схемы сэмплируются независимо с возвращением.

Число различных значений d рекомендуется выбирать не менее 10, однако для повышения качества определения достоверности следует брать больше значений до полного затухания экспоненциальной зависимости до 1/2. Дальнейшее повышение d не даёт повышения точности и не рекомендуется.

Оценка погрешности

Поскольку процедура бенчмаркинга включает в себя множество различных измерений, рекомендуется выполнять оценку погрешности определения достоверности посредством бутстрэпинга (bootstrapping) данных. Пусть R есть объём ресэмплинга (resampling), k – количество наблюдений целевого состояния в некоторой квантовой схеме, которая была измерена n раз. Тогда для данной схемы независимо генерируется R случайных величин $k_1, \ldots, k_R$ из биномиального распределения с вероятностью успеха k/n и числом испытаний n. Данная процедура выполняется для каждой измеренной квантовой схемы. Это позволяет построить R зависимостей вероятности успеха от глубины схемы, из которых затем определяется R значений достоверности $\hat{F}_1, \ldots, \hat{F}_R$. Тогда оценка достоверности есть $\hat{F} = \langle \hat{F}_i \rangle \pm 3\sigma_F$, где

$$\langle \hat{F}_i \rangle = \frac{1}{R} \sum_{i=1}^{R} \hat{F}_i, \; \sigma_F = \frac{1}{R} \sqrt{\sum_{i=1}^{R} (\hat{F}_i - \langle \hat{F}_i \rangle)^2}. \qquad (6)$$

Описанная процедура не требует дополнительных измерений и позволяет учесть особенности статистического распределения достоверности по отношению к дробовому шуму (она, однако, не учитывает особенностей случайного сэмплинга квантовых схем). Рекомендуется выбирать объём ресэмплинга R не менее 200.

Описание алгоритма

Входные параметры:

- $\{d\}$ – набор значений глубины квантовой схемы;
- M_{max} – максимальное число случайных схем на каждое d;
- $N \geq M_{max}$ – общее число измерений на каждое d;
- R – объём ресэмплинга.

Выходные значения:

- $\hat{F}$ – оценка достоверности последовательности двух $\pi/2$-импульсов.

Последовательность действий:

1. Задать R пустых наборов $\hat{p}_1, \ldots, \hat{p}_R = \{\}$.
2. Для каждого d:
   2.1. Задать $k_1 = \cdots = k_R = 0$.
   2.2. Если $M_{max} \geq 24^d$, сгенерировать набор квантовых схем $\{C\}$, состоящий из всех 24^d комбинаций преобразований из Таблицы 1 длины d. Если $24^{d-1} \leq M_{max} < 24^d$, сгенерировать набор из M_{max} случайных квантовых схем $\{C\}$, где каждая схема выбирается без возвращения из набора их всех 24^d комбинаций преобразований из Таблицы 1 длины d. Если $M_{max} < 24^{d-1}$, сгенерировать набор из M_{max} случайных квантовых схем $\{C\}$ глубины d, где каждое из d преобразований выбирается независимо и равномерно из Таблицы 1.
   2.3. Задать $j = 0$.
   2.4. Задать $zero\_has\_more\_shots = 1$.
   2.5. Для каждого C из $\{C\}$:
      2.5.1. $j \longrightarrow j + 1$.
      2.5.2. Задать $n \longrightarrow N/|C|$
      2.5.3. $n \longrightarrow n + 1$, если $j \leq N \mathrm{mod} |C|$.
      2.5.4. Если n – чётное число: задать $n_0 = n_1 = n/2$.
      2.5.5. Если n – нечётное число: $n_0 = (n+1)/2$, если $zero\_has\_more\_shots = 1$ и $n_0 = (n-1)/2$ в противном случае; $n_1 = n - n_0$; $zero\_has\_more\_shots \longrightarrow 1 - zero\_has\_more\_shots$.
      2.5.6. Рассчитать выходное состояние $|\varphi\rangle$ схемы C, используя эмулятор идеального квантового процессора.
      2.5.7. Составить квантовую схему C_0 путём добавления к C преобразования, которое задаст

целевое состояние $|0\rangle$ (см. табл. 2). Запустить схему C_0 на квантовом процессоре n_0 раз, получить число k_0 результатов измерения «0»*.

2.5.8. Составить квантовую схему C_1 путём добавления к C преобразования, которое задаст целевое состояние $|1\rangle$ (см. Таблицу 2). Запустить схему C_1 на квантовом процессоре n_1 раз, получить число k_1 результатов измерения «1»*.

2.5.9. Для каждого $i = 1, ..., R$:

2.5.9.1. Разыграть биномиальную случайную величину k_{i0} с вероятностью успеха k_0/n_0 и числом повторений n_0.

2.5.9.2. Разыграть биномиальную случайную величину k_{i1} с вероятностью успеха k_1/n_1 и числом повторений n_1.

2.5.9.3. $k_i \longrightarrow k_i + k_{i0} + k_{i1}$.

2.6. Для каждого $i = 1, ..., R$: добавить к набору $\hat{p}_i$ значение k_i/N.

3. Для каждого $i = 1, ..., R$:

3.1. Используя метод наименьших квадратов, определить коэффициенты $\hat{A}_i$ и $\hat{\gamma}_i$, которые наилучшим образом приближают зависимость $p(d) = A\gamma^d + 1/2$ к полученному набору значений $\hat{p}_i$.

3.2. Задать $\hat{F}_i = 1/2 + (1 - 1/2)\ \hat{\gamma}_i$.

4. Вычислить среднее арифметическое $\langle\hat{F}_i\rangle$ и среднеквадратичное отклонение σ_F по формуле (4).

5. $\hat{F}_i = \langle\hat{F}_i\rangle \pm 3\sigma_F$.

* При запуске квантовых схем на квантовом процессоре каждый отдельный гейт квантовой схемы раскладывается на нативные операции процессора. Объединение отдельных квантовых гейтов и последующее разложение не допускается.

Описание эксперимента

В качестве примера реализации данного алгоритма был проведен эксперимент с использованием ионного квантового вычислителя. В его основе лежит линейная ионная ловушка, в которой захвачено 10 ионов иттербия-171 [8]. Перед каждым экспериментальным циклом ионы подвергались доплеровскому лазерному охлаждению [9] до температуры порядка 1 мК. После этого все ионы методом оптической накачки подготавливались в состояние $|0\rangle = |^2S_{1/2}(F = 0, m_F = 0)$. Далее к ионам прикладывалась заданная цепочка операций при помощи микроволнового поля на частоте 12,6 ГГц, которое связывает кубитные уровни $|1\rangle$ и $|0\rangle = |^2S_{1/2}(F = 1, m_F = 0)$. Операции типа X(b), заданные матрицей (4), производятся путем приложения микроволновых импульсов при помощи антенны, резонансных с переходом $|0\rangle \longrightarrow |1\rangle$. Угол поворота b задается длительностью импульса. Операция $Z(a)$ является виртуальной [10] и производится путем сдвига фазы всех последующих за ней микроволновых импульсов на a. После выполнения всех операций в цепочке производится считывание квантового состояния кубитов. Считывание производится методом квантовых скачков [9].

Результаты и выводы

Алгоритм рандомизированного бенчмаркинга был применён к анализу средней достоверности однокубитного квантового преобразования, выполняемого на ионном квантовом вычислителе на одном из ионов в регистре. При этом использовалось разложение преобразований группы Клиффорда из таблицы 2. Ввиду изначально высокой точности гейта использовалась логарифмическая сетка значений глубины d. Максимальное число квантовых схем на каждую глубину $M_{max} = 100$, число измерений на каждую глубину $N = 20000$, объём ресэмплинга для оценки статистической погрешности $R = 500$. Как видно из рисунка 1, экспериментальные точки хорошо описываются теоретической экспоненциальной функцией. Небольшие отличия можно объяснить конечной выборкой случайных клиффордовских схем. Полученная средняя точность клиффордовской однокубитной операции равняется $F = (99.944 \pm 0.002)$ %.

Таким образом, детально описан метод для определения точности однокубитных операций, а также представлены результаты его применения для ионного квантового процессора.

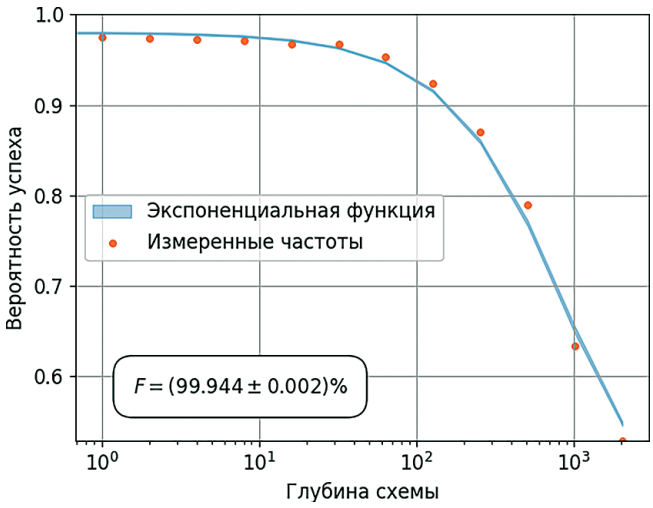


Рис. 1. Зависимость вероятности успеха (получения целевого состояния при измерении) от глубины однокубитной квантовой схемы. Показаны экспериментально измеренные вероятности и приближение точек экспоненциальной функцией $p(d) = A\gamma^d + 1/2$. Закрашенная область отображает доверительный интервал (1-й и 99-й процентили) функции для различных реализаций ресэмплинга.

Статья подготовлена по гранту № К1-2022-027 программы «Приоритет 2030».

Литература
1. Федоров, А. К. Вычислимое и невычислимое в квантовом мире: утверждения и гипотезы / А. К. Федоров, Е. О. Киктенко, Н. Н. Колачевский // Успехи физических наук. – 2024. – Т. 194, № 9. – С. 960-966. – DOI 10.3367/UFNr.2024.07.039721.
2. Randomized Benchmarking of Quantum Gates / E. Knill, D. Leibfried, R. Reichle, et al. // Physical Review A. 2008. № 77(1). С. 012307. DOI 10.1103/PhysRevA.77.012307.
3. Gate Set Tomography / E. Nielsen, J. K. Gamble, K. Rudinger, et al. // Quantum. 2021. № 5. С. 557. DOI 10.22331/q-2021-10-05-557.
4. Levy R., Luo D., Clark B. K. Classical shadows for quantum process tomography on near-term quantum computers // Physical Review Research. 2024. Vol. 6. Iss. 1. P. 013029. DOI: 10.1103/PhysRevResearch.6.013029
5. Non-Markovian quantum process tomography / G. A. L. White, F. A. Pollock, L. C. L. Hollenberg et al. // PRX Quantum. 2022. Vol. 3. Iss. 2. С. 020344. DOI: 10.1103/PRXQuantum.3.020344.
6. Variational quantum process tomography of unitaries / S. Xue, Y. Liu, Y. Wang et al. // Physical Review A. 2022. Vol. 105. Iss. 3. С. 032427. DOI: 10.1103/PhysRevA.105.032427.
7. Statistical analysis of randomized benchmarking / R. Harper, I. Hincks, C. Ferrie, et al. // Physical Review A. 2019. Vol. 99. Iss. 5. P. 052350. DOI 10.1103/PhysRevA.99.052350.
8. Realizing quantum gates with optically addressable Yb+ 171 ion qudits / M. A. Aksenov, I. V. Zalivako, I. A. Semerikov et al. // Physical Review A. 2023. Vol. 107. Iss. 5. – С. 052612. DOI: 10.1103/PhysRevA.107.052612.
9. Ejtemaee S., Thomas R., Haljan P. C. Optimization of Yb+ fluorescence and hyperfine-qubit detection // Physical Review A. 2010. № 82(6). С. 063419. DOI: 10.1103/PhysRevA.82.063419.
10. Efficient Z gates for quantum computing / D. C. McKay, C. J. Wood, S. Sheldon et al. // Physical Review A. 2017. № 96(2). С. 022330. DOI: 10.1103/PhysRevA.96.022330.

DETERMINING THE FIDELITY OF SINGLE-QUBIT OPERATIONS USING RANDOMIZED BENCHMARKING

Bantysh B. I.[5], Zalivako I. V.[6], Kolachevsky N. N.[7], Fedorov A. K.[8]

Keywords: *quantum computing, qubits, ions, single-qubit operations.*

The purpose of the research: *to determine an efficient and error-resilient method for assessing the fidelity of single-qubit quantum operations, as well as to formulate and experimentally implement an algorithm for determining the average accuracy of single-qubit quantum transformations*

Research methods: *the theory of noisy quantum operations, randomization of single-qubit quantum circuits composed of Clifford group transformations, the theory of unitary 2-design, experimental validation on a quantum computer based on ytterbium-171 trapped ions*

Research results: *an algorithm for estimating the average fidelity of single-qubit operations and its statistical error is described; experimental validation confirmed the correctness of the exponential decay model of the probability of obtaining the target state during measurement as the depth of the quantum circuit increases; the resulting experimental average fidelity of the single-qubit quantum operation is 99.94%*

Scientific novelty: *the application of the randomized benchmarking method to determine the average fidelity of single-qubit quantum operations in quantum computing, particularly for an ion-based quantum processor with ytterbium-171 ions.*

References
1. Fedorov, A. K. Vychislimoe i nevychislimoe v kvantovom mire: utverzhdenija i gipotezy / A. K. Fedorov, E. O. Kiktenko, N. N. Kolachevskij // Uspehi fizicheskih nauk. – 2024. – T. 194, № 9. – S. 960–966. – DOI 10.3367/UFNr.2024.07.039721.
2. Randomized Benchmarking of Quantum Gates / E. Knill, D. Leibfried, R. Reichle, et al. // Physical Review A. 2008. № 77(1). S. 012307. DOI: 10.1103/PhysRevA.77.012307.
3. Gate Set Tomography / E. Nielsen, J. K. Gamble, K. Rudinger, et al. // Quantum. 2021. № 5. S. 557. DOI 10.22331/q-2021-10-05-557.
4. Levy R., Luo D., Clark B. K. Classical shadows for quantum process tomography on near-term quantum computers // Physical Review Research. 2024. Vol. 6. Iss.1. P. 013029. DOI: 10.1103/PhysRevResearch.6.013029.
5. Non-Markovian quantum process tomography / G. A. L. White, F. A. Pollock, L. C. L. Hollenberg et al. // PRX Quantum. 2022. Vol.3. Iss. 2. S. 020344. DOI: 10.1103/PRXQuantum.3.020344.
6. Variational quantum process tomography of unitaries / S. Xue, Y. Liu, Y. Wang et al. // Physical Review A. 2022. Vol. 105. Iss. 3. S. 032427. DOI: 10.1103/PhysRevA.105.032427.
7. Statistical analysis of randomized benchmarking / R. Harper, I. Hincks, C. Ferrie, et al. // Physical Review A. 2019. Vol. 99. Iss. 5. P. 052350. DOI 10.1103/PhysRevA.99.052350.
8. Realizing quantum gates with optically addressable Yb+ 171 ion qudits / M. A. Aksenov, I. V. Zalivako, I. A. Semerikov et al. // Physical Review A. 2023. Vol. 107. Iss. 5. – S. 052612. DOI: 10.1103/PhysRevA.107.052612.
9. Ejtemaee S., Thomas R., Haljan P. C. Optimization of Yb+ fluorescence and hyperfine-qubit detection // Physical Review A. 2010. № 82(6). S. 063419. DOI: 10.1103/PhysRevA.82.063419.
10. Efficient Z gates for quantum computing / D. C. McKay, C. J. Wood, S. Sheldon et al. // Physical Review A. 2017. № 96(2). S. 022330. DOI: 10.1103/PhysRevA.96.022330.

5 Boris I. Bantysh, PhD, National University of Science and Technology «MISIS», e-mail: bbantysh60000@gmail.com
6 Ilya V. Zalivako, PhD, P.N. Lebedev Physical Institute of the Russian Academy of Sciences, e-mail: zalikes@yandex.ru
7 Nikolay N. Kolachevsky, Dr.Sc., professor, corresponding member of the Russian Academy of Sciences, P.N. Lebedev Physical Institute of the Russian Academy of Sciences, e-mail: kolachevsky@lebedev.ru
8 Aleksey K. Fedorov, PhD, National University of Science and Technology «MISIS», e-mail: lex1026@gmail.com

НОВЫЕ ПОДХОДЫ К ОЦЕНКАМ ИНФОРМАЦИИ ПЕРЕХВАТЧИКА В ПРОБЛЕМАХ КВАНТОВОЙ КРИПТОГРАФИИ

Кронберг Д. А.[1], Холево А. С.[2]

DOI: 10.21681/2311-3456-2025-3-110-117

Цель работы: *провести обзор новых аспектов вопроса извлечения информации из ансамблей квантовых состояний, продиктованных практическими задачами квантовой криптографии.*

Метод исследования: *использованы математические методы квантовой теории информации, в частности, процедура безошибочного различения квантовых состояний.*

Результаты исследования: *в работе проведен анализ литературы по теме оценок информации перехватчика в квантовой криптографии при наличии затухания в линии связи, в том числе в отсутствие квантовой памяти. Указаны особенности применения фундаментального информационного ограничения к количеству информации перехватчика в условиях затухания, продемонстрированы угрозы применения «ad hoc» методов борьбы с атакой безошибочным различением состояний. Сформулированы задачи нахождения эффективного преобразования перехватчика, использующего постселекцию, а также проведения измерения в условиях отсутствия квантовой памяти у перехватчика.*

Научная новизна: *научная новизна заключается в интеграции разрозненных подходов к задаче оценки информации перехватчика в квантовой криптографии и борьбы с атаками в условиях затухания. Обзор описывает особенности применения информационного ограничения к вопросам квантовой криптографии и формализует задачи, стоящие перед перехватчиком в условиях затухания.*

Ключевые слова: *квантовая криптография, квантовая теория информации, квантовые преобразования с постселекцией.*

1. Введение

Отличительное свойство квантовой информации, содержащейся в ансамбле квантовых состояний, – невозможность ее копирования [1]. Другое важное свойство – запрет на получение полной информации из ансамбля неортогональных чистых квантовых состояний, вытекающий из ограничения на количество классической информации, извлекаемой из ансамбля квантовых состояний [2]. Эти особенности квантовой информации лежат в основе протоколов передачи квантовой информации, препятствующих ее перехвату.

Уникальной чертой квантовой криптографии является принципиальная возможность математического доказательства безусловной стойкости протокола, в отличие от классической криптографии, где стойкость доказывается лишь против ряда известных атак. При этом представляют интерес как нижние, так и верхние оценки стойкости протоколов квантового распределения ключей.

Часто действия перехватчика в квантовой криптографии сводят к попыткам провести наилучшее измерение над ансамблем передаваемых состояний. Однако в данном обзоре мы хотим привлечь внимание к двум другим ресурсам перехватчика, важным для стойкости практических систем квантового распределения ключей:

1. Линии связи имеют затухание, и легитимные пользователи ожидают, что не все посылки будут зафиксированы на принимающей стороне. Это позволяет перехватчику проводить квантовые преобразования с постселекцией, при которых он иногда извлекает много информации, а иногда ему это не удается, и у перехватчика есть возможность блокировать посылки в последнем случае, что не будет обнаружено легитимными пользователями.
2. Легитимные пользователи общаются между собой, при этом они раскрывают некоторую информацию о ключе или об особенностях приготовлениях сигнала.

В статье будет рассмотрено то, как указанные ресурсы могут быть использованы перехватчиком и как их наличие изменяет формулировку и решение некоторых задач квантовой теории информации. Мы концентрируемся на случае большого затухания в линии связи, и поэтому рассматриваем атаки с нулевой ошибкой, значимые при большом затухании. В рамках данной работы мы не рассматриваем

1 Кронберг Д. А., кандидат физико-математических наук, старший научный сотрудник, Математический институт им. В. А. Стеклова Российской академии наук, г. Москва, Россия. ORCID: https://orcid.org/0000-0003-1652-6376. Scopus Author ID: 26648798700. E-mail: dmitry.kronberg@gmail.com

2 Холево Александр Семенович, доктор физико-математических наук, профессор, академик РАН, заведующий отделом, главный научный сотрудник, Математический институт им. В. А. Стеклова Российской академии наук, г. Москва, Россия. ORCID: https://orcid.org/0000-0001-5699-521X. Scopus Author ID: 6603727683. E-mail: holevo@mi-ras.ru

атаки, которым сопутствует внесение ошибки перехватчиком, актуальные при малых длинах линии связи; этот случай существенно сложнее из-за появления смешанных состояний.

2. Информация в условиях постселекции

Информационное ограничение [2] гласит, что при любом квантовом измерении из ансамбля квантовых состояний $\{p_j, \rho_j\}$ нельзя извлечь больше информации, чем $\mathcal{X}$-величина этого ансамбля

$$\mathcal{X} = H(\sum_j p_j \rho_j) - \sum_j p_j H(\rho_j),$$

где $H(\rho) = -Tr\rho \log \rho$ энтропия фон Неймана оператора плотности ρ. Мы хотим здесь подчеркнуть, что этот результат применим в условиях, когда учитываются все исходы измерения. Однако в квантовой криптографии в условиях сильного затухания не все сигналы доходят до принимающей стороны. Поэтому представляет интерес ситуация, при которой некоторые исходы измерения можно отбросить, заблокировав соответствующие сигналы, так что они не будут вносить вклад в распределяемый ключ. В такой ситуации $\mathcal{X}$-величина исходного ансамбля уже не может использоваться как верхняя оценка информации перехватчика.

Рассмотрим этот вопрос подробнее.

Самым простым примером нарушения информационного ограничения в условиях постселекции является так называемое безошибочное различение состояний [3, 4, 5]. В простейшем варианте при таком измерении двух неортогональных состояний $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ можно добиться в случае успеха их безошибочного различения. Но это достигается ценой возможности неудачи, которая имеет вероятность $|\langle\varphi_0|\varphi_1\rangle|$ (в несимметричном случае эту вероятность можно уменьшить для одного состояния, но тогда для другого состояния она увеличится; такая асимметрия может представлять интерес при различных исходных вероятностях состояний и максимизации средней вероятности успеха). Информационное ограничение выполняется в среднем в смысле математического ожидания классической информации, если учесть нулевую информацию в случае неудачи различения, но не выполняется, если рассматривать только успешные исходы.

На основе безошибочного различения состояний можно рассмотреть атаку в квантовой криптографии, при которой перехватчик проводит попытку безошибочного различения для каждого сигнала, и в случае неудачи блокирует посылку, а в случае удачи отправляет ее на принимающую сторону (в последнем случае перехватчик может применить дополнительные методы увеличения вероятности обнаружения посылки, такие как усиление сигнала). При такой атаке некоторые сигналы из-за блокировки не будут достигать принимающей стороны, но при передаче данных на большие расстояния легитимные пользователи и в отсутствие перехватчика ожидают потери существенной части сигналов. Поэтому начиная с некоторой критической длины линии связи атака безошибочным различением состояний оказывается возможной, то есть перехватчик не вносит больше затухания, чем ожидается легитимными сторонами. При этом перехватчик обладает полной информацией о ключе, поскольку посылал на принимающую сторону только те сигналы, о которых он получил полную информацию.

Возникает естественное предложение рассматривать безошибочное различение состояний как отдельную операцию, принципиально отличную от других атак в квантовой криптографии, и защищаться именно от нее. Возможные методы защиты [6] ставят своей целью уменьшить вероятность успеха безошибочного различения состояний, что приводит к увеличению критической длины линии связи, или вовсе сделать безошибочное различение невозможным. Они включают увеличение количества состояний [7, 8, 9], для которых в симметричном случае существуют верхние оценки вероятности успеха безошибочного различения [10], или линейную зависимость состояний [11]. Однако даже если безошибочное различение состояний невозможно, эффект превышения информационного ограничения за счет постселекции может иметь место [12].

Приведем простой пример ансамбля состояний, для которых невозможна операция безошибочного различения, но имеет место эффект превышения информационного ограничения. Рассмотрим двумерную систему (кубит) и два смешанных равновероятных квантовых состояния $\{\rho_0, \rho_1\}$. Для таких состояний невозможно безошибочное различение [13], поскольку их носители совпадают, и не существует элемента квантовой наблюдаемой, для которого соответствующая вероятность исхода была бы равна нулю для одного состояния и не равна нулю для другого состояния.

Рассмотрим, однако, разложение состояний $\{\rho_0, \rho_1\}$ по двум чистым состояниям

$$\begin{aligned} \rho_0 &= (1 - \alpha_0)\,|\varphi_0\rangle\langle\varphi_0| + \alpha_0\,|\varphi_1\rangle\langle\varphi_1|, \\ \rho_1 &= \alpha_1|\varphi_0\rangle\langle\varphi_0| + (1 - \alpha_1)\,|\varphi_1\rangle\langle\varphi_1|, \end{aligned} \qquad (1)$$

которое соответствует разложению по крайним точкам хорды на сфере Блоха. Для неортогональных состояний $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ возможно безошибочное различение, которое точно определит состояние в случае успеха. Если сопоставить успешным исходам безошибочного различения ортогональные состояния $\{|e_0\rangle, |e_1\rangle\}$, то в случае успеха имеем отображение

$$\rho_0 \longrightarrow \sigma_0 = (1-\alpha_0)\,|e_0\rangle\langle e_0| + \alpha_0\,|e_1\rangle\langle e_1|,$$
$$\rho_1 \longrightarrow \sigma_1 = \alpha_1\,|e_0\rangle\langle e_0| + (1-\alpha_1)\,|e_1\rangle\langle e_1|, \quad (2)$$

для которого коэффициенты $\{\alpha_0,\alpha_1\}$ не изменяются в случае равных вероятностей успеха для обоих состояний $\{|\varphi_0\rangle, |\varphi_1\rangle\}$.

Теперь можно построить квантовый канал, который отображает состояния $\{\sigma_0, \sigma_1\}$ в состояния $\{\rho_0, \rho_1\}$:

$$\Phi[\rho] = |\varphi_0\rangle\langle e_0|\rho|e_0\rangle\langle\varphi_0| + |\varphi_1\rangle\langle e_1|\rho|e_1\rangle\langle\varphi_0|. \quad (3)$$

Это канал с операторами Крауса $\{K_0 = |\varphi_0\rangle\langle e_0|, K_1 = |\varphi_1\rangle\langle e_1|\}$.

Следовательно, в силу свойства монотонности, $\mathcal{X}$-величина состояний $\{\sigma_0, \sigma_1\}$ строго превосходит $\mathcal{X}$-величину состояний $\{\rho_0, \rho_1\}$, если последние не коммутируют (то есть в случае, когда состояния $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ неортогональны). Таким образом, $\mathcal{X}$-величина монотонна относительно детерминированных преобразований, но не обязательно монотонна относительно постселективных. В силу ортогональности $|e_0\rangle$ и $|e_1\rangle$ $\mathcal{X}$-величина состояний $\{\sigma_0, \sigma_1\}$ в точности равна информации, которая извлекается из этих состояний при измерении в базисе $\{|e_0\rangle, |e_1\rangle\}$, и только что было показано, что эта информация больше $\mathcal{X}$-величины исходных состояний $\{\rho_0, \rho_1\}$, несмотря на то что для этих состояний невозможно безошибочное различение. Таким образом, эффект увеличения информации при постселективных измерениях, в том числе превышение $\mathcal{X}$-величины, это более общее явление, чем безошибочное различение состояний.

Эти рассуждения можно обобщить на два произвольных некоммутирующих квантовых состояния: для них также будет явное постселективное измерение, которое дает больше информации, чем $\mathcal{X}$-величина. Но для трех состояний это, вообще говоря, уже не так, и существует пример [12], когда $\mathcal{X}$-величина исходных состояний больше, чем информация, которую можно извлечь с помощью индивидуальных постселективных измерений: это одно из проявлений того эффекта, что коллективные измерения над состояниями эффективнее, чем индивидуальные [14, 15]. Информационное ограничение включает возможность коллективных измерений, а индивидуальные постселективные действия такой возможностью не обладают.

3. Постселективные действия перехватчика

В предыдущем разделе в качестве примера рассматривались постселективные измерения квантовых состояний, на выходе которых появляются классические (т.е. коммутирующие) сигналы, которые можно описать распределениями вероятностей. Но множество преобразований квантовых состояний шире, и в этом разделе будут рассмотрены постселективные преобразования с квантовыми состояниями на выходе. Они актуальны для построения успешных стратегий перехвата, использующих затухание.

Упомянутая выше атака безошибочным различением состояний, при которой перехватчик (Ева) пытается получить полную информацию о сигнале, передаваемом от легитимного участника (Алисы) другому легитимному участнику (Бобу), и блокирует состояния в случае неудачи, не очень эффективна для современных протоколов квантовой криптографии, поскольку они используют явные методы защиты от этой атаки, и вероятность успешного безошибочного различения состояний оказывается очень малой, что означает применимость атаки только на очень больших длинах линии связи.

Более эффективной атакой с нулевой ошибкой является атака, при которой Ева в случае успеха получает квантовое состояние, скоррелированное с сигналом Алисы, и после объявления базисов может совершить над ними нужное измерение. Будем стремиться построить такую атаку, но сначала рассмотрим задачу нахождения вероятности успеха довольно общего постселективного преобразования состояний. Преобразование, при котором состояния Алисы переходят в состояния Боба и Евы, можно описать так:

$$|\varphi_i\rangle_A \longrightarrow |\psi_i\rangle_B \otimes |\varepsilon_i\rangle_E, \quad (4)$$

где $\{|\varphi_i\rangle_A\}_i$ – набор состояний Алисы на входе, а $\{|\psi_i\rangle_B\}_i$ и $\{|\varepsilon_i\rangle_E\}_i$ – наборы состояний Боба и Евы соответственно.

Если учитывать состояния и в случае неудачи, то итоговое преобразование будет отображать состояния Алисы в сцепленные состояния на выходе:

$$|\varphi_i\rangle_A \longrightarrow \sqrt{p_{succ}}\,|\psi_i\rangle_B \otimes |\varepsilon_i\rangle_E \otimes |s\rangle_D + \sqrt{1-p_{succ}}\,|f_i\rangle_{BE} \otimes |f\rangle_D, \quad (5)$$

где p_{succ} – вероятность успеха, а $|s\rangle_D$ и $|f\rangle_D$ – взаимно ортогональные флаги успеха или неудачи во вспомогательном пространстве H_D. Их можно измерить, чтобы получить данные об успехе или неудаче преобразования. В случае успеха в пространстве $H_B \otimes H_E$ получается результат преобразования (4).

Условие изометричности отображения (5), которое отвечает его принципиальной реализуемости [15], записывается как

$$\langle\varphi_i|\varphi_j\rangle \longrightarrow p_{succ}\langle\psi_i|\psi_j\rangle\langle\varepsilon_i|\varepsilon_j\rangle + (1-p_{succ})\langle f_i|f_j\rangle \quad (6)$$

для всех возможных индексов $\{i, j\}$, что можно записать в матричной форме:

$$G_A = p_{succ}\,G_B \circ G_E + (1-p_{succ})\,G_F, \quad (7)$$

где G_A, G_B и G_E – матрицы Грама соответственно Алисы, Боба и Евы, то есть матрицы, составленные

из скалярных произведений, а $G_B \circ G_E$ – поэлементное (адамарово) произведение матриц. Матрица G_F соответствует скалярным произведениям в случае неудачи.

Состояния $\{|f_i\rangle_{BE}\}_{ij}$ в случае неудачи не столь важны, но требуется, чтобы этот набор состояний существовал, и это означает неотрицательную определенность соответствующей матрицы G_F. Поэтому для вероятности успеха p_{succ} преобразования (4) имеем условие (подробности, в том числе для более общего случая различных вероятностей успеха см. в [16, 17])

$$G_A - p_{succ}\, G_B \circ G_E \geq 0, \tag{8}$$

или следующую верхнюю оценку на вероятность успеха [17]

$$p_{succ} = \max_{G_E \geq 0} 2^{-D_{max}(G_B \circ G_E \| G_A)}, \tag{9}$$

где

$$D_{\max}(\rho\|\sigma) = -\log_2 \max\{\lambda : \sigma - \lambda\rho \geq 0\},$$

– max – относительная энтропия [18].

Теперь можно рассмотреть математическую задачу построения эффективной атаки в условиях затухания. Как уже отмечалось выше, это, с одной стороны, атака, дающая перехватчику много информации при малых вносимых помехах, а с другой – соответствующее преобразование (4) должно иметь большую вероятность успеха, чтобы атака была применима при небольших расстояниях между легитимными сторонами. Для этого нужно подобрать подходящие состояния для принимающей стороны $\{|\psi_i\rangle_B\}_i$ и для перехватчика $\{|\varepsilon_i\rangle_E\}_i$.

Состояния принимающей стороны должны вносить мало ошибок, давать высокую вероятность детектирования сигналов и при этом позволять построить преобразование (4) с высокой вероятностью успеха. С учетом этих требований их поиск может быть нетривиальной задачей, связанной с конкретными протоколами квантовой криптографии и используемой в них аппаратурой для детектирования состояний. Ниже мы рассмотрим важный частный случай когерентных состояний, а пока просто фиксируем состояния $\{|\psi_i\rangle_B\}_i$, тогда будет зафиксирована и матрица G_B, и требуется подобрать матрицу G_E, что проще формализовать математически.

Рассмотрим сначала случай получения Евой полной информации. Тогда для каждого базиса протокола соответствующие состояния Евы должны быть взаимно ортогональны. Если протокол использует N состояний, разделенных на $N/2$ базисов, то это означает, что матрица G_E содержит N нулей в позициях, соответствующих скалярным произведениям состояний одного базиса. Тогда остальные внедиагональные элементы матрицы G_E требуется заполнять числами, которые минимизируют величину $D_{\max}(G_B \circ G_E \| G_A)$, с учетом требования неотрицательности G_E. Это формализует построение эффективной атаки в квантовой криптографии, дающей полную информацию перехватчику для данных состояний $\{|\psi_i\rangle_B\}_i$ принимающей стороны, при этом мы не утверждаем оптимальность построенной атаки.

В более общем случае перехватчик может не стремиться получить полную информацию о ключе, что может быть невозможно для данной величины затухания. Тогда задачей перехватчика является поиск матрицы G_E, для которой его информация $I_{AE} \in (0,1]$ принимает фиксированное значение, и при этом максимизируется вероятность успеха преобразования. Рассмотрим случай симметричной атаки, при которой информация перехватчика в каждом базисе совпадает. Параметром атаки является модуль скалярного произведения $s \in [0,1)$ состояний каждого базиса, от которого информация перехватчика, равная $\mathcal{X}$-величине двух состояний базиса, зависит как

$$I_{AE} = h_2\left(\frac{1-s}{2}\right), \tag{10}$$

где $h_2(x) = -x \log_2 x - (1-x)\log_2(1-x)$ – бинарная энтропия.

Это означает, что соответствующие N элементов матрицы G_E в общем случае заполняются уже не нулями (как это происходило в случае требования полной информации перехватчика), а числами, равными по модулю s, и задачей является поиск остальных элементов матрицы G_E, которые бы максимизировали вероятность успеха преобразования (9) с учетом требования $G_E \geq 0$.

Для состояний Боба $\{|\psi_i\rangle_B\}_i$ уже нельзя учитывать лишь скалярные произведения и соответствующие матрицы Грама, поскольку сам вид состояний ограничен физическими характеристиками измеряемой аппаратуры: эти состояния не должны приводить к ошибке, либо, в более общем случае, должны давать небольшую ошибку. Поэтому математическая формализация имеет смысл именно для задачи поиска матрицы G_E.

Важным частным случаем является использование легитимными сторонами чистых когерентных состояний, которые характеризуются в том числе исходной интенсивностью μ_A. Тогда на стороне Боба логично использовать состояния того же вида, но с интенсивностью μ_B, которая является параметром атаки для оптимизации. Если обозначить вероятность детектирования состояния в зависимости от интенсивности как $P_{det}(\mu)$ (конкретная формула зависит от протокола), то условием применимости атаки для длины линии связи l является

$$p_{succ}\, P_{det}(\mu_B) = P_{det}(\mu_A\, 10^{-\frac{\delta l}{10}}), \tag{11}$$

где слева стоит вероятность детектирования сигналов при применении атаки, а справа – в отсутствие

атаки, но с затуханием в линии связи длины l с коэффициентом пропускания δ дБ/км. Отметим, что в этом случае также не утверждается оптимальность построенного преобразования.

Условие вида (11) можно привести и в других ситуациях для других параметров, таких как количество фотонов. В общем случае в задачу вмешивается физика возможных состояний Боба и ошибка в зависимости от оптической схемы на принимающей стороне.

Таким образом, главная практическая задача перехватчика в квантовой криптографии состоит в получении максимальной информации при данной длине линии связи l. Для решения этой задачи нужно найти как подходящие состояния Боба, что сопряжено с протоколом и аппаратурой, так и состояния Евы. Если состояния Боба фиксированы, то нахождение состояний Евы можно представить как математическую задачу поиска значений элементов матрицы Грама G_E, которые максимизируют вероятность (9) с учетом заполнения ряда элементов G_E фиксированными числами, равными по модулю s (параметр атаки, отвечающий различимости состояний внутри базиса, от которого информация перехватчика зависит согласно (10)).

4. Измерения с учетом дополнительной информации

Традиционно в квантовой криптографии предполагается, что перехватчик никак не ограничен технически. Но возможны подходы, при которых предполагается очень высокий, но все же не безграничный технологический уровень перехватчика [19]. Одним из предположений в этой модели является отсутствие у перехватчика долговременной квантовой памяти [20]. Это означает, прежде всего, что перехватчик не может совершить измерение, дождавшись объявления базисов, а должен делать это раньше, еще не зная базис, так что измерение не может зависеть от базиса.

В самом деле, легитимные пользователи могут просто задержать объявление базисов на некоторое время [21], скажем, на сутки, а предположение, что перехватчик может в течение суток хранить квантовые состояния в идеальной квантовой памяти это предположение о чрезвычайно высоком уровне перехватчика, которое может быть избыточным для существующих коммерческих приложений квантовой криптографии.

Рассмотрим перехватчика, который обладает состояниями $\{|\varepsilon_i\rangle_E\}_i$, что соответствует атаке (4) из предыдущего раздела (про некоторые отличия от этой атаки будет сказано ниже). Состояния с учетом битов ключа и базиса можно записать как

$$|\Psi_i\rangle = |k_i\rangle_K|b_i\rangle_B|\varepsilon_i\rangle_E, \tag{12}$$

где k_i – значение бита ключа, b_i – базис в данной позиции, $|\varepsilon_i\rangle$ – измеряемое состояние. Например, для протокола BB84, использующего 4 состояния $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$, разделенные на базисы Z (это состояния $\{|0\rangle,|1\rangle\}$) и X (состояния $\{|+\rangle,|-\rangle\}$), исходные состояния Алисы в этих обозначениях

$$\begin{aligned}
|\Phi_0\rangle &= |0\rangle_K|Z\rangle_B|0\rangle_A,\\
|\Phi_1\rangle &= |1\rangle_K|Z\rangle_B|1\rangle_A,\\
|\Phi_2\rangle &= |0\rangle_K|X\rangle_B|+\rangle_A,\\
|\Phi_3\rangle &= |1\rangle_K|X\rangle_B|-\rangle_A,
\end{aligned} \tag{13}$$

а состояния перехватчика после взаимодействия

$$\begin{aligned}
|\Psi_0\rangle &= |0\rangle_K|Z\rangle_B|\varepsilon_0\rangle_E,\\
|\Psi_1\rangle &= |1\rangle_K|Z\rangle_B|\varepsilon_1\rangle_E,\\
|\Psi_2\rangle &= |0\rangle_K|X\rangle_B|\varepsilon_2\rangle_E,\\
|\Psi_3\rangle &= |1\rangle_K|X\rangle_B|\varepsilon_3\rangle_E.
\end{aligned} \tag{14}$$

Важно, что перехватчик, совершая измерение над подсистемой E, стремится получить информацию о ключе K, но при этом он знает, что получит информацию B о базисе, и эта информация может увеличить информацию о ключе. Но измерение при этом не может зависеть от подсистемы B, поскольку на момент измерения доступа к этой подсистеме нет. Следовательно, стоит задача подбора наблюдаемой над E, которая бы максимизировала информацию

$$I(K;E|B), \tag{15}$$

но которая сама бы не зависела от B.

Эта задача отличается от максимизации $I(K;E)$ без учета B; последняя в приведенном примере является задачей получения максимума информации при измерении смешанных состояний

$$\begin{aligned}
\rho_0 &= \frac{1}{2}\left(|\varepsilon_0\rangle\langle\varepsilon_0| + |\varepsilon_2\rangle\langle\varepsilon_2|\right),\\
\rho_1 &= \frac{1}{2}\left(|\varepsilon_1\rangle\langle\varepsilon_1| + |\varepsilon_3\rangle\langle\varepsilon_3|\right),
\end{aligned} \tag{16}$$

Также задача отличается и от максимизации $I(K;E)$ в условиях знания B, поскольку в последнем случае речь уже идет о различении либо состояний $\{|\varepsilon_0\rangle, |\varepsilon_1\rangle\}$ (в базисе Z), либо состояний $\{|\varepsilon_2\rangle, |\varepsilon_3\rangle\}$ (в базисе X).

В качестве примера рассмотрим ситуацию, которая может возникнуть при атаке разделением по числу фотонов [22] на реализацию протокола BB84 на когерентных состояниях. Пусть исходная посылка содержала 3 фотона, и перехватчик отвел два фотона себе, а один фотон направил на принимающую сторону. Состояния Евы (14) в таком случае принимают вид

$$\begin{aligned}
|\Psi_0\rangle &= |0\rangle_K|Z\rangle_B|0\rangle_E^{\otimes 2},\\
|\Psi_1\rangle &= |1\rangle_K|Z\rangle_B|1\rangle_E^{\otimes 2},\\
|\Psi_2\rangle &= |0\rangle_K|X\rangle_B|+\rangle_E^{\otimes 2},\\
|\Psi_3\rangle &= |1\rangle_K|X\rangle_B|-\rangle_E^{\otimes 2}.
\end{aligned} \tag{17}$$

Если обращаться с этими состояниями как в задаче Хелстрома о различении двух смешанных состояний [23], то при различении состояний

$$\rho_0 = \frac{1}{2}\ (|00\rangle\langle 00| + |{+}{+}\rangle\langle{+}{+}|),$$
$$\rho_1 = \frac{1}{2}\ (|11\rangle\langle 11|+|{-}{-}\rangle\langle{-}{-}|) \qquad (18)$$

неизбежна ошибка. В то же время, если учесть, что базис потом станет известен, то полную информацию о ключе дает наблюдаемая

$$M_{0Z} = |0\rangle\langle 0| \otimes I,$$
$$M_{1Z} = |1\rangle\langle 1| \otimes I,$$
$$M_{0X} = I \otimes |+\rangle\langle +|, \qquad (19)$$
$$M_{1X} = I \otimes |-\rangle\langle -|,$$

соответствующая измерению первого фотона в базисе Z, а второго фотона в базисе X. После объявления базиса Ева получает информацию о том, в каком базисе исход соответствует биту ключа, а в каком базисе он неинформативен.

Этот пример показывает, что оптимальная по Хелстрому наблюдаемая не обязательно оптимальна в смысле максимизации величины (15).

Отметим, что мы использовали преобразование вида (4) и выходные состояния Евы $\{|\varepsilon_i\rangle_E\}_i$, как и в предыдущем разделе. Но следует иметь в виду, что если раньше эффективность этого преобразования понималась в том смысле, что нужно добиться наибольшей $\mathcal{X}$-величины внутри базиса, то в условиях отсутствия квантовой памяти у перехватчика преобразование вида (4) или его обобщение должны строиться из расчета на увеличение величины (15), что может привести к другому виду эффективного преобразования.

Говоря об отсутствии квантовой памяти у перехватчика, мы в первую очередь рассматривали его незнание базиса на момент измерения. Но есть еще одно, менее тривиальное, следствие отсутствия квантовой памяти, а именно то, что перехватчику уже не имеет смысла совершать коллективные измерения. Известно, что коллективные измерения дают больше информации, чем индивидуальные [14, 15, 24], именно поэтому в квантовой криптографии для учета информации перехватчика используется $\mathcal{X}$-величина, а не достижимая информация при индивидуальных измерениях. Но для эффективного применения коллективных измерений необходимо знание набора кодовых слов для проектирования больших кортежей состояний. Если же перехватчик не знает набор кодовых слов, он уже не может извлечь выгоду из коллективных измерений, даже если кратковременная квантовая память позволяет ему собрать несколько состояний и провести над ними коллективное измерение (см. теорему 2 в [24]). Поэтому в условиях отсутствия квантовой памяти для оценки информации перехватчика следует использовать информацию, достижимую при индивидуальных измерениях.

5. Заключение

В этой статье рассматривалась задача извлечения информации из ансамбля квантовых состояний и был дан обзор новых подходов к этой задаче, которые становятся актуальными в практических условиях квантовой криптографии.

При квантовом распределении ключей на большие расстояния неизбежно затухание в линии связи, и легитимные пользователи предполагают возможность детектирования на принимающей стороне не всех отправленных сигналов. В этих условиях перехватчик может блокировать часть посылок, и эта блокировка не будет замечена. Возможность отбирать часть посылок для отправки на принимающую сторону (т.е. проводить постселекцию) – важный ресурс перехватчика в квантовой криптографии, и в разделе 2 рассматривалось, как этот ресурс влияет на ограничения информации, извлекаемой из ансамбля квантовых состояний. Фундаментальное информационное ограничение выполняется в смысле математического ожидания информации, когда все исходы (в том числе неудачные для перехватчика) были приняты во внимание, но уже не выполняется, если был произведен отбор удачных результатов. Приведен пример, когда информация после постселекции оказывается больше, чем $\mathcal{X}$-величина исходных состояний. Было продемонстрировано, что указанное явление более общее, чем хорошо известное в квантовой теории информации безошибочное различение состояний, так как в приведенном примере оно невозможно. Следовательно, те меры, которые в протоколах квантовой криптографии используются для противодействия атаке безошибочным различением состояний, не обязательно эффективны против общей атаки с использованием постселекции. Важным выводом является то, что $\mathcal{X}$-величина исходных состояний не является верхней оценкой информации перехватчика при использовании им постселекции в условиях затухания.

Раздел 3 посвящен вопросу эффективного использования затухания перехватчиком. Было построено постселективное преобразование, которое дает перехватчику много информации о ключе в случае успеха. При этом становится актуальным использование еще одного важного ресурса, а именно информации, которую легитимные стороны раскрывают при объявлении базисов. Перехватчик не может построить преобразование с учетом этой информации, потому что не обладает ей на момент совершения преобразования, но строит преобразование с учетом дальнейшего получения этой информации.

Поэтому задача перехватчика состоит в том, чтобы сделать состояния каждого базиса как можно более различимыми, в то время как соотношения между векторами разных базисов не играют роли и могут быть любыми. В терминах матриц Грама это означает заполнение матрицы G_E рядом элементов с фиксированным модулем, и остальных позиций числами, при которых вероятность успеха оказывается максимальной. Эффективные состояния Боба при этом сложнее формализовать, так как их вид продиктован в том числе физическими аспектами протокола квантовой криптографии.

В разделе 4 была рассмотрена задача построения эффективного измерения, с учетом последующего объявления информации о базисах. Эта задача актуальна при отсутствии у перехватчика долговременной квантовой памяти, что в настоящее время является одной из допустимых моделей в квантовой криптографии. В этом случае оптимальной наблюдаемой уже не обязательно будет наблюдаемая оптимального различения двух смешанных квантовых состояний, соответствующих разным битам ключа. Это связано с тем, что перехватчик получает информацию о базисе приготовления состояний, и может улучшить результаты измерения в соответствии с этой информацией.

Темой будущих исследований может быть как решение задач, рассмотренных в настоящей статье, так и исследование ситуации с внесением перехватчиком ошибки при построении атаки, что означает дальнейшее сближение верхних и нижних оценок стойкости в квантовой криптографии.

Исследование выполнено за счет гранта Российского научного фонда № 24-11-00145, https://rscf.ru/project/24-11-00145/

Литература

1. W. K. Wootters, W. H. Zurek, A single quantum cannot be cloned. Nature, 299(5886). 802-803 (1982).
2. Холево А. С. Некоторые оценки для количества информации, передаваемого квантовым каналом связи // Проблемы передачи информации, 9(3), 3–11 (1973).
3. D. Ivanovic, How to differentiate between non-orthogonal states. Physics Letters A. 123(6), 257–259 (1987).
4. D. Dieks, Overlap and distinguishability of quantum states. Physics Letters A, 126(5-6), 303–306 (1988).
5. Peres, How to differentiate between non-orthogonal states. Physics Letters A. 128(1-2), 19 (1988).
6. Gaidash, A. Kozubov, G. Miroshnichenko, Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems. JOSA B, 36(3), B16-B19 (2019).
7. Молотков С. Н. О секретности волоконных систем квантовой криптографии без контроля интенсивности квазиоднофотонных когерентных состояний // Письма в ЖЭТФ, 101(8), 637–643 (2015).
8. K. S. Kravtsov, S. N. Molotkov, Practical quantum key distribution with geometrically uniform states. Physical Review A, 100(4), 042329 (2019). https://arxiv.org/pdf/1906.10978.
9. Gaidash, G. Miroshnichenko, A. Kozubov, Subcarrier wave quantum key distribution with leaky and flawed devices. JOSA B, 39(2), 577–585 (2022). DOI:10.1364/JOSAB.439776.
10. Chefles, S. M. Barnett, Optimum unambiguous discrimination between linearly independent symmetric states. Physics letters A, 250(4–6), 223–229 (1998). https://arxiv.org/pdf/quant-ph/9807023.
11. Gaidash, A. Kozubov, G. Miroshnichenko, Overcoming unambiguous state discrimination attack with the help of Schrödinger Cat decoy states. arXiv preprint arXiv:1808.08145 (2018).
12. N. R. Kenbaev, D. A. Kronberg, Quantum postselective measurements: Sufficient condition for overcoming the Holevo bound and the role of max-relative entropy. Physical Review A, 105(1), 012609 (2022). DOI:10.1103/PhysRevA.105.012609.
13. U. Herzog, J. A. Bergou, Optimum unambiguous discrimination of two mixed quantum states. Physical Review A, 71(5), 050301 (2005).
14. Холево А. С. Квантовые теоремы кодирования // Успехи математических наук, 53(6) (324), 193–230 (1998).
15. Холево А. С. Математические основы квантовой информатики // Лекц. курсы НОЦ, 30, МИАН, М., 2018, 118 с.
16. Chefles, R. Jozsa, A. Winter, On the existence of physical transformations between sets of quantum states. International Journal of Quantum Information, 2(01), 11–21 (2004).
17. D. A. Kronberg, Success probability for postselective transformations of pure quantum states. Physical Review A, 106(4), 042447 (2022). DOI:10.1103/PhysRevA.106.042447.
18. N. Datta, Min- and max-relative entropies and a new entanglement monotone. IEEE Transactions on Information Theory, 55(6), 2816–2826 (2009).
19. B. Damgård, S. Fehr, L. Salvail, C. Schaffner, Cryptography in the bounded-quantum-storage model. SIAM Journal on Computing, 37(6), 1865–1890 (2008).
20. H. Bechmann-Pasquinucci, Eavesdropping without quantum memory. Physical Review A Atomic, Molecular, and Optical Physics, 73(4), 044305 (2006).
21. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography. Reviews of modern physics, 74(1), 145 (2002).
22. G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, Limitations on practical quantum cryptography. Physical Review Letters, 85(6), 1330 (2000).
23. К. Хелстром, Квантовая теория проверки гипотез и оценивания. Мир, 1979.
24. M. Sasaki, K. Kato, M. Izutsu, O. Hirota, Quantum channels showing superadditivity in classical capacity. Physical Review A, 58(1), 146 (1998).

NEW APPROACHES TO EAVESDROPPER INFORMATION BOUNDS IN QUANTUM CRYPTOGRAPHY PROBLEMS

Kronberg D. A.[3], Holevo A. S.[4]

Keywords: *quantum cryptography, quantum information theory, postselective quantum transformations.*

Purpose of work *is to review new aspects for the task of information extraction from ensembles of quantum states, dictated by practical tasks of quantum cryptography.*

Research methods: *mathematical methods of quantum information theory, in particular, unambiguous discrimination of quantum states.*

Results of the study: *the paper analyzes the literature on the topic of eavesdropper information bounds in quantum cryptography in the presence of channel attenuation, including in the absence of quantum memory. The features of application of the fundamental information bound to the eavesdropper information in the presence of attenuation, the threats of application of ad hoc countermeasures for unambiguous state discrimination attack are demonstrated. The problems of finding an effective postselective eavesdropping transformation, as well as measurement in the absence of eavesdropper's quantum memory, are formulated.*

Scientific novelty: *the scientific novelty consists in the integration of disparate approaches to the problem of eavesdropper information bounds in quantum cryptography and resisting attacks in case of lossy channel. The review describes the peculiarities of applying information bound to quantum cryptography problems and formalizes the challenges facing the eavesdropper under attenuation conditions.*

References

1. W. K. Wootters, W. H. Zurek, A single quantum cannot be cloned. Nature, 299(5886). 802-803 (1982).
2. Holevo A. S. Nekotorye ocenki dlja kolichestva informacii, peredavaemogo kvantovym kanalom svjazi // Problemy peredachi informacii, 9(3), 3–11 (1973).
3. D. Ivanovic, How to differentiate between non-orthogonal states. Physics Letters A. 123(6), 257–259 (1987).
4. D. Dieks, Overlap and distinguishability of quantum states. Physics Letters A, 126(5-6), 303–306 (1988).
5. Peres, How to differentiate between non-orthogonal states. Physics Letters A. 128(1-2), 19 (1988).
6. Gaidash, A. Kozubov, G. Miroshnichenko, Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems. JOSA B, 36(3), B16-B19 (2019).
7. Molotkov S. N. O sekretnosti volokonnyh sistem kvantovoj kriptografii bez kontrolja intensivnosti kvaziodnofotonnyh kogerentnyh sostojanij // Pis'ma v ZhJeTF, 101(8), 637–643 (2015).
8. K. S. Kravtsov, S. N. Molotkov, Practical quantum key distribution with geometrically uniform states. Physical Review A, 100(4), 042329 (2019). https://arxiv.org/pdf/1906.10978
9. Gaidash, G. Miroshnichenko, A. Kozubov, Subcarrier wave quantum key distribution with leaky and flawed devices. JOSA B, 39(2), 577–585 (2022). DOI:10.1364/JOSAB.439776.
10. Chefles, S. M. Barnett, Optimum unambiguous discrimination between linearly independent symmetric states. Physics letters A, 250(4–6), 223–229 (1998). https://arxiv.org/pdf/quant-ph/9807023.
11. Gaidash, A. Kozubov, G. Miroshnichenko, Overcoming unambiguous state discrimination attack with the help of Schrödinger Cat decoy states. arXiv preprint arXiv:1808.08145 (2018).
12. N. R. Kenbaev, D. A. Kronberg, Quantum postselective measurements: Sufficient condition for overcoming the Holevo bound and the role of max- relative entropy. Physical Review A, 105(1), 012609 (2022). DOI:10.1103/PhysRevA.105.012609.
13. U. Herzog, J. A. Bergou, Optimum unambiguous discrimination of two mixed quantum states. Physical Review A, 71(5), 050301 (2005).
14. Holevo A. S. Kvantovye teoremy kodirovanija // Uspehi matematicheskih nauk, 53(6) (324), 193–230 (1998).
15. Holevo A. S. Matematicheskie osnovy kvantovoj informatiki // Lekc. kursy NOC, 30, MIAN, M., 2018, 118 s.
16. Chefles, R. Jozsa, A. Winter, On the existence of physical transformations between sets of quantum states. International Journal of Quantum Information, 2(01), 11–21 (2004).
17. D. A. Kronberg, Success probability for postselective transformations of pure quantum states. Physical Review A, 106(4), 042447 (2022). DOI:10.1103/PhysRevA.106.042447.
18. N. Datta, Min- and max-relative entropies and a new entanglement monotone. IEEE Transactions on Information Theory, 55(6), 2816–2826 (2009).
19. B. Damgård, S. Fehr, L. Salvail, C. Schaffner, Cryptography in the bounded-quantum-storage model. SIAM Journal on Computing, 37(6), 1865–1890 (2008).
20. H. Bechmann-Pasquinucci, Eavesdropping without quantum memory. Physical Review A Atomic, Molecular, and Optical Physics, 73(4), 044305 (2006).
21. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography. Reviews of modern physics, 74(1), 145 (2002).
22. G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, Limitations on practical quantum cryptography. Physical Review Letters, 85(6), 1330 (2000).
23. K. Helstrom, Kvantovaja teorija proverki gipotez i ocenivanija. Mir, 1979.
24. M. Sasaki, K. Kato, M. Izutsu, O. Hirota, Quantum channels showing superadditivity in classical capacity. Physical Review A, 58(1), 146 (1998).

3 Kronberg D.A., PhD in Physics and Mathematics, Senior Researcher, Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow, Russia. ORCID: https://orcid.org/0000-0003-1652-6376. Scopus Author ID: 26648798700. E-mail: dmitry.kronberg@gmail.com

4 Kholevo Alexander Semenovich, Doctor of Physical and Mathematical Sciences, Professor, Academician of the Russian Academy of Sciences, Head of Department, Chief Researcher, Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow, Russia. ORCID: https://orcid.org/0000-0001-5699-521X. Scopus Author ID: 6603727683, E-mail: holevo@mi-ras.ru

CYBERSECURITY ISSUES

SCIENTIFIC PEER-REVIEWED JOURNAL

2025, № 3 (67)

Cybersecurity Issues is a research periodical scientific and practical publication specializing in information security.
Published six times a year

https://cyberrus.info

The journal is being published from 2013
(Registration Certificate PI No. FS 77-75239).
CrossRef number (DOI): 10.21681/2311-3456

The journal is included in the Russian list of peer-reviewed academic publications of the Higher Attestation Commission (VAK), it is registered in the Russian Science Citation Index (RSCI/RINTs) on the Web of Science (WoS) platform and holds the 1st place in its cyber security rating. The journal's articles are available in full text

Founder and publisher
JSC «NPO «Echelon»
Postal address: Elektrozavodskaya str., 24, bld. 1, 107023, Moscow, Russia
E-mail: editor@cyberrus.info

CONTENTS

Эшелон
комплексная безопасность

{KOMRAD}
Enterprise SIEM

ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ И МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

KOMRAD Enterprise SIEM позволяет осуществлять централизованный сбор событий ИБ, выявлять инциденты ИБ и оперативно на них реагировать. Применение комплекса позволяет эффективно выполнять требования, предъявляемые регуляторами к защите персональных данных, к обеспечению безопасности государственных информационных систем и контролю критической информационной инфраструктуры предприятия. KOMRAD позволяет отправлять данные о событиях и инцидентах ИБ во внешние системы (например, ГосСОПКА).

- Визуальный конструктор запро и директив корреляции
- Высокая производительность
- Гибкая интеграция с нестандар источкниками событий
- Широкий спектр поддержки источников событий
- Ролевая модель управления доступом
- Оперативное оповещение об инциденте
- Масштабируемость

Чтобы получить демо-версию KOMRAD Enterprise SIEM или заказать пилот у наших партнеров в вашем регионе, свяжитесь с нашим отделом продаж по e-mail: sales@npo-echelon.ru.

CYBERSECURITY ISSUES
VOPROSY KIBERBEZOPASNOSTI

№3 2025

Университет Сириус

10 лет
ОБРАЗОВАТЕЛЬНОМУ ЦЕНТРУ

www.cyberrus.info
editor@cyberrus.info