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