Вводное слово ректора Университета Иннополис А. Г. Тормасова

Дорогие читатели!

Предлагаемая вашему вниманию монография посвящена решению одной из актуальных проблем цифровой экономики Российской Федерации — *обеспечению устойчивости современных блокчейн-экосистем и платформ государства и бизнеса* в условиях атак злоумышленников с использованием квантовых компьютеров[1]. Дело в том, что, несмотря на широкое распространение технологии блокчейн и распределенного реестра (DLT), применяемые криптопримитивы (хеш-функции, электронные подписи и схемы асимметричного шифрования) уже недостаточны для обеспечения требуемой киберустойчивости блокчейна.

Достижения IBM, а также ряда других высокотехнологичных производителей квантовых компьютеров убедительно свидетельствуют о реалистичности так называемой квантовой угрозы к 2025 году. Поэтому в технологически развитых странах мира, главным образом в США, Китае, России и государствах Евросоюза, запланирован переход к постквантовой криптографии[2].

Актуальность тематики исследований подтверждается требованиями Паспорта национального проекта «Национальная программа “Цифровая экономика Российской Федерации” (утв. Президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 года № 7). В котором «обеспечение устойчивости и безопасности функционирования информационной инфраструктуры и сервисов передачи, обработки и хранения больших объемов данных», в том числе национальных блокчейн-экосистем и платформ, является одной из пяти ключевых целей проекта «Информационная безопасность».

Вместе с тем в специализированной литературе вопросам *устойчивости* блокчейна в условиях беспрецедентного роста угроз безопасности уделено

---

1 http://government.ru/info/35568/.

2 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-175b.pdf.

не так много внимания. Поэтому появление настоящей книги — значимое событие в этой предметной области. Монография «Квантово-устойчивый блокчейн» написана приглашенным доцентом Университета Иннополис *Алексеем Сергеевичем Петренко* на основе его собственного весомого научно-практического опыта в данной области. В том числе в рамках выполнения научных грантов Университета Иннополис.

- Грант РФФИ 20-04-60080/22. Отчет НИР «Математический аппарат для создания квантово-устойчивых блокчейн-платформ на основе постквантовых криптопримитивов». Номер ЦИТиС АААА-А20-120081290051-5.
- Грант РФФИ № 18-47-160011/2021. Отчет НИР «Модель угроз безопасности эталонной блокчейн-платформы по аналитике зарубежных национальных квантовых программ». Номер ЦИТиС АААА-А18-118101290047-8.
- Грантовое соглашение с Академией наук Республики Татарстан (АН РТ). Отчет НИР «Методика оценивания квантовой устойчивости блокчейн-платформ на основе квантовых алгоритмов Шора и Гровера». № 18-47-160011/2021. Номер ЦИТиС АААА-А18-118101290047-8 и др.

Автор впервые рассмотрел и предложил варианты решений ряда актуальных задач квантового криптоанализа и синтеза постквантовых криптопримитивов для квантово-устойчивых блокчейнов. В том числе новый метод оценивания квантовой устойчивости блокчейн-платформ на основе результативного решения задач криптоанализа схем асимметричного шифрования (RSA, схема Эль-Гамаля) и цифровой подписи (DSA, ECDSA или RSA-PSS), а также метод параметрического выбора постквантовых криптопримитивов на основе целочисленных решеток (lattice-based cryptography); кодов, исправляющих ошибки (code-based cryptography); многочленов от многих переменных (multivariate cryptography); криптографических хеш-функций (hash-based cryptography); изогений суперсингулярных эллиптических кривых (supersingular isogeny-based cryprography) и др.

Практическая значимость исследований автора заключается в том, что были разработаны программные платформы (SDK) «Квант-К» и «Постквант-К» для квантового криптоанализа и параметрического выбора постквантовых криптопримитивов соответственно. При этом полученные результаты опробованы в гибридной вычислительной среде квантового компьютера IBM Q (16, 20 и 100 кубит), суперЭВМ IBM BladeCenter (2021), РВС на ПЛИС Virtex UltraScale (2021), ВС РФЯЦ-ВНИИЭФ (2021) и СКИФ П-0.5 (2018).

Монография выделяется как методом изложения, так и набором рассматриваемых вопросов. Благодаря удачному методическому подходу автору

удалось выбрать ту форму изложения материала, которая без ущерба для понимания существа дела позволила найти разумный баланс между постановкой задач по созданию требуемых квантово-устойчивых блокчейнов, с одной стороны, и описанием нетривиальных решений инженерных задач квантового криптоанализа и синтеза постквантовых криптопримитивов — с другой. Монография, безусловно, заинтересует специалистов, связанных с разработкой и реализацией национальных блокчейн-экосистем и платформ. В том числе разработчиков блокчейн-проектов InnoChain (Innopolis University), Waves Enterprise (Waves, Vostok), Hyperledger Fabric (Linux, IBM), Corda Enterprise, Bitfury Exonum, Blockchain Industrial Alliance, Exonum (Bitfury CIS), Nodes Plus (b41), «Мастерчейн 1.0» и «Мастерчейн 2.0», Microsoft Azure Blockchain, Enterprise Ethereum Alliance («Эфириум 1.0» и «Эфириум 2.0») и др. Она может служить прекрасным базовым пособием для студентов и аспирантов, обучающихся по направлениям подготовки «Информационная безопасность» (10.03.01, 10.05.01, 10.05.03 и 10.06.01) и «Кибербезопасность», ориентированным на практические вопросы обеспечения квантовой устойчивости блокчейн-экосистем и платформ. Также она будет полезна преподавателям для подготовки лекционных и практических занятий и научным сотрудникам, специализирующимся на квантовом криптоанализе и синтезе постквантовых криптопримитивов.

Существенно, что монография содержит результаты не только качественного, но и количественного изучения квантовой устойчивости национальных *блокчейн-экосистем* и *платформ*. Это позволяет впервые открыть предельный закон эффективности для защиты упомянутых компонентов критической информационной инфраструктуры цифровой экономики Российской Федерации.

Ректор Университета Иннополис,
доктор физико-математических наук, профессор
Александр Геннадьевич Тормасов

Введение

Следует констатировать, что большинство используемых криптопримитивов в современных блокчейн-экосистемах и платформах, в том числе хеш-функции (ГОСТ Р 34.11-2018, SHA-2, SHA-3, SHA256, Ethash, SCrypt, X11, Equihash, RIPEMD160 и др.), электронные подписи (ГОСТ 34.10-2018, ECDSA, EdDSA, Ring, One-Time, Borromean, Multi-signature и др.), асимметричные криптографические алгоритмы (RSA, Диффи — Хеллмана и др.) и соответствующие протоколы уже не являются квантово-устойчивыми. То есть устойчивыми относительно атак злоумышленников с использованием квантового компьютера. Сегодня известны эффективные квантовые алгоритмы, в частности алгоритм Шора для факторизации и дискретного логарифмирования, которые могут успешно применяться с целью взлома перечисленных криптопримитивов.

В 1994 году математик Питер Шор (Peter Shor), в то время работавший в компании AT&T Bell Laboratories, разработал алгоритм, который позволяет решить задачу факторизации за *полиномиальное время* (стало быть, полиномиальное количество гейтов) и на *полиномиальном количестве кубитов*, в то время как классические алгоритмы решают ее за *суперполиномиальное (субэкспоненциальное) время*. Это значит, что, как только квантовый компьютер с достаточным количеством кубитов (до 20 млн физических кубитов) будет создан, вся современная криптография окажется под угрозой компрометации. Собственно, она будет сразу скомпрометирована, поскольку любая информация, сокрытая с использованием этого подхода, может быть получена любым лицом, имеющим доступ к такому квантовому компьютеру.

Алгоритм Шора отличается от других известных квантовых алгоритмов прикладной значимостью и является более сложным с точки зрения математики и архитектуры. Для его реализации задействованы две вычислительные парадигмы: классическая часть готовит входные данные для алгоритма Шора, а также управляет циклами и возвратами в целях нахождения требуемого результата; квантовая часть исполняет линейную последовательность унитарных преобразований над специально подготовленными состояниями входных кубитов. Суть алгоритма факторизации Шора в сведении задачи факторизации к поиску периода функции. Если известен период функции,

то упомянутая факторизация осуществляется с помощью алгоритма Евклида за полиномиальное время. Квантовая часть алгоритма факторизации как раз занимается поиском периода функции, а классическая сначала особым образом готовит оную функцию, а затем проверяет найденный квантовой частью период на достаточность для решения задачи. Если период найден правильно, задача становится решенной. Если нет, квантовая часть алгоритма прогоняется еще раз. При этом проверка правильности решения для задачи факторизации достаточна проста (умножение двух чисел и сравнение с третьим), поэтому данную часть алгоритма обычно не учитывают при подсчете сложности.

Среди всех квантовых алгоритмов (их более 40) алгоритм Шора наиболее известен. Можно даже утверждать, что из-за упомянутого алгоритма новая вычислительная модель, основанная на законах квантовой механики, получила столь широкое развитие. Дело в том, что многочисленные современные алгоритмы и системы криптографии основаны именно на гипотезе алгоритмической сложности задачи факторизации числа. При этом ученые, работающие в области криптографии, полагают, что Агентство национальной безопасности (АНБ) (National Security Agency, NSA)[1] и другие разведывательные агентства мира накопили огромное количество зашифрованных данных из Интернета, которые сегодня не поддаются расшифровке современными средствами. Эти данные сохраняются и пополняются, и резонно предположить, что в АНБ смогут их расшифровать, когда получат в свое распоряжение соответствующий квантовый компьютер. При таком сценарии риску (квантовой угрозе) подвергнется не только личная переписка граждан за минувшие десятилетия; под угрозой окажется текущая корреспонденция, которую мы до этого считали надежно защищенной. Еще более категоричен в высказываниях известный профессор информатики Монреальского университета Жиль Брассар (Gilles Brassard)[2]: «Было бы абсолютным сумасшествием полагать, что где-то там нет кого-нибудь, а может быть, и множества тех, кто записывает весь сетевой трафик и просто ждет, когда появится техника, способная взломать все старые шифры. Поэтому, хотя достаточного для этих целей квантового компьютера еще не существует, и даже если его не разработают в течение следующих 5–10 лет, как только он появится, вся ваша корреспонденция, которую вы отправили с первого дня, используя эти классические методы шифрования, окажется скомпрометирована, то есть доступна тому, кому она не предназначалась»[3].

---

1 https://www.nsa.gov/.

2 http://www.iro.umontreal.ca/~brassard/web/en/.

3 https://spkurdyumov.ru/uploads/2016/04/kvantovyj-vzlom.pdf.

Таким образом, *квантовый алгоритм Шора* позволяет решать *задачи факторизации и дискретного логарифмирования* и может быть использован для криптоанализа большинства практически применимых криптосистем (RSA, DSA, ECDSA, ГОСТ Р 34.10 и др.). Ожидается, что в ближайшие пять лет квантовые компьютеры превзойдут классические компьютеры архитектуры фон Неймана в решении задачи криптоанализа. В том числе криптоанализа криптосистемы RSA (одной и самых распространенных систем асимметричного шифрования, названной в честь ее авторов — Рона Ривеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman)). К 2025 году квантовые компьютеры смогут эффективно взламывать RSA с длиной ключа 2048 бит (минимум, рекомендуемый международными криптографическими стандартами).

На данный момент с помощью алгоритма Шора на квантовых компьютерах успешно факторизованы числа[1] $15 = 3 \times 5$ и $21 = 3 \times 7$. Для решения задачи факторизации также был адаптирован 4-кубитовый адиабатический квантовый компьютер, факторизовавший число $143 = 11 \times 13$[2] и $56\,153 = 233 \times 241$[3]. Любопытно, что факторизацию большего числа исследователи сперва не заметили. Только через два года было показано, что в ходе эксперимента факторизован целый класс чисел. Далее методом квантового отжига на компьютере D-Wave 2X факторизовали число 200 099[4]. Следующим интересным результатом стала факторизация числа 291 311 с помощью квантового компьютера[5], основанного на принципах ядерного магнитного резонанса. А рекордным факторизованным числом на текущий момент времени является $1\,099\,551\,473\,989 = 1\,048\,589 \times 1\,048\,601$[6].

Заметим, что практические результаты применения *алгоритмов Гровера и Саймона* к анализу даже модельных криптосистем еще слабо изучены, поскольку реализация таких систем требует большого количества квантовых вентилей, недоступного на современном уровне развития *Q-технологии*. Однако выборочные примеры имплементации применения *метода Гровера* на модельных задачах и его реализации, в том числе на облачном квантовом

---

1 https://research-information.bris.ac.uk/en/publications/experimental-realization-of-shors-quantum-factoring-algorithm-usi.

2 https://arxiv.org/pdf/1111.3726v1.pdf.

3 https://arxiv.org/abs/1411.6758.

4 https://arxiv.org/abs/1604.05796.

5 https://www.researchgate.net/scientific-contributions/Richard-Tanburn-2079794789.

6 https://4627su41pzrvhaad34118k3y-wpengine.netdna-ssl.com/wp-content/uploads/2020/12/Analyzing-the-Performance-of-Variational-Quantum-Factoring-on-a-Superconducting-Quantum-Processor.pdf.

компьютере IBM, представлены в научных работах[1]. Реализация *алгоритма Саймона* описана в техническом пособии по квантовым алгоритмам[2]. Кроме того, интересно отметить, что наиболее впечатляющие результаты по факторизации были получены с помощью квантовых компьютеров, реализующих модели, которые ранее считались не вполне подходящими для решения задач криптоанализа, такие, например, как модель квантового отжига.

Таким образом, развитие алгоритмической базы может сократить сроки появления эффективных квантовых вычислителей относительно нашей оценки. Более того, перспективы появления «практического» квантового компьютера, способного выполнять поставленные задачи криптоанализа, становятся еще ближе, если учитывать результаты компании IBM по разработке квантовых процессоров. Так, в ноябре 2021 года IBM представила 127-кубитовый *процессор Eagle*, а к 2023 году прогнозирует преодоление 1000-кубитового предела[3]. В свое время исследователи компании *Google* показали, что для эффективного криптоанализа *RSA* достаточно порядка 20 млн физических (доступных на текущем уровне технологии) кубитов[4]. С учетом возможности эффективного распараллеливания вычислений между несколькими устройствами с существенно меньшим числом кубитов, продемонстрированной в указанной работе, достижения *IBM* убедительно свидетельствуют о реалистичности реализации квантовой угрозы. Поэтому в ближайшее время в технологически развитых странах мира, главным образом в США, Китае, России и государствах Евросоюза, запланирован переход к постквантовой криптографии[5].

Монография ориентирована на основные группы читателей.

1. **Руководителей служб автоматизации (CIO)** и **информационной безопасности (CISO)**, которые хотят получить ответы на следующие вопросы.

- Является ли корпоративная блокчейн-платформа киберустойчивой к атакам злоумышленников с применением квантового компьютера?
- Какие методы и средства рекомендуется использовать для оценивания квантовой устойчивости блокчейна?
- Являются ли криптопримитивы корпоративной блокчейн-платформы стойкими к квантовым криптоатакам?

---

1 https://cis.temple.edu/~boji/papers/REU2018.pdf и https://arxiv.org/pdf/1804.03719.pdf.

2 https://qiskit.org/textbook/ch-algorithms/simon.html.

3 https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor.

4 https://arxiv.org/pdf/1905.09749.pdf.

5 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-175b.pdf.

- Каковы последствия для компании в случае взлома криптопримитивов корпоративной блокчейн-платформы?
- Какие отечественные и международные криптографические стандарты применимы для создания корпоративной квантово-устойчивой блокчейн-платформы?
- Какие постквантовые криптопримитивы рекомендуется использовать для обеспечения требуемой киберустойчивости блокчейна?

Ответы на эти вопросы даны в главах 1, 2, 3, 4.

2. **Разработчиков, проектировщиков и внедренцев технологии блокчейн**, которые желают получить детальное представление о механизмах обеспечения киберустойчивости корпоративных блокчейн-экосистем или платформ, достаточное для того, чтобы грамотно разбираться в этих вопросах, а возможно, и руководить работами, связанными с разработкой, проектированием и внедрением технологии блокчейн. Данной категории читателей адресованы главы 2, 3, 4.

3. **Внутренних и внешних аудиторов, консультантов и тренеров по вопросам безопасности и устойчивости блокчейн.**

Данная категория читателей может получить ответы на интересующие вопросы в главах 1, 2, 3, 4.

Монографию также могут использовать в качестве учебного пособия студенты и аспиранты соответствующих специальностей по направлениям «Информационная безопасность» и «Кибербезопасность», тем более что материалы ее глав основаны в том числе на опыте преподавания автора в Московском физико-техническом институте (МФТИ) и Университете Иннополис.

Монография содержит четыре главы, которые посвящены:

- проблемным вопросам обеспечения киберустойчивости современных блокчейн-экосистем или платформ цифровой экономики Российской Федерации и возможным путям их разрешения. В том числе авторским моделям и методам обеспечения киберустойчивости блокчейна;
- актуальным вопросам разработки моделей угроз безопасности и моделей нарушителей для национальных блокчейн-проектов. В том числе противодействию классическим и квантовым угрозам безопасности для обеспечения требуемой киберустойчивости блокчейн-экосистем и платформ цифровой экономики Российской Федерации;

- перспективным методам оценивания квантовой устойчивости блокчейна, позволяющим проводить не только качественные, но и количественные измерения киберустойчивости блокчейн-экосистем или платформ цифровой экономики Российской Федерации. Разработке и программно-технической реализации авторских квантовых алгоритмов криптоанализа на квантовых схемах;
- примерам разработки квантово-устойчивых блокчейнов, созданных в ходе выполнения задач федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации». В том числе перспективным методам синтеза и параметрического выбора постквантовых криптопримитивов блокчейна.

Автор заранее выражает признательность всем читателям, которые готовы поделиться своим мнением о данной книге. Отправлять письма можно лично автору по адресу A.Petrenko1999@rambler.ru.

Алексей Петренко.
Москва — Санкт-Петербург — Иннополис.
Июль 2022 года