

V (ПЯТАЯ)

**МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ
КОНФЕРЕНЦИЯ**

Май 2026 г.

ИНДЕКСАЦИЯ



OpenAIRE | EXPLORE

zenodo

НАПРАВЛЕНИЯ КОНФЕРЕНЦИИ



 **НАУЧНЫЕ
ТЕХНОЛОГИИ
ПЕДАГОГИКА
ПСИХОЛОГИЯ
ФИЛОСОФИЯ
ИСТОРИЯ**



 **ИНФОРМАТИКА
ТЕХНИЧЕСКИЕ
НАУКИ
МАТЕМАТИЧЕСКИЙ
АНАЛИЗ**



 **ЭКОНОМИКА
ФИНАНСЫ**

Введение

В сборнике материалов конференции, посвященных роли науки, образования и производства в эпоху глобализации, актуальным проблемам взаимодействия этих процессов, отзывам об их решениях, были представлены зрелые специалисты отрасли.

Кроме того, представлены исследования на научно-практическую тему, проводимые в области экономики, точных наук, естественных и социально-гуманитарных наук в период глобализации, представлена информация в научно-практической сфере, которая включает в себя новейшие инновационные технологии в сферах производства.

Можно утверждать, что этот сборник является одним из специфических перекрестков современных мыслей и инновационных идей в мире науки. В этой научно-практической конференции приняли активное участие профессоры и научные сотрудники, занимающиеся научными исследованиями в Узбекистане и зарубежных странах. Значительный вклад в повышение позиций научно-практической конференции внесли профессора и преподаватели отечественных и зарубежных высших учебных заведений.

Профессора и преподаватели зарубежных высших учебных заведений, активно участвовавшие в работе конференции, внесли достойный вклад в высокий уровень взаимодействия с учеными нашей страны. Процессы международного сотрудничества с зарубежными странами и обмена с ними в области науки в эпоху глобализации оказывают положительное влияние на развитие высшего образования, сфер науки и производства. Материалы этой конференции особенны тем, что включают в себя широкий спектр исследований, от теоретических разработок до практических решений, демонстрирующих разнообразие подходов и направлений в этой области.

В заключение следует отметить, что данная научно-практическая конференция станет очень полезным собранием для всех, кто интересуется современными исследованиями в области дальнейшего развития высшего образования, науки, воспитательной работы и производства в эпоху глобализации. Авторы несут ответственность за содержание и качество статей и тезисов, включенных в сборник.



КВАНТОВЫЕ КОМПЬЮТЕРЫ И НОВАЯ ЭРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: НАУЧНЫЕ ОСНОВЫ И ПРАКТИЧЕСКОЕ ЗНАЧЕНИЕ

Алдай Мактагул ¹

Мамараимов Абзор Камолиддин угли ²

¹ заведующая кафедрой фундаментальной математики, механико-математический факультет, Евразийский национальный университет имени Л. Н. Гумилёва, г. Астана, Республика Казахстан

² старший преподаватель кафедры информационных систем и технологий, Джизакский филиал Национального университета Узбекистана имени Мирзо Улугбека, г. Джизак, Республика Узбекистан

Аннотация. В статье рассматриваются фундаментальные принципы квантовых вычислений и их принципиальное значение для современной информационной безопасности. На основе анализа ключевых квантовых алгоритмов — алгоритма Шора и алгоритма Гровера — показано, что широко используемые криптографические системы RSA, ECC и AES становятся уязвимыми при достижении достаточного масштаба квантовых вычислительных ресурсов. Представлен обзор пост-квантовой криптографии (PQC), включая финализированные стандарты NIST: CRYSTALS-Kyber, CRYSTALS-Dilithium и FALCON. Проведён сравнительный анализ классических и квантовых угроз по параметрам временной сложности, длины ключа и вычислительных ресурсов. Рассмотрена квантовое распределение ключей (QKD) как практически реализуемый механизм информационно-теоретической защиты. Материал адресован специалистам в области кибербезопасности, математики и разработчикам информационных систем, которым предстоит адаптировать существующую инфраструктуру к постквантовой эпохе.

Ключевые слова: квантовые вычисления, квантовая криптография, пост-квантовая криптография, алгоритм Шора, алгоритм Гровера, RSA, NIST PQC, информационная безопасность, QKD, CRYSTALS-Kyber.

ВВЕДЕНИЕ

Развитие квантовых вычислений является одним из наиболее значимых технологических событий XXI века, способным коренным образом изменить ландшафт информационной безопасности. Концептуальный фундамент квантовых вычислений был заложен Р. Фейнманом в 1982 году [1], а практическое воплощение идея получила в работах П. Шора (1994) [2] и Л. Гровера (1996) [3], показавших, что квантовые компьютеры способны решать отдельные классы задач экспоненциально быстрее по сравнению с классическими архитектурами.

Мировой объём данных, требующих криптографической защиты, к 2025 году превысил 120 зеттабайт [4]. При этом подавляющее большинство систем защиты информации по-прежнему опирается на вычислительную сложность задач факторизации целых чисел и дискретного логарифмирования, которые уязвимы к атакам на основе алгоритма Шора. По оценкам экспертов NIST, технически значимый квантовый компьютер, способный сломать 2048-битный ключ RSA, может стать реальностью уже в 2030-е годы [5].

Ключевым вызовом текущего момента является так называемая угроза типа «собери сейчас — расшифруй потом» (harvest now, decrypt later): противники уже сегодня могут перехватывать и накапливать зашифрованные данные в расчёте на последующую расшифровку с помощью квантовых компьютеров [6]. Это делает проблему перехода к постквантовым стандартам критически срочной, не зависящей от фактических сроков появления масштабируемых квантовых устройств.

Настоящая работа преследует две взаимосвязанные цели: (1) систематизировать научные основы квантовых вычислений применительно к задачам криптоанализа; (2) провести сравнительный анализ существующих и перспективных механизмов защиты информации с учётом квантовых угроз.

МАТЕРИАЛЫ И МЕТОДЫ

Исследование выполнено методами теоретического анализа и систематического обзора литературы. В качестве источниковой базы использованы: (1) первичные публикации в рецензируемых журналах IEEE Transactions on Information Theory, ACM Computing Surveys, Physical Review Letters за период 1994–2024 гг.; (2) официальные стандарты и технические отчёты NIST (SP 800-208, FIPS 203–205); (3) материалы Европейского агентства по сетевой и информационной безопасности (ENISA).

Сравнительный анализ криптографических схем проводился по следующим параметрам: временная сложность атаки на классическом и квантовом компьютере (в нотации «О большое»), минимальная длина ключа, обеспечивающая 128-битный уровень стойкости в постквантовой модели безопасности, а также практическая реализуемость в рамках существующей инфраструктуры открытых ключей (PKI). Для описания квантовых алгоритмов применялся формализм линейной алгебры над полем комплексных чисел и теория квантовых схем.

Ключевые понятия. Кубит (квантовый бит) — базовый элемент квантовой информации, описываемый состоянием $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in \mathbb{C}$ и $|\alpha|^2 + |\beta|^2 = 1$. Суперпозиция позволяет кубиту одновременно представлять оба базисных состояния, а запутанность (entanglement) обеспечивает нелокальные корреляции между кубитами, что является основой квантового параллелизма. Квантовое преимущество достигается за счёт интерференции квантовых амплитуд, позволяющей усиливать вклад правильного ответа и подавлять вклад неправильных [7].

РЕЗУЛЬТАТЫ

1. Алгоритм Шора и угроза асимметричной криптографии

Алгоритм Шора (1994) решает задачу факторизации целого числа N за время $O((\log N)^3)$, тогда как наилучший классический алгоритм — метод решета числового поля — требует $O(\exp((\log N)^{1/3} \cdot (\log \log N)^{2/3}))$ операций [2]. Для 2048-битного числа N это означает переход от астрономического числа операций ($\sim 10^{90}$) к вычислительно тривиальной задаче ($\sim 10^{10}$).

Алгоритм работает в два этапа: (1) квантовый этап — нахождение периода r функции $f(x) = a^x \bmod N$ с помощью квантового преобразования Фурье за $O((\log N)^2 \cdot \log \log N \cdot \log \log \log N)$; (2) классический этап — вычисление $\text{НОД}(a^{(r/2)} \pm 1, N)$ для извлечения нетривиального делителя. Уязвимость RSA и криптографии на эллиптических кривых (ECC) перед данным алгоритмом является прямым следствием вычислительной сложности соответствующих математических задач — факторизации и дискретного логарифма.

2. Алгоритм Гровера и угроза симметричной криптографии

Алгоритм Гровера (1996) решает задачу поиска в неупорядоченной базе данных размером N за $O(\sqrt{N})$ операций против $O(N)$ для классического поиска [3]. Применительно к симметричным шифрам это означает, что эффективная длина ключа уменьшается вдвое: 128-битный ключ AES обеспечивает лишь 64-битный уровень стойкости в квантовой модели. Практическое следствие — необходимость удвоения длины ключей симметричного шифрования: AES-128 должен быть заменён AES-256 для сохранения приемлемого уровня безопасности [8].

3. Сравнительный анализ криптографических схем

В таблице 1 представлено сравнение классических и постквантовых криптографических схем по ключевым параметрам безопасности.

Таблица 1.

Сравнение классических и постквантовых криптографических схем

Схема	Тип	Классич. стойкость	Квантовая стойкость	Статус
RSA-2048	Асимм.	$O(\exp(N^{1/3}))$	$O((\log N)^3)$ — уязвима	Устаревает
ECC-256	Асимм.	128 бит	Уязвима (алг. Шора)	Устаревает
AES-128	Симм.	128 бит	64 бит (алг. Гровера)	Использ. AES-256
AES-256	Симм.	256 бит	128 бит	Рекомендуется
CRYSTALS-Kyber	КЕМ/PQC	128+ бит	128 бит	Стандарт NIST 2024

CRYSTALS-Dilithium	ЦП/PQC	128+ бит	128 бит	Стандарт NIST 2024
FALCON	ЦП/PQC	128+ бит	128 бит	Стандарт NIST 2024
SPHINCS+	ЦП/PQC	128+ бит	128 бит	Альт. NIST 2024

4. Пост-квантовая криптография: стандарты NIST

В августе 2024 года NIST опубликовал три финальных постквантовых стандарта [9]: FIPS 203 (CRYSTALS-Kyber — механизм инкапсуляции ключей на основе задачи Learning With Errors на решётках), FIPS 204 (CRYSTALS-Dilithium — схема цифровой подписи) и FIPS 205 (FALCON — альтернативная схема цифровой подписи на основе решёток NTRU). Дополнительно зарегистрирован SPHINCS+ (хэш-основанные подписи) как резервный алгоритм без зависимости от решётчатых задач.

Криптосистемы на основе задачи Learning With Errors (LWE) строятся следующим образом. Пусть q — простое число, $s \in \mathbb{Z}_n_q$ — секретный вектор. Публичный ключ формируется как пара (A, b) , где $A \in \mathbb{Z}^{(m \times n)}_q$ — случайная матрица, $b = As + e \pmod{q}$, e — малый вектор ошибок. Задача LWE состоит в восстановлении s по (A, b) , что считается вычислительно трудным как для классических, так и для квантовых алгоритмов — лучший известный квантовый алгоритм имеет сложность $2^{\Omega(n)}$ [10].

5. Квантовое распределение ключей (QKD)

QKD — единственный на сегодняшний день механизм, обеспечивающий информационно-теоретическую (безусловную) стойкость, не зависящую от вычислительных возможностей противника. Протокол BB84 (Bennett & Brassard, 1984) использует поляризационные состояния фотонов для передачи ключевых битов: любое подслушивание неизбежно нарушает квантовые состояния вследствие теоремы о запрете клонирования (no-cloning theorem) и обнаруживается по аномальному возрастанию QBER (Quantum Bit Error Rate, норма $< 11\%$) [11].

Практические реализации QKD (Toshiba, ID Quantique, QuantumCTek) демонстрируют дальность до 500–600 км по оптоволокну в специализированных лабораторных условиях, тогда как коммерческие системы стабильно работают на расстоянии до 200 км [12]. Спутниковый канал QKD (эксперимент Micius, 2017) достиг дальности 7600 км [13]. Ключевым ограничением остаётся невозможность использования классических ретрансляторов — квантовые повторители находятся на стадии лабораторных разработок.

6. Временные параметры миграции на постквантовые стандарты

Таблица 2 иллюстрирует прогнозируемые временные рамки квантовой угрозы и рекомендуемые стратегии миграции.

Таблица 2.

Прогнозируемые временные рамки и стратегии перехода к
постквантовой безопасности

Горизонт	Квантовая угроза	Рекомендуемые меры	Уязвимые системы
2025–2027	Алгоритм Шора на 1000–2000 физ. кубитах	Инвентаризация криптоактивов; тестирование PQC	Долгосрочные архивы, государственные системы
2027–2030	Алгоритм Шора на 4000+ кубитах (оценка NIST)	Гибридные схемы: классика + PQC; пилотный QKD	Финансовые сети, PKI, TLS
2030+	Полноценные NISQ/FTQ устройства	Полный переход на CRYSTALS-Kyber/Dilithium/FALCON	Вся инфраструктура открытых ключей

ОБСУЖДЕНИЕ

Полученные результаты систематизации позволяют сделать ряд принципиальных наблюдений. Во-первых, угроза квантового взлома асимметричных криптосистем имеет не вероятностный, а детерминированный характер: алгоритм Шора теоретически совершенен, и вопрос состоит исключительно в сроках появления достаточно масштабируемого квантового оборудования. Это фундаментально отличает квантовую угрозу от классических криптоаналитических атак, реализуемость которых определяется вычислительными ресурсами [14].

Во-вторых, принятие стандартов NIST PQC в 2024 году ознаменовало переход от исследовательской фазы к фазе внедрения. Однако масштаб предстоящей криптографической миграции сопоставим с переходом от DES к AES в 1990-е — 2000-е годы, с той принципиальной разницей, что нынешняя инфраструктура несравнимо обширнее и гетерогеннее [15]. Особую сложность представляют встроенные системы (IoT), обновление программного обеспечения которых технически затруднено или невозможно.

В-третьих, QKD и PQC следует рассматривать не как конкурирующие, а как взаимодополняющие технологии. PQC обеспечивает квантовоустойчивую защиту на основе вычислительных допущений (хотя и более сильных, чем для RSA), тогда как QKD предоставляет информационно-теоретические гарантии ценой значительных инфраструктурных издержек. Гибридные архитектуры, сочетающие оба подхода, признаются наиболее перспективными для критических применений [5].

Необходимо подчеркнуть ограничения настоящей работы. Сроки появления масштабируемых квантовых компьютеров остаются предметом дискуссий; ряд экспертов полагает, что барьер в виде квантовой коррекции ошибок может существенно отодвинуть реализацию алгоритма Шора в промышленном масштабе [16]. Кроме того, безопасность PQC-схем на

решётках, несмотря на обширную теоретическую базу, не имеет доказательства сводимости к задачам с известной вычислительной сложностью в той же мере, что классические схемы — к факторизации.

Для стран Центральной Азии, включая Казахстан и Узбекистан, рассматриваемая проблематика приобретает особое измерение в контексте формирования национальных стандартов информационной безопасности и цифровизации государственного управления. Своевременное включение PQC-требований в нормативную документацию регуляторов позволит избежать повторного дорогостоящего обновления инфраструктуры [17].

ЗАКЛЮЧЕНИЕ

Квантовые вычисления формируют принципиально новую парадигму угроз информационной безопасности, требующую системного ответа на уровне стандартов, инфраструктуры и регулирования. Ключевые выводы настоящей работы состоят в следующем.

1. Алгоритм Шора теоретически обеспечивает полиномиальное (а не просто ускоренное) решение задач факторизации и дискретного логарифма, что делает RSA и ECC принципиально нежизнеспособными в постквантовом мире, тогда как алгоритм Гровера требует лишь удвоения длины ключа для симметричных шифров.

2. Принятые NIST стандарты CRYSTALS-Kyber, CRYSTALS-Dilithium и FALCON обеспечивают документально подтверждённый 128-битный уровень постквантовой стойкости и готовы к промышленному внедрению.

3. QKD предоставляет безусловные гарантии секретности ключевого обмена, однако ограничена дальностью и инфраструктурными требованиями; гибридные архитектуры QKD+PQC наиболее обоснованы для критических применений.

4. Угроза типа «собери сейчас — расшифруй потом» требует немедленного начала криптографической миграции, не дожидаясь физического появления масштабируемых квантовых компьютеров.

Перспективы дальнейших исследований связаны с разработкой методологии оценки рисков при гибридном переходе, а также с анализом практических аспектов внедрения NIST PQC в государственных информационных системах Республики Казахстан и Республики Узбекистан.

СПИСОК ЛИТЕРАТУРЫ

1. Feynman R. P. Simulating physics with computers / R. P. Feynman // International Journal of Theoretical Physics. — 1982. — Vol. 21. — № 6/7. — P. 467–488.
2. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor // SIAM Journal on Computing. — 1997. — Vol. 26. — № 5. — P. 1484–1509.

3. Grover L. K. A fast quantum mechanical algorithm for database search / L. K. Grover // Proceedings of the 28th Annual ACM Symposium on Theory of Computing. — 1996. — P. 212–219.
4. Seagate / IDC. DataSphere Forecast 2024 // Rethink Data Report. — 2024. — URL: <https://www.seagate.com> (дата обращения: 12.04.2025).
5. NIST. Post-Quantum Cryptography: The Story So Far // NIST Internal Report 8413. — Gaithersburg: NIST, 2023. — 32 p.
6. Mosca M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? / M. Mosca // IEEE Security & Privacy. — 2018. — Vol. 16. — № 5. — P. 38–41.
7. Nielsen M. A. Quantum Computation and Quantum Information / M. A. Nielsen, I. L. Chuang. — Cambridge: Cambridge University Press, 2010. — 702 p.
8. Bernstein D. J. Post-Quantum Cryptography / D. J. Bernstein, T. Lange. — Berlin: Springer, 2009. — 245 p.
9. NIST. Federal Information Processing Standards 203, 204, 205 (CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON). — Gaithersburg: NIST, 2024.
10. Regev O. On lattices, learning with errors, random linear codes, and cryptography / O. Regev // Journal of the ACM. — 2009. — Vol. 56. — № 6. — Article 34. — 40 p.
11. Bennett C. H. Quantum cryptography: Public key distribution and coin tossing / C. H. Bennett, G. Brassard // Theoretical Computer Science. — 2014. — Vol. 560. — P. 7–11.
12. Pirandola S. Advances in quantum cryptography / S. Pirandola [et al.] // Advances in Optics and Photonics. — 2020. — Vol. 12. — № 4. — P. 1012–1236.
13. Liao S.-K. Satellite-Relayed Intercontinental Quantum Network / S.-K. Liao [et al.] // Physical Review Letters. — 2018. — Vol. 120. — № 3. — Article 030501.
14. Preskill J. Quantum Computing in the NISQ Era and Beyond / J. Preskill // Quantum. — 2018. — Vol. 2. — P. 79.
15. Chen L. Report on Post-Quantum Cryptography / L. Chen [et al.] // NIST Internal Report 8105. — Gaithersburg: NIST, 2016. — 15 p.
16. Bravyi S. The future of quantum computing with superconducting qubits / S. Bravyi [et al.] // Journal of Applied Physics. — 2022. — Vol. 132. — № 16. — Article 160902.
17. ITU-T Recommendation X.1710. Security framework for quantum key distribution networks. — Geneva: ITU, 2021. — 56 p.