УДК 003.26

О НЕКОТОРЫХ АКТУАЛЬНЫХ НАУЧНО-ТЕХНИЧЕСКИХ НАПРАВЛЕНИЯХ В ОБЛАСТИ СТАНДАРТИЗАЦИИ КВАНТОВОЙ И ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

А.М. Коренева
ООО «Код Безопасности», Москва, Россия
Финансовый университет при Правительстве РФ, Москва, Россия

Аннотация. В данной обзорной статье предлагается рассмотреть области квантовой и постквантовой криптографии, а также обозначить актуальные направления в области стандартизации. С использованием общедоступной информации на примере деятельности Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) предлагается рассмотреть два направления в области стандартизации:
– постквантовые криптографические механизмы;
– квантовые криптографические системы выработки и распределения ключей.
Дополнительно, в работе отмечается еще одно направление, которое, по мнению автора, может представлять интерес для настоящих и будущих исследований.
Ключевые слова: квантовые криптографические системы; квантовый компьютер; криптографическая защита информации; постквантовая криптография; стандартизация.

CURRENT DIRECTIONS IN QUANTUM AND POST-QUANTUM CRYPTOGRAPHY STANDARDIZATION

A.M. Koreneva
Security Code LLC, Moscow, Russia
Financial university under the Government of the Russian Federation, Moscow, Russia

Abstract. In the present paper, we consider quantum and post-quantum cryptography. Further, we highlight current directions in the field of quantum and post-quantum cryptographic mechanisms standardization. Using publicly available information about Technical Committee for Standardization "Cryptography and security mechanisms" (TC 26), we observe the following standardization directions:
– post-quantum cryptographic mechanisms;
– quantum key exchange schemes.
Moreover, we highlight another direction for future comprehensive research.
Keywords: cryptography; post-quantum cryptography; quantum key exchange schemes; quantum computer; standardization.

Введение

Идея квантовых вычислений насчитывает более 40 лет. За это время проделана существенная работа по созданию специальных алгоритмов и построению квантового компьютера. Становление и развитие этой области заслуживает отдельного анализа и систематизации, что выходит за рамки данной статьи. В России широко известен научно-технологический центр, занимающийся исследованиями и разработкой коммерческих продуктов на основе квантовых технологий.

В настоящее время ряд государств, включая РФ, ведут работы по созданию полноценного квантового вычислителя, который, как предполагается, превзойдет классический компьютер в решении задач криптографического анализа. В связи с этим актуальна разработка квантовоустойчивых (или постквантовых) криптографических механизмов и их стандартизация.

В работе рассматривается два направления, интересных для стандартизации:

–постквантовые криптографические механизмы;

–квантовые криптографические системы выработки и распределения ключей.

Статья состоит из четырех разделов. В разделе 1 в общих чертах рассматриваются постквантовые криптографические механизмы. В разделе 2 приведены актуальные направления в области стандартизации. Раздел 3 посвящен стандартизации в области квантовых криптографических систем выработки и распределения ключей. В разделе 4 отмечено направление, которое, по мнению автора, может представлять интерес для настоящих и будущих исследований.

Квантовоустойчивые (или постквантовые) криптографические механизмы

Проблематика, задачи и перспективы постквантовой криптографии активно обсуждались в 2024 году на Пленарном заседании конференции РусКрипто [1, 2].

Как и в случае «классических» криптографических систем с открытым ключом, постквантовые криптографические механизмы основаны на некоторых вычислительно трудных математических задачах. Важно, чтобы эти задачи были вычислительно трудными и для квантового компьютера. К таким задачам сейчас относят:

–задача нахождения кратчайшего вектора решетки (shortest vector problem, SVP);

–задача нахождения кратчайшего целочисленного решения (short integer solution, SIS);

–обучение с ошибками (learning with errors, LWE);

–обучение с округлением (learning with rounding, LWR);

–декодирование произвольного линейного кода;

–вычисление изогении с неизвестным ядром;

–нахождение решений систем полиномиальных уравнений от многих переменных.

Известны четыре изучаемых подхода к построению квантовоустойчивых криптографических механизмов [3]. В основе каждого постквантового механизма лежит известная математическая либо криптографическая конструкция, для которой может быть сформулирована одна из задач, перечисленных выше. Такими конструкциями являются:

–функции хэширования;

–коды, исправляющие ошибки;

–алгебраические решетки;

–изогении эллиптических кривых.

Первые две стали известны на заре криптографии с открытым ключом (1970-е годы), но тогда они не получили развития из соображений вычислительной неэффективности в сравнении с другими подходами. Две других конструкции предложены менее 30 лет назад.

Далее кратко рассмотрим упомянутые конструкции, после чего отметим некоторые схемы, разработанные российскими исследователями, которые представляют интерес для стандартизации в области постквантовых криптографических механизмов.

Функции хэширования. Алгоритмы, использующие функции хэширования, реализуют однотипные конструкции, в основе которых лежат сжимающее хэширующее дерево и одноразовая схема подписи Винтерница. К особенностям таких схем можно отнести сводимость свойств безопасности к соответствующим свойствам применяемой функции хэширования, а также малую величину открытого ключа вкупе с большим размером подписи в сравнении с классическими алгоритмами. На основе функций хэширования реализуются схемы электронной подписи.

Коды. Алгебраическим линейным кодом, исправляющим ошибки, в общем случае называется линейное векторное пространство размерности k, где k – натуральное число, над некоторым полем F. Кодирование информационного слова при этом формализуется в виде нахождения некоторого вектора, который при декодировании и отсутствии ошибок в канале, дает исходное информационное слово. Известно, что задача декодирования произвольного линейного кода является NP-полной, но для ряда кодов при известном строении можно построить эффективные (полиномиальные) алгоритмы декодирования. Первой схемой, основанной на кодах, является криптосистема МакЭлиса, которая первоначально была построена на основе кодов Рида-Маллера. Впоследствии были найдены слабости этой конструкции, а также предложена модификация на основе кодов Гоппы, которая на текущий момент остается стойкой и считается оптимальной по своим эксплуатационным характеристикам.

Решетки. Целочисленной решеткой над некоторым полем называется множество линейных комбинаций векторов над этим полем с целочисленными коэффициентами. Для данной конструкции известно, что задача построения приведенного, ортонормированного базиса, содержащего кратчайший вектор, также является NP-полной. Это означает, что вычисление в некотором «хорошем» базисе можно производить относительно легко, поэтому этот базис является закрытым ключом, а «плохой» базис, в котором вычисления производятся труднее, – открытым. Это – общая идея использования «решетчатых» криптосистем, основанных на задаче поиска кратчайшего вектора. К исходному вектору пользователя можно также добавлять случайный «шум», в таком случае мы получим криптосистему на решетках, основанную на задаче обучения с ошибками или обучения с округлением.

Изогении эллиптических кривых. Изогении эллиптических кривых представляют собой рациональные отображения между эллиптическими кривыми. При этом кривые разбиваются на классы изогенности. Изогенная кривая эффективно вычислима при известном ядре изогении. Однако обратное утверждение при определенных условиях не верно. Перспектива появления квантового компьютера достаточной производительности для реализации алгоритма Шора делает нестойкими традиционные схемы выработки общего ключа типа Диффи-Хеллмана, основанные на задаче дискретного логарифмирования. По аналогии с хорошо известной схемой Диффи-Хеллмана, изогении позволяют реализовать эффективный протокол выработки общего секрета.

Следует отметить, что для одной из двух наиболее известных подобных схем оценка стойкости понижена до полиномиальной. Несмотря на применение при этом свойств анализируемого протокола, подход дискредитирован в целом и на текущий момент криптографические конструкции на основе изогений в процессах стандартизации не рассматриваются.

Стандартизация в области постквантовых криптографических механизмов

Считается, что первым стандартизованным постквантовым криптографическим механизмом стала схема подписи XMSS (eXtended Merkle Signature Scheme, см. RFC 8391, 2015–2018). Практически в то же время институт NIST начал конкурс NIST PQ (2016–2024). В результате в США были приняты стандарты:

–FIPS 203: инкапсуляция ключа с применением арифметики решеток;

–FIPS 204: схема подписи с применением арифметики решеток;

–FIPS 205: схема подписи с применением конструкции хэширующего дерева.

В России вопросами стандартизации в области постквантовых криптографических механизмов занимается Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26). Согласно открытой информации о структуре ТК 26 рабочая группа «Постквантовые криптографические механизмы» входит в подкомитет 2 «Криптографические алгоритмы и протоколы для применения в поставляемых для федеральных государственных нужд шифровальных (криптографических) средствах защиты информации, содержащей сведения, относимые к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа».

Рабочая группа собрана в 2019 году для создания стандартов в области постквантовой криптографии – схем постквантовой электронной подписи и схем защищенного распределения ключей.

В настоящее время разрабатываются и исследуются механизмы:

– «Шиповник» – схема постквантовой электронной подписи, основанная на криптосистеме МакЭлиса (данная криптосистема построена на основе кодов Гоппы) [4];

– «Кодиеум» – постквантовая схема инкапсуляции ключа, построенная на основе крипосистемы Нидеррайтера, тоже использует алгебраические коды в своей основе [5];

– «Гиперикум» – схема постквантовой электронной подписи, основанная на сжимающем хэширующем дереве [6];

– «Крыжовник» – схема постквантовой электронной подписи, основанная на решетках [2].

Еще одно из решений, схема постквантовой инкапсуляции ключа, основанная на изогениях суперсингулярных эллиптических кривых под названием «Форзиция», предлагалось в 2021 году [7], но ряд публикаций о слабостях реализации данной конструкции [8] стал основанием для приостановки исследований. В связи с опубликованной в 2022 году атакой Кастрика-Декру [9] на похожую криптосистему SIKE (участвовала в конкурсе NIST), работы над «Форзицией» приостановлены.

На текущий момент перспективными признаны схемы, основанные на следующих конструкциях:

– алгебраические решетки,

– коды, исправляющие ошибки,

– хэш-функции.

Некоторыми достоинствами схем, основанных на решетках, является достаточно высокая производительность. Современные криптосистемы на решетках, такие как Kyber, Dilithium (финалисты конкурса NIST), «Крыжовник» используют модификацию задачи обучения с ошибками для колец алгебраических чисел (Module-LWE).

Схемы на основе кодов не вошли в число финалистов конкурса NIST. В России к таким схемам относятся «Шиповник» и «Кодиеум». Основным их преимуществом перед схемами, основанными на решетках, является меньшая длина ключей.

Схемы на основе хэш-функций сейчас представлены алгоритмом SPHINCS+ (NIST) и «Гиперикум».

Синтез и исследование механизмов, построенных на изогениях эллиптических кривых и системах полиномиальных уравнений от многих переменных, на данный момент приостановлены.

Кроме того, в настоящее время востребованы исследования в следующих направлениях:

– Подходы к встраиванию перспективных постквантовых криптографических механизмов в протокол TLS версии 1.2;

– Подходы к построению механизмов инкапсуляции ключа с использованием одновременно классических и постквантовых криптографических механизмов;

– Использование нескольких ключевых обменов и дополнительных симметричных ключей в протоколе IKEv2 (протокол IPSec).

Технология квантового распределения ключей для задач защиты информации и стандартизация

В направлении защиты информации от квантовой угрозы созданы и развиваются:

– программные решения на основе квантово-устойчивых алгоритмов шифрования;

– программно-аппаратные комплексы квантового распределения ключей.

Согласно открытой информации, рабочая группа «Квантовые криптографические системы выработки и распределения ключей» (далее – РГ ККС ВРК) входит в подкомитет 4 «Российские шифровальные (криптографические) средства защиты информации», не содержащей сведений, составляющих государственную тайну, или относимых к охраняемой в соответствии с законодательством Российской Федерации к информации ограниченного доступа, а также зарубежные шифровальные (криптографические) средства защиты информации на территории Российской Федерации».

К настоящему моменту в РФ утверждены рекомендации по стандартизации, разработанные с участием РГ ККС ВРК:

– Р 1323565.1.060–2024 «Информационная технология. Криптографическая защита информации. Ключевая система сети шифрованной связи с использованием ККС ВРК с сетевой топологией «звезда»;

– Р 1323565.1.061–2024 «Информационная технология. Криптографическая защита информации. Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ»;

Текущие работы связаны с разработкой методических рекомендаций в областях:

– Термины и определения в области ККС ВРК;

– Принципы разработки и модернизации квантовых криптографических систем выработки и распределения ключей;

– Принципы разработки квантового генератора случайных чисел;

– Математические алгоритмы, сопутствующие реализации квантового генератора случайных чисел;

– Механизмы гибридизации ключей.

Другие возможные направления настоящих и будущих исследований

С учетом возможного влияния квантового вычислителя на системы защиты информации представляет интерес направление, связанное с разработкой рекомендаций по оценке стойкости симметричных криптографических конструкций, что отмечено в 2018 году в работе [10]. Является актуальной оценка необходимого количества логических кубитов и квантовых вентилей для реализации алгоритмов блочного шифрования в виде квантовых схем. Результаты для алгоритмов Simplified-DES и ГОСТ 34.12-2018 представлены в 2019 году в докладе [11].

Исследования постквантовой стойкости симметричных криптографических примитивов включают изучение алгоритмов Гровера, Саймона и их комбинации. Квантовый алгоритм Гровера [12], позволяет решать задачу нахождения элемента в неупорядоченном массиве размерности N за $O(\sqrt{N})$ обращений к квантовому оракулу. Этот алгоритм часто используют в криптоанализе для ускорения атаки полным перебором. Известна работа [13], в которой алгоритм Гровера используется для нахождения решения систем полиномиальных уравнений. Представляет интерес исследование возможности построения алгебраических атак на блочные алгоритмы шифрования со следующими этапами:

– Построение системы полиномиальных уравнений над полем $GF(2)$ по описанию алгоритма блочного шифрования;

– Построение квантовой схемы оракула для алгоритма Гровера на основе полученной в п.1 системы полиномиальных уравнений;

– Оценка трудоемкости построенной атаки: число итераций схемы и необходимое количество кубитов и квантовых вентилей.

В работе [14] представлена модель доказуемой (редукционистской) стойкости, формализующая обеспечение конфиденциальности в условиях наличия у нарушителя доступа к квантовому оракулу.

Заключение

В статье представлены некоторые актуальные направления в области стандартизации квантовой и постквантовой криптографии, среди которых наиболее активно развиваются постквантовые криптографические механизмы и квантовые криптографические системы выработки и распределения ключей. Представлено направление, связанное связанное с разработкой рекомендаций по оценке стойкости симметричных криптографических конструкций в условия наличия у нарушителя квантового вычислителя.

Список использованных источников

1. Маршалко Г.Б. Страх и ненависть в постквантовой криптографии. *Конференция РусКрипто'24*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/01_marshalko.pdf (дата обращения 08.03.2025)

2. Смышляев С.В. Массовая постквантовая криптография: задачи и перспективы. *Конференция РусКрипто'24*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/ 01_smyshlyaev.pdf (дата обращения 08.03.2025)

3. Post-Quantum Cryptography. Editors: Daniel J. Bernstein. Johannes Buchmann, Erik Dahmen. 2009. URL: https://link.springer.com/book/10.1007/978-3-540-88702-7 (дата обращения 08.03.2025)

4. Высоцкая В., Дас Д. Анализ устойчивости постквантовой электронной подписи «Шиповник» к атакам, нацеленным на хэш-функции. *Конференция РусКрипто'24*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/05_vysotskaya_das.pdf (дата обращения 08.03.2025)

5. Высоцкая В., Чижов И. Постквантовая схема инкапсуляции ключа «Кодиеум». *Конференция РусКрипто'24*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/ 05_vysotskaya_chizhov.pdf (дата обращения 08.03.2025)

6. Гребнев С. Гиперикум – проект квантово-устойчивой цифровой подписи для стандартизации в России. *Конференция РусКрипто'23*. URL: https://ruscrypto.ru/resource/ archive/rc2023/files/02_grebnev.pdf (дата обращения 08.03.2025)

7. Гребнев С., Ключарев П., Коренева А., Кошелев Д., Тараскин О., Тулебаев А. Форзиция: протокол выработки общего ключа на основе аппарата изогений суперсингулярных эллиптических кривых. Конференция РусКрипто'21. URL: https://ruscrypto.ru/resource/archive/rc2021/files/02_grebnev_klucharev_koreneva_koshelev_taraskin_tulebayev.pdf (дата обращения 08.03.2025)

8. Udovenko A., Vitto G. Revisiting Meet-in-the-Middle Cryptanalysis of SIDH/SIKE with Application to the $IKEp182 Challenge. 2021. DOI: 10.1007/978-3-031-58411-4_10

9. Castryck W., Decru T. An efficient key recovery attack on SIDH. 2022.

10. Naya-Plasencia M. New results on symmetric quantum cryptanalysis. *Crossfyre 2018 - 8th international workshop on cryptography, robustness, and provably secure schemes for female young researcher*s. Sep 2018, Surrey, United Kingdom.

11. Денисенко Д.В., Никитенкова М.В., Поляков М.В., Рудской В.И. Влияние теории квантовых вычислений на развитие современной криптографии. *Конференция РусКрипто'19*. URL: https://ruscrypto.ru/resource/archive/rc2019/files/02_Denisenko_Ni kitenkiva_Polyakov_Rudskoy.pdf (дата обращения 08.03.2025)

12. Lov K. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery*. pp. 212-219

13. S. Jaques. M. Naehrig, M. Roettler. F. Virdia. Implementing Grover oracles for quantum key search on AES and LowMC. arXiv:1910.01700

14. Коренева А. М., Фирсов Г. В. Атака различения на один режим работы блочных шифров при наличии у нарушителя доступа к квантовому оракулу. *ПДМ. Приложение*. 2024, № 17. 98–102

References

1. Marshalko G.B. Fear and loathing in post-quantum cryptography. *RusCrypto'24 conference*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/01_marshalko.pdf (accessed 08.03.2025)

2. Smyshlyaev S.V. Mass post-quantum cryptography: challenges and prospects. *RusCrypto'24 conference*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/ 01_smyshlyaev.pdf (accessed 08.03.2025)

3. Post-Quantum Cryptography, Editors: Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, 2009. URL: https://link.springer.com/book/10.1007/978-3-540-88702-7 (accessed 08.03.2025)

4. Vysotskaya V., Das D. Analyzing the resistance of post-quantum electronic signature "Shipovnik" to attacks targeting hash functions. RusCrypto'24 conference. URL: https://ruscrypto.ru/resource/archive/rc2024/files/05_vysotskaya_das.pdf (accessed 08.03.2025)

5. Visotskaya V., Chizhov I. A post-quantum encapsulation scheme for "Codieum" key encapsulation. *RusCrypto'24 conference*. URL: https://ruscrypto.ru/resource/archive/rc2024/files/ 05_vysotskaya_chizhov.pdf (accessed 08.03.2025)

6. Grebnev S. Hypericum - quantum-resistant digital signature project for standardization in Russia. *RusCrypto'23 conference*. URL: https://ruscrypto.ru/resource/ archive/rc2023/files/02_grebnev.pdf (accessed 08.03.2025)

7. Grebnev S., Klyucharev P., Koreneva A., Koshelev D., Taraskin O., Tulebaev A. Forzizia: a protocol for generating a shared key based on the isogeny apparatus of super-singular elliptic curves. *RusCrypto'21 conference*. URL: https://ruscrypto.ru/resource/archive/rc2021/files/02_grebnev_klucharev_koreneva_koshelev_taraskin_tulebayev.pdf (accessed 08.03.2025)

8. Udovenko A., Vitto G. Revisiting Meet-in-the-Middle Cryptanalysis of SIDH/SIKE with Application to the $IKEp182 Challenge. 2021. DOI: 10.1007/978-3-031-58411-4_10

9. Castryck W., Decru T. An efficient key recovery attack on SIDH. 2022.

10. Naya-Plasencia M. New results on symmetric quantum cryptanalysis. *Crossfyre 2018 – 8th international workshop on cryptography, robustness, and provably secure schemes for female young researcher*s. Sep 2018, Surrey, United Kingdom.

11. Denisenko D.V., Nikitenkova M.V., Polyakov M.V., Rudskoy V.I. Influence of the theory of quantum computing on the development of modern cryptography. *RusCrypto'19 conference*. URL: https://ruscrypto.ru/resource/archive/rc2019/files/02_Denisenko_Ni kitenkiva_Polyakov_Rudskoy.pdf (accessed 08.03.2025)

12. Lov K. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery*. pp. 212-219

13. S. Jaques. M. Naehrig. M. Roettler. F. Virdia. Implementing Grover oracles for quantum key search on AES and LowMC. arXiv:1910.01700

14. Koreneva A.M., Firsov G.V. Post-quantum distinguishing attack on one block ciphers mode of operation. *Applied Discrete Mathematics. Supplement*. 2024. № 17, 98–102

Сведения об авторе

Коренева А.М., канд. физ.-мат. наук, доцент. Финансовый университет при Правительстве РФ, начальник отдела криптографического анализа. ООО «Код Безопасности». a.koreneva@securitycode.ru.

Information about the author

Koreneva A., Cand. Sci. (Phys.-Math.). Associate Professor. Financial university under the Government of the Russian Federation. Head of cryptography department. Security Code LLC. a.koreneva@securitycode.ru.