http://dx.doi.org/10.35596/1729-7648-2025-23-6-65-70

УДК 004.021:004.056.55

ВЫБОР АЛГОРИТМОВ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ ДЛЯ СТАНДАРТИЗАЦИИ И ОЦЕНКИ ИХ БЕЗОПАСНОСТИ

С. Ю. МИХНЕВИЧ[1,2], П. И. ГЛАДУН[1]

[1]Белорусская государственная академия связи (Минск, Республика Беларусь)
[2]Белорусский государственный университет информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. Показан процесс выбора алгоритмов постквантовой криптографии для стандартизации на основе параметров, предлагаемых Национальным институтом стандартов и технологий США. Выполнена оценка стойкости алгоритмов постквантовой криптографии к атакам классических и квантовых компьютеров с учетом их особенностей. Обосновано различное количество операций для атак со стороны квантовых и классических компьютеров. Проанализированы возможности распараллеливания алгоритмов постквантовой криптографии. Отмечено, что несмотря на предполагаемое использование квантовых компьютеров, основная задача криптографии – применение алгоритмов, построенных на задачах, не сводимых к задачам P-типа сложности.

Ключевые слова: алгоритмы постквантовой криптографии, стандартизация, параметры безопасности криптографических алгоритмов, глубина схемы, распараллеливание.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Михневич, С. Ю. Выбор алгоритмов постквантовой криптографии для стандартизации и оценки их безопасности / С. Ю. Михневич, П. И. Гладун // Доклады БГУИР. 2025. Т. 23, № 6. С. 65–70. http://dx.doi.org/10.35596/1729-7648-2025-23-6-65-70.

SELECTION OF POST-QUANTUM CRYPTOGRAPHY ALGORITHMS FOR STANDARDIZATION AND ASSESSMENT OF THEIR SECURITY

SVETLANA YU. MIKHNEVICH[1,2], PAVEL I. HLADUN[1]

[1]Belarusian State Academy of Communications (Minsk, Republic of Belarus),
[2]Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. The process of selecting post-quantum cryptography algorithms for standardization based on parameters proposed by the National Institute of Standards and Technology (NIST) is described. The resistance of post-quantum cryptography algorithms to attacks by classical and quantum computers is assessed, taking into account their specific features. The different numbers of operations for attacks by quantum and classical computers are substantiated. The parallelization potential of post-quantum cryptography algorithms is analyzed. It is noted that, despite the proposed use of quantum computers, the primary goal of cryptography is the application of algorithms based on problems that are not reducible to problems of P-class complexity.

Keywords: post-quantum cryptography algorithms, standardization, cryptographic algorithm security parameters, circuit depth, parallelization.

Conflict of interests. The authors declare that there is no conflict of interests.

For citation. Mikhnevich S. Yu., Hladun P. I. (2025) Selection of Post-Quantum Cryptography Algorithms for Standardization and Assessment of Their Security. *Doklady BGUIR*. 23 (6), 65–70. http://dx.doi.org/10.35596/1729-7648-2025-23-6-65-70 (in Russian).

Введение

Неотъемлемая часть информатизации – защита персональных данных и другой служебной информации при их пересылке. Для этого наравне с защищенными каналами связи используются криптографические методы. Криптография основана на математически сложных задачах, решение которых требует временных и материальных ресурсов. Благодаря квантовым вычислительным алгоритмам можно значительно сократить время, необходимое для решения задач такого вида [1, 2]. Некоторые глобальные компании уже переходят к использованию алгоритмов постквантового шифрования [3].

Вместе с тем остается много вопросов, связанных с постквантовыми алгоритмами шифрования. Например, на чем основывается выбор алгоритма постквантовой криптографии и длины ключа для конкретной задачи? Какие параметры описывают стойкость постквантовых алгоритмов и их допустимые значения? Можно ли сделать настоящие криптографические схемы совместимыми с постквантовыми? Какие параметры в постквантовых алгоритмах можно стандартизировать [2]? Для ответа на эти вопросы Национальный институт стандартов и технологий США (NIST) в 2016 г. начал процесс стандартизации алгоритмов постквантовой криптографии (PQC). Оценка происходила в четыре этапа, на которых изучались все предложенные алгоритмы (82) по следующим критериям в порядке значимости: безопасность, стоимость и производительность, практичность[1234].

Выбор алгоритмов постквантовой криптографии для стандартизации

Следует отметить, что абсолютно стойкие криптографические шифры очень дорогие и не практичны в использовании [4]. Поэтому NIST оценивал соотношение стойкости криптографического алгоритма и его практичности.

Для оценки безопасности в NIST определили пять уровней криптографической стойкости[5], а также изучили устойчивость к атакам по сторонним каналам, к многоключевым атакам и несанкционированному использованию. На последних этапах стойкость алгоритма проверялась на неразличимость при атаке с помощью выбранного шифротекста (IND-CCA).

При оценке стоимости и производительности изучались:

– размеры открытых ключей, шифр текста и подписей;

– эффективность вычислений при генерации ключей, а также операций с открытыми и закрытыми ключами;

– вероятность ошибок дешифрования.

Практичность оценивалась преимущественно алгоритмами, способными эффективно работать на большем количестве платформ, расширять набор команд для достижения лучшей производительности с учетом гибкости, простоты и легкости внедрения. На последних этапах важной характеристикой представленных алгоритмов было их потенциальное влияние на производительность существующих широко используемых протоколов (например, TLS, IPsec, SSH) и сертификатов. Кроме того, учитывался один их важных оценочных факторов – может ли патент помешать принятию криптографического стандарта. Заключительные отчеты по этапам оценки были опубликованы в 2019, 2020, 2022 и 2025 гг. На третьем (предпоследнем) этапе стандартизации остались:

• алгоритмы шифрования с открытым ключом, механизм инкапсуляции ключей (PKE/KEM): Classic McEliece, CRYSTALS-Kyber, NTRU, Saber;

• схемы цифровой подписи: CRYSTALS-Dilithium, Falcon, Rainbow.

[1] Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process: NISTIR 8240. 2019. https://doi.org/10.6028/NIST.IR.8240.

[2] Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process: NISTIR 8309. 2020. https://doi.org/10.6028/NIST.IR.8309.

[3] Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process: NISTIR 8413. 2022. https://doi.org/10.6028/NIST.IR.8413.

[4] Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process: NISTIR 8545. 2025. https://doi.org/10.6028/NIST.IR.8545.

[5] Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. Mode of access: https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/call-for-proposals-final-dec-2016.pdf. Date of access: 22.07.2025.

Альтернативные алгоритмы-кандидаты включали:

• алгоритмы PKE/KEM: BIKE, FrodoKEM, HQC, NTRU Prime, SIKE;

• схемы цифровой подписи: GeMSS, Picnic, SPHINCS+.

Проведя оценку этапов, NIST выбрал четыре алгоритма для стандартизации сразу после третьего раунда – алгоритм PKE/KEM CRYSTALS-Kyber и цифровые подписи CRYSTALS-Dilithium, Falcon, SPHINCS+.

Различные криптографические алгоритмы применяются для разных целей. Например, в настоящее время алгоритмы симметричного шифрования AES, DES, 3DES и другие используются для шифрования/дешифрования большого объема информации (работают в основном быстрее ассиметричных алгоритмов, но требуют безопасного обмена ключами). Алгоритмы ассиметричного шифрования RSA, DSA, Diffie-Hellman, ECC и т. п. решают проблему обмена ключами. Для шифрования при передаче информации используются RSA, AES, DES, для цифровой подписи – DSA, ECDSA, RSA. Цель алгоритмов цифровой подписи – аутентификация отправителя и проверка целостности сообщения, т. е. подтверждение, что сообщение не было изменено после подписи. В качестве алгоритма формирования ключа используется в основном Diffie-Hellman.

В PQC сформированы следующие основные направления разработки криптографических алгоритмов:

– криптография на основе решеток (Lattice-based cryptography);

– криптография на основе хеш-функций (Hash-based cryptography);

– криптография на изогениях суперсингулярных эллиптических кривых (Isogeny based cryptography);

– многомерная криптография, в которой используются системы многомерных полиномиальных уравнений (Multivariate cryptography);

– криптография на основе кодов (Code-based cryptography)[1–4].

Пропорциональный объем публикаций за последние пять лет по данным направлениям и алгоритмам, выделенным NIST, приведен на диаграмме Венна на рис. 1. Диаграмма описывает области исследований PQC [1].

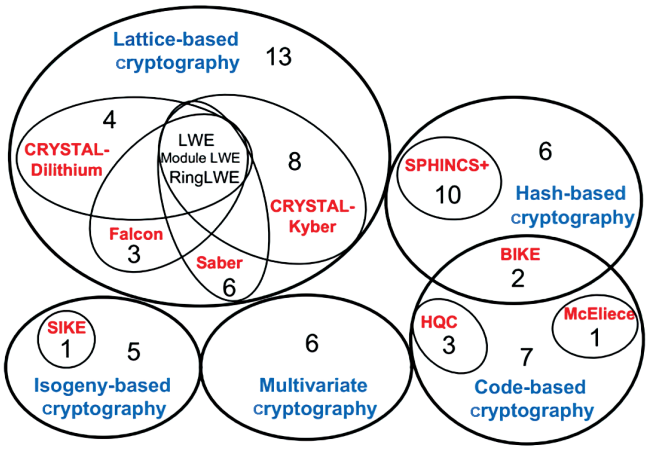

Рис. 1. Диаграмма Венна, отображающая пропорциональный объем публикаций за последние пять лет по алгоритмам

Fig. 1. A Venn diagram showing the proportional volume of publications over the past five years by algorithm

В 2024 г. NIST выпустил серию стандартов для федерального использования:

– FIPS 203 – стандарт механизма инкапсуляции ключей на основе модульной решетки, основан на алгоритме CRYSTALS-Kyber[6];

– FIPS 204 – стандарт цифровой подписи на основе модульной решетки, основан на алгоритме CRYSTALS-Dilithium[7];

[6] Module-Lattice-Based Key-Encapsulation Mechanism Standard: Federal Information Processing Standards Publication 203, 2024. https://doi.org/10.6028/NIST.FIPS.203.ipd.

[7] Module-Lattice-Based Digital Signature Standard: Federal Information Processing Standards Publication 204, 2024. https://doi.org/10.6028/NIST.FIPS.204.

– FIPS 205 – стандарт цифровой подписи на основе хеша без сохранения состояния, основан на алгоритме SPHINCS+[8].

Эти стандарты обязательны для применения к информационным системам, используемым или эксплуатируемым федеральными агентствами и их подрядчиками, но они не применяются к системам национальной безопасности США. В настоящее время Международная организация по стандартизации (ISO) рассматривает алгоритм Classic McEliece (основан на использовании двоичных кодов Гоппы) для стандартизации.

В последнем отчете 2025 г. NIST сравнивал KEM-алгоритмы на основе кодов BIKE, HQC, Classic McEliece и алгоритм на основе изогений суперсингулярных эллиптических кривых SIKE. В результате для стандартизации выбран алгоритм HQC (квазициклический алгоритм Хэмминга)[4].

Оценка криптографической стойкости алгоритмов постквантовой криптографии

Следует отметить, что стандартизация алгоритмов PQC должна учитывать атаки классических и квантовых компьютеров или их совместное использование. Вместе с тем тестирование стойкости алгоритмов к атакам проводилось с применением классических компьютеров. NIST признает неопределенность в оценке уровней безопасности алгоритмов PQC при использовании квантовых компьютеров, которые в настоящее время еще развиваются, и их итоговые характеристики не известны. Кроме того, еще не разработаны основные алгоритмы для квантовых компьютеров. Для оценки защищенности алгоритмов от атак с помощью квантовых компьютеров приняты следующие подходы.

В [5] на основе применения алгоритма Гровера для взлома стандартизированных FIPS-алгоритмов AES-k (AES – симметричный алгоритм блочного шифрования; k составляет 128, 192 и 256 бит) при оценке ресурсов квантового компьютера предложено использовать три параметра: количество вентилей (гейтов), глубину схемы (количество последовательных слоев квантовых вентилей) и количество кубитов. Для временной оценки реализации алгоритма достаточно использовать только глубину схемы.

NIST определил отдельную категорию для каждого из требований безопасности, которые перечислены в порядке возрастания силы.

1. Любая атака, нарушающая соответствующее определение безопасности, должна требовать вычислительных ресурсов, сопоставимых или превышающих те, которые нужны для поиска ключа в блочном шифре со 128-битным ключом (например, AES-128).

2. Любая атака, нарушающая соответствующее определение безопасности, должна требовать вычислительных ресурсов, сопоставимых или превышающих те, которые нужны для поиска коллизий в 256-битной хеш-функции (например, SHA-256/SHA3-256) (SHA – алгоритм хеширования).

3. Любая атака, нарушающая соответствующее определение безопасности, должна требовать вычислительных ресурсов, сопоставимых или превышающих те, которые нужны для поиска ключа в блочном шифре со 192-битным ключом (например, AES-192).

4. Любая атака, нарушающая соответствующее определение безопасности, должна требовать вычислительных ресурсов, сопоставимых или превышающих те, которые нужны для поиска коллизий в 384-битной хеш-функции (например, SHA-384/SHA3-384).

5. Любая атака, нарушающая соответствующее определение безопасности, должна требовать вычислительных ресурсов, сопоставимых или превышающих те, которые нужны для поиска ключа в блочном шифре с 256-битным ключом (например, AES-256)[5].

Для оценки длительности вычислений применяются алгоритмы AES и SHA потому, что время их взлома путем перебора на квантовом компьютере может быть ускорено по сравнению с классическим компьютером всего лишь в корень квадратный для AES и корень кубический для SHA. Следует отметить, что алгоритм Шора тоже эффективно решает задачи факторизации целых чисел и дискретного логарифмирования за полиномиальное время на квантовом компьютере. Алгоритм AES-256 считается в некотором приближении устойчивым к атакам квантового компьютер [2]. В табл. 1 приведены уровни сложности криптографических алгоритмов.

[8] Stateless Hash-Based Digital Signature Standard: Federal Information Processing Standards Publication 205, 2024. https://doi.org/10.6028/NIST.FIPS.205.

Таблица 1. Уровни сложности криптографических алгоритмов[5]
Table 1. Complexity levels of cryptographic algorithms[5]

Алгоритм	Уровень сложности
AES-128	2^{170}/MAXDEPTH* квантовых вентилей или 2^{143} классических операций
SHA3-256	2^{146} классических операций
AES-192	2^{233}/MAXDEPTH квантовых вентилей или 2^{207} классических операций
SHA3-384	2^{210} классических операций
AES-256	2^{298}/MAXDEPTH квантовых вентилей или 2^{272} классических операций
SHA3-512	2^{274} классических операций
*MAXDEPTH – глубинная схема.	

В качестве параметра времени выполнения NIST предлагает использовать подход, при котором квантовые атаки ограничиваются фиксированным временем выполнения или MAXDEPTH. Возможные значения MAXDEPTH варьируются от 2^{40} логических вентилей (приблизительное количество вентилей, которое, как ожидается, современные архитектуры квантовых вычислений смогут последовательно выполнить за год) до 2^{64} логических вентилей (приблизительное количество вентилей, которое современные архитектуры классических вычислений могут последовательно выполнить за десятилетие), и до не более 2^{96} логических вентилей (приблизительное количество вентилей, которое кубиты атомного масштаба со скоростью распространения света могли бы выполнить за тысячелетие)[5].

Тот факт, что количество вентилей для квантового компьютера больше, чем для классического, объясняется разными алгоритмами. Даже базовые логические операции на квантовом и классическом компьютерах отличаются, поэтому будут отличаться и алгоритмы, реализующие аналогичные вычисления. Но квантовые вычисления могут быть значительно ускорены благодаря возможности параллельного анализа большого пространства решений. В общем, весь криптоанализ основан на сложной с точки зрения математики задаче, что позволяет в методе перебора при увеличении длины ключа говорить об экспоненциальной ($O(2^n)$) или почти экспоненциальной сложности, если, конечно, математическая задача не может быть сведена к алгоритму полиномиальной сложности на детерминированной машине Тьюринга.

Распараллеливание алгоритмов постквантовой криптографии может в принципе ускорить процесс криптоанализа. Многие алгоритмы постквантовой криптографии используют как минимум операцию умножения матриц, которую можно эффективно распараллелить на нескольких процессорах. Так, криптография на основе кода может быть распараллелена, поскольку шифрование сообщения состоит просто в применении соответствующего корректирующего кода, т. е. в выполнении векторного матричного произведения. В методе криптографии на основе решеток также используются матрицы. В качестве примера можно привести следующее: выбираются два секретных полинома d, e с небольшими коэффициентами (–1, 0, 1) и вычисляется $c = hd + e(\mathrm{mod} x^p - 1)\mathrm{mod} q$ (c – зашифрованный текст; h – открытый ключ; x – сообщение; p, q – параметры криптографического алгоритма). Здесь применяется матричное произведение полиномов h и d, поскольку в виде матриц полиномы умножаются гораздо быстрее. Метод криптографии на основе сигнатур многомерных квадратных уравнений содержит аффинные преобразования многочленов, что также можно представить в матричном виде.

Однако ускорение за счет возможного распараллеливания алгоритма шифрования для ускорения метода перебора в сети классических компьютеров не даст большого эффекта из-за большого пространства решений (2^n). А перевод напрямую классических алгоритмов на квантовый компьютер и использование его возможностей для параллельного анализа большого пространства решений невозможны вследствие разных логик классического и квантового компьютеров. Таким образом, несмотря на создание квантовых компьютеров, основная задача криптоанализа заключается в разработке алгоритма, уменьшающего пространство решений для конкретных алгоритмов шифрования, а задача криптографии – использование алгоритмов, которые не могут быть сведены к задачам P-типа, т. е. алгоритмам полиномиальной сложности на детерминированной машине Тьюринга.

Выводы

Рассмотрены процесс выбора алгоритмов постквантовой криптографии для стандартизации и параметры их отбора. Приведен параметр оценки стойкости постквантовых алгоритмов к атакам с использованием классических и квантовых компьютеров. Проанализирована возможность распараллеливания алгоритмов постквантовой криптографии. Показано, что это неэффективно для атак со стороны как квантовых, так и классических компьютеров. Обосновано, что основной задачей криптографии остается использование алгоритмов, не сводимых к задачам P-типа.

Список литературы / References

1. Duc-Thuan Dam, Thai-Ha Tran, Van-Phuc Hoang (2023) A Survey of Post-Quantum Cryptography: Start of a New Race. *Cryptography*. (7). https://doi.org/10.3390/ryptography7030040.
2. Niederhagen R., Waidner M. (2017) *Practical Post–Quantum Cryptography*. Darmstadt, Fraunhofer Institute for Secure Information Technology.
3. Google Announces New Algorithm That Makes FIDO Encryption Safe From Quantum Computers. *Ars Technica.* Available: https://arstechnica.com/security/2023/08/passkeys-are-great-but-not-safe-from-quantum-computers-dilithium-could-change-that/ (Accessed 20 March 2025).
4. Yashchenko V. V. (1998) Basic Concepts of Cryptography. *Mathematical Education*. 3 (2), 53–70 (in Russian).
5. Grassl M., Langenberg B., Roetteler M., Steinwandt R. (2025) Applying Grover's Algorithm to AES: Quantum Resource Estimates. *arXiv:1512.04965v1*. Available: https://doi.org/10.48550/arXiv.1512.04965 (Accessed 20 March 2025).

Поступила 19.09.2025
Received: 19 September 2025

Принята в печать 09.10.2025
Accepted: 9 October 2025

Вклад авторов

Михневич С. Ю. провела анализ стандартизации алгоритмов постквантовой криптографии.

Гладун П. И. принимал участие в рассмотрении вопросов, связанных с криптографической стойкостью алгоритмов постквантовой криптографии.

Authors' contribution

Mikhnevich S. Yu. conducted the standardization analysis of post-quantum cryptography algorithms.

Gladun P. I. took part in the consideration of issues related to the cryptographic stability of post-quantum cryptography algorithms.

Сведения об авторах

Михневич С. Ю., канд. физ.-мат. наук, доц., зав. каф. инфокоммуникационных технологий, Белорусская государственная академия связи; доц. каф. информационных радиотехнологий, Белорусский государственный университет информатики и радиоэлектроники

Гладун П. И., преп. каф. инфокоммуникационных технологий, Белорусская государственная академия связи

Information about the authors

Mikhnevich S. Yu., Cand. Sci. (Phys. and Math.), Associate Professor, Head of the Department of Infocommunication Technologies, Belarusian State Academy of Communications; Associate Professor at the Department of Information Radiotechlogies, Belarusian State University of Informatics and Radioelectronics

Hladun P. I., Lecturer at the Department of Infocommunication Technologies, Belarusian State Academy of Communications

Адрес для корреспонденции

220076, Республика Беларусь,
Минск, ул. Ф. Скорины, 8/2
Белорусская государственная академия связи
Тел.: +375 44 701-15-67
E-mail: s.mikhnevich@bsac.by
Михневич Светлана Юрьевна

Address for correspondence

220076, Republic of Belarus,
Minsk, F. Skoryna St., 8/2
Belarusian State Academy of Communications
Tel.: +375 44 701-15-67
E-mail: s.mikhnevich@bsac.by
Mikhnevich Svetlana Yurievna