DOI: 10.25559/SITITO.020.202401.27-33
УДК 004.056.55

Оригинальная статья

Применение алгоритмов на решётках в постквантовой криптографии

Н. А. Урбан*, Е. А. Мельникова
ФГБОУ ВО «Российский государственный социальный университет», г. Москва, Российская Федерация
Адрес: 129226, Российская Федерация, г. Москва, ул. Вильгельма Пика, д. 4, стр. 1
* urbannikolai@mail.ru

Аннотация
В статье приведён анализ подходов к разработке постквантовых алгоритмов, проведён обзор прогресса в сфере квантовых компьютеров и постквантовых криптографических систем шифрования. Рассматривается один из наиболее перспективных подходов который основывается на теории решёток. Приведены трудно решаемые задачи, на основе которых построены криптографические примитивы теории решёток. В статье боле подробно рассмотрена схема шифрования Goldreich Goldwasser Halevi, построенная на теории решёток. В статье представлен программный комплекс, который позволяет пользователю изучать основные функции схемы GGH: алгоритмы генерации ключей, алгоритмы шифрования и расшифровки сообщения. В статье указаны основные назначения модулей программного комплекса, описан пользовательский интерфейс программы. Также программный комплекс даёт возможность провести атаку на схему шифрования с помощью алгоритма Ленстра-Ленстра-Ловаса. Данное приложение может быть использовано как часть лабораторного комплекса при изучении криптографических средств защиты информации.

Ключевые слова: постквантовые алгоритмы шифрования, криптосистема, кубит, схема шифрования Goldreich Goldwasser Halevi, криптография на основе теории решёток

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Урбан Н. А., Мельникова Е. А. Применение алгоритмов на решётках в постквантовой криптографии // Современные информационные технологии и ИТ-образование. 2024. Т. 20, № 1. С. 27-33. https://doi.org/10.25559/SITITO.020.202401.27-33

Original article

Application of Algorithms on Lattices in Post-Quantum Cryptography

N. A. Urban*, E. A. Melnikova
Russian State Social University, Moscow, Russian Federation
Address: 4 Wilhelma Pika St., building 1, Moscow 129226, Russian Federation
* urbannikolai@mail.ru

Abstract
The article analyzes approaches to the development of post-quantum algorithms, reviews progress in the field of quantum computers and post-quantum cryptographic encryption systems. One of the most promising approaches is considered, which is based on the theory of lattices. Difficult-to-solve problems are presented, on the basis of which cryptographic primitives of lattice theory are constructed. The article discusses in more detail the Goldreich Goldwasser Halevi encryption scheme based on the theory of lattices. The article presents a software package that allows the user to study the main functions of the GGH scheme: key generation algorithms, encryption algorithms and message decryption. The article specifies the main purposes of the modules of the software package, and describes the user interface of the program. Also, the software package makes it possible to carry out an attack on the encryption scheme using the Lenstra-Lenstra-Lovasz algorithm. This application can be used as part of a laboratory complex when studying.

Keywords: post-quantum encryption algorithms, cryptosystem, qubit, Goldreich Goldwasser Halevi scheme, lattice-based cryptography

Conflict of interests: The authors declare no conflict of interest.

For citation: Urban N.A., Melnikova E.A. Application of Algorithms on Lattices in Post-Quantum Cryptography. *Modern Information Technologies and IT-Education.* 2024;20(1):27-33. https://doi.org/10.25559/SITITO.020.202401.27-33

Введение

Ещё в 2001 году темпы роста вычислительной мощности квантовых компьютеров позволили предсказать, что квантовые компьютеры, способные эффективно решать задачи криптоанализа используемых сейчас криптосистем, будут доступны в диапазоне 2028-2033 годов.

В опубликованном Научно-исследовательским институтом стандартизации США отчёте[1] эксперты предупреждают о способности квантовых компьютеров сделать небезопасным применение алгоритма RSA уже к 2030 году. Однако, прирост вычислительной мощности квантовых компьютеров уже превысил прогнозные показатели, а эффективность разрабатываемых вычислительных комплексов увеличивается с масштабированием таких систем [1].

Защищенность информации в современном цифровом мире зависит от устойчивости современных криптографических систем к различным атакам. И, если современные классические компьютеры уже способны на обработку колоссальных объёмов информации, то квантовые компьютеры в силу специфики вычислений, способны эффективно решать задачи из категории трудно вычислимых[2].

В ноябре 2022 года IBM представила самый мощный квантовый процессор в мире – Osprey, который имеет 433 кубита. На его основе готовится многопроцессорная система Quantum System Two[3]. А в апреле 2023 года канадская компания D-Wave представила результаты применения своего квантового процессора D-wave Advantage, имеющего 5760 кубитов, который показал наивысшую эффективность в задачах оптимизации 3D-спинового стекла, задачах, принадлежащих к классу трудно решаемых задачах оптимизации. В данный момент компания D-Wave работает над прототипом шестого поколения своего квантового компьютера – Advantage 2, который будет иметь 7 тысяч кубитов [2].

Появление мощных суперкомпьютеров и квантовых компьютеров поставило под угрозу безопасность классического шифрования. Развитие науки привело к созданию новых схем цифровой подписи и шифрования, поскольку основные используемые в настоящее время системы, RSA, ECDSA, не являются квантово-устойчивыми [3]. В случае использования классических вычислительных машин, для достижения достаточной криптостойкости, требуется слишком большая длина ключей [4].

Таким образом сформировалась задача поиска и разработки криптографических алгоритмов, устойчивых к квантовым вычислениям, и к сегодняшнему дню были предложены различные криптографические системы, которые могут быть надёжными при условии достаточности размера ключа.

С 2016 года Научно-исследовательским институтом стандартизации США проводится международный конкурс алгоритмов для формирования стандарта по квантово-безопасным криптосистемам, который на данный момент уже близится к завершению. При техническом комитете Росстандарта (ТК-26) ведется разработка отечественного набора квантово-устойчивых криптосистем, которые в ближайшем будущем дополнят семейство национальных стандартов. Подобный конкурс по выбору постквантовой криптографической системы проводился и в Китае силами Китайской ассоциации криптографических исследований [5-7].

Цель исследования: разработать программную реализацию одной из постквантовых криптографических систем, позволяющую в интерактивном режиме изучать принципы работы криптосистемы и возможности её взлома.

Современные подходы к построению постквантовых криптографических систем

При разработке постквантовых алгоритмов применяются следующие подходы [8, 9]:

- использование многомерных квадратичных систем [10, 11];
- построение электронных подписей на односторонних хэш-функциях [12];
- применение теории алгебраического кодирования [13];
- использование изогений эллиптических кривых [14];
- применение теории решеток [15-17];
- квантовое хеширование [18, 19].

В целях противодействия квантовым вычислениям хорошо подходит концепция обучения с ошибками, суть которой заключается в том, что в простые вычислительные задачи намеренно вносится ошибка, это делает их практически не решаемыми за приемлемое время с помощью известных методов.

Основные разработчики постквантовой криптографии используют эту концепцию в составе своих задач. Так, существует подход, использующий коды исправления ошибок (система Мак-Элиса и их модификации [20]), и подход, основывающийся на теории решёток (схема GGH, система NTRUEncrypt и их модификации[4]) [21].

К сегодняшнему дню, в рамках конкурса стандартизации NIST были выделены лучшие постквантовые схемы шифрования [22], среди которых одна схема подходит для реализации инкапсуляции ключей (PKE/KEM) – Crystalls-Kyber [23] и две схемы, подходящие для реализации цифровой подписи: Crystalls-Dilithium и SPHINCS+. В то время, как схема SPHINCS+ основана на построении односторонних хэш-функций, остальные являются представителями теории решёток.

Криптографические примитивы на основе задач теории решеток обладают очень сильной криптостойкостью, при этом

[1] Report on Post-Quantum Cryptography (NISTIR 8105) / L. Chen [et al.]. NIST, U.S. Department of Commerce, 2016. [Электронный ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (дата обращения: 08.12.2023).

[2] Матвеев Г. В. Разделение секрета в постквантовый период // Информационные системы и технологии: Материалы международного научного конгресса по информатике. В 3-х частях, Минск, 27-28 октября 2022 года / Редколлегия: С.В. Абламейко (гл. ред.) [и др.]. Том Часть 1. Минск : БГУ, 2022. С. 95-101. EDN: KOIRBJ

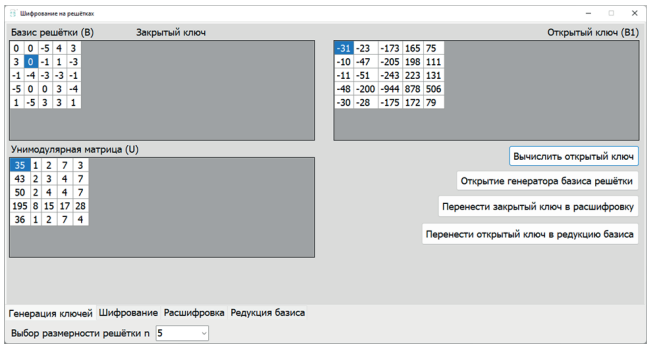
[3] IBM представляет квантовый процессор с более чем 400 кубитами [Электронный ресурс] // HPCwire. 10 нояб. 2022. URL: https://www.hpcwire.com/off-the-wire/ibm-unveils-400-qubit-plus-quantum-processor-and-next-gen-quantum-system-two/ (дата обращения: 08.12.2023).

[4] Черкесова Л. В., Ревякина Е. А., Ляшенко Н. Г. Разработка модификации постквантового алгоритма NTRUENCRYPT для противодействия атаке на основе подобранного шифротекста // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: Сб. статей Всероссийской научно-технической конференции, Таганрог, 10-15 апреля 2023 года. Таганрог: ЮФУ, 2023. С. 20-22. EDN: VACUPC

достаточно эффективно выполняются на компьютерах. Их криптостойкость основана на таких трудно вычислимых задачах теории решёток [24], как:
– нахождение кратчайшего вектора;
– нахождение идеального кратчайшего вектора;
– нахождение кратчайшего независимого вектора.
Goldreich-Goldwasser-Halevi (GGH) – первая схема подписи, основанная на решетках. В этой схеме сообщение необходимо хэшировать в пространство, на которое была проецирована решетка, а подпись для данного хэша в этом пространстве является ближайшим узлом решетки [13].
В основе алгоритма лежит функция с потайным входом. Эта функция, в свою очередь, опирается на сложность решения задачи нахождения ближайшего вектора. Функция реализуется добавлением вектора ошибки *в* вектор шифротекста[5].
Таким образом, закрытым ключом в схеме являются вектор ошибки e и две матрицы:
– ортогональная матрица – матрица B, чьи строки образуют базис решетки и представлены в виде ортогональных векторов;
– унимодулярная матрица – матрица U, определитель которой равен единице.
Открытым ключом является открытая матрица B1, получаемая умножением унимодулярной матрицы U на базис решётки B.
Для шифрования сообщения, необходимо произвести следующие действия: $c = Bm + e$, где c – вектор шифротекста, m – вектор исходного сообщения, e – вектор ошибки размерности n.
Для расшифровки вычисляем: $m = c * B^{-1} * U^{-1}$.
В 2006 г. модифицированная версия системы GGH была взломана Nguyen и Regev. Тем не менее, развитие криптосистемы считается перспективным [13, 25].

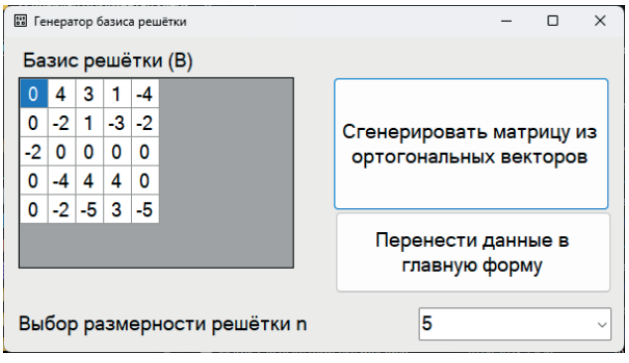
Разработка программного приложения

Был создан программный комплекс, позволяющий показать принципы работы схемы шифрования GGH, включая генерацию ключей, алгоритмы шифрования, расшифрования, а также реализацию атаки на эту криптосистему.
Программный продукт был написан на языке программирования C++/CLI или иначе C++/Common Language Infrastructure, что было удобно для реализации поддержки .Net Framework, сохраняя преимущества языка C++ в плане производительности, выделения и освобождения памяти, в то же время поддерживая реализацию интерфейса взаимодействия через API Windows Forms.
При открытии программы пользователя встречает вкладка генерации ключей. Сама генерация заключается в формировании закрытого и открытого ключа. Закрытый ключ состоит из базиса решётки, унимодулярной матрицы и вектора ошибки. При инициализации пользовательской формы прописана функция, задающая готовые значения для закрытого ключа, что удобно для того, чтобы можно было сразу начать ознакомление с устройством этой криптографической схемы.
Пользователю также предоставляется возможность самому ввести значения закрытого ключа: унимодулярной матрицы и базиса решётки. Причём, если введённые данные не будут корректны, то пользователю выводится подсказка, например, о том, что вводимые вектора должны быть линейно независимыми.
Вектор ошибки задан заранее, для каждой размерности он разный и обычно принимает небольшие положительные или отрицательные значения.
Интерфейс программы представлен на рисунке 1.



Р и с. 1. Интерфейс разработанной программы
F i g. 1. Interface of the developed program
Источник: здесь и далее в статье все рисунки составлены авторами.
Source: Hereinafter in this article all figures were drawn up by the authors.

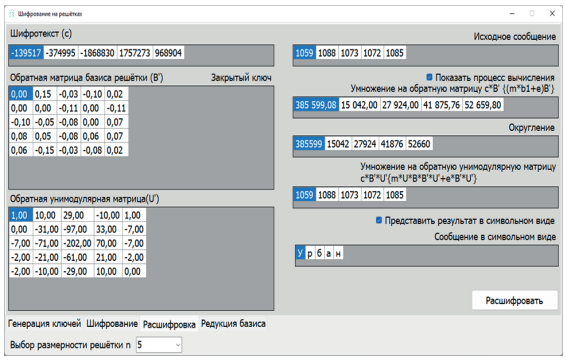
Пользователю предоставляется возможность воспользоваться генератором базисных векторов решётки. Генератор основывается на псевдослучайных алгоритмах, получаемые значения зависят от текущего момента времени, что повышает защиту от коллизий, то есть вероятность генерации абсолютно одинаковых матриц достаточно низка. Внешний вид формы с генератором базиса решётки приведён на рисунке 2.



Р и с. 2. Внешний вид формы генератора
F i g. 2. External appearance of the generator form

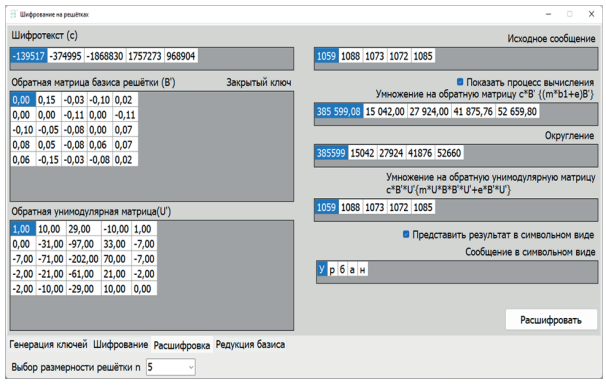
В разделе шифрование представлена возможность зашифровать сообщение, имеющее вид целых чисел или одиночных символов с помощью данной схемы шифрования.
Во вкладке Расшифровка представлен процесс вычисления исходного сообщения из шифротекста, рисунок 3а, 3б.

[5] Терентьев А. Д., Негрозов М. А., Мельникова Е. А. Разработка комплекса программ для изучения основ криптографии на решетках // Современные информационные технологии в образовании, науке и промышленности: XX Межд. конф. : сборник трудов. М. : Издательство «Экон-Информ», 2021. С. 171-173. EDN: YEUZHB



Р и с. 3а. Закрытый ключ

F i g. 3a. The private key



Р и с. 3б. Алгоритм шифрования

F i g. 3б. Encryption algorithm

Вкладка «Редукция базиса» предоставляет пользователю возможность провести атаку на схему шифрования с помощью алгоритма Ленстра-Ленстра-Ловаса (LLL). Редукция базиса построена на основе процесса Грама-Шмидта.

Заключение

Были проанализированы существующие подходы по построению устойчивых к квантовым вычислениям криптографических систем, среди которых был отмечен наиболее перспективный подход – подход с применением теории решёток. Разработанный программный комплекс позволяет пользователю исследовать основные функции криптосистемы GGH: генерацию ключей, шифрование и расшифрование, а также проведение атаки с помощью LLL-алгоритма. Данное приложение может быть использовано как часть лабораторного комплекса при изучении криптографических средств защиты информации.

Список использованных источников

[1] Mousa N., Shirazi F. A survey analysis of quantum computing adoption and the paradigm of privacy engineering // Security and Privacy. 2024. Vol. 7, issue 6. Article number: e419. https://doi.org/10.1002/spy2.419

[2] Quantum critical dynamics in a 5,000-qubit programmable spin glass / A. D. King [et al.] // Nature. 2023. Vol. 617. P. 61-66. https://doi.org/10.1038/s41586-023-05867-2

[3] Кириченко Е. А. Квантовое превосходство как угроза кибербезопасности и постквантовые методы криптографии // Вестник ИМСИТ. 2021. № 1(85). С. 37-39. EDN: KFKKBQ

[4] Квантовая устремленность как угроза информационной безопасности / А. В. Лукашев [и др.] // Международный журнал информационных технологий и энергоэффективности. 2023. Т. 8, № 6(32). С. 97-101. EDN: IQDQNH

[5] Назаренко А. П., Дмитриев Е. В. Современное состояние постквантовой криптографии в России и за рубежом // Системы синхронизации, формирования и обработки сигналов. 2021. Т. 12, № 6. С. 77-83. EDN: FNKIVP

[6] Минбалеев А. В., Берестнев М. А., Евсиков К. С. Обеспечение информационной безопасности оборудования добывающей промышленности в квантовую эпоху // Известия Тульского государственного университета. Науки о Земле. 2023. № 1. С. 567-584. https://doi.org/10.46689/2218-5194-2023-1-1-567-584

[7] A Survey of Post-Quantum Cryptography: Start of a New Race / D.-T. Dam [et al.] // Cryptography. 2023. Vol. 7, issue 3. Article number: 40. https://doi.org/10.3390/cryptography7030040

[8] Основные подходы к построению постквантовых криптосистем: описание, сравнительная характеристика / Е. С. Малыгина [и др.] // Прикладная дискретная математика. Приложение. 2023. № 16. С. 58-65. https://doi.org/10.17223/2226308X/16/16

[9] Кудряшов В. Е., Фионов А. Н. Проблема устойчивости современных криптосистем на фоне появления квантовых компьютеров // Интерэкспо Гео-Сибирь. 2022. Т. 6. С. 109-115. https://doi.org/10.33764/2618-981X-2022-6-109-115

[10] Selection Strategy of F4-Style Algorithm to Solve MQ Problems Related to MPKC / T. Kurokawa [et al.] // Cryptography. 2023. Vol. 7, issue 1. Article number: 10. https://doi.org/10.3390/cryptography7010010

[11] Макаров А. О. Схема постквантовой агрегированной подписи с ленивой проверкой на основе многомерных квадратичных многочленов // Безопасность информационных технологий. 2023. Т. 30, № 3. С. 30-50. https://doi.org/10.26583/bit.2023.3.02

[12] Матвеев Г. Математические аспекты постквантовой криптографии // Наука и инновации. 2023. № 8(246). С. 52-56. EDN: ELRJNN
[13] Анализ современных постквантовых алгоритмов шифрования / В. А. Буковшин [и др.] // Научное обозрение. Технические науки. 2019. № 4. С. 36-44. EDN:VGXBXK
[14] Drzazga B., Krzywiecki Ł. Review of Chosen Isogeny-Based Cryptographic Schemes // Cryptography. 2022. Vol. 6, issue 2. Article number: 27. https://doi.org/10.3390/cryptography6020027
[15] On Advances of Lattice-Based Cryptographic Schemes and Their Implementations / H. Bandara [et al.] // Cryptography. 2022. Vol. 6, issue 4. Article number: 56. https://doi.org/10.3390/cryptography6040056
[16] A High-Efficiency Modular Multiplication Digital Signal Processing for Lattice-Based Post-Quantum Cryptography / T.-H. Nguyen [et al.] // Cryptography. 2023. Vol. 7, issue 4. Article number: 46. https://doi.org/10.3390/cryptography7040046
[17] Timing-Attack-Resistant Acceleration of NTRU Round 3 Encryption on Resource-Constrained Embedded Systems / E. Camacho-Ruiz [et al.] // Cryptography. 2023. Vol. 7, issue 2. Article number: 29. https://doi.org/10.3390/cryptography7020029
[18] Орлов М. А., Нечаев К. А., Резниченко С. А. Оценка статистических свойств и криптографической стойкости случайных последовательностей, полученных квантовым компьютером IBM // Безопасность информационных технологий. 2023. Т. 30, № 1. С. 14-26. https://doi.org/10.26583/bit.2023.1.01
[19] Азман А. В., Растамханов Р. Н., Цуканов И. Р. Аутентификация распределения квантовых ключей с помощью постквантовой криптографии // Известия Тульского государственного университета. Технические науки. 2023. № 1. С. 29-35. https://doi.org/10.24412/2071-6168-2023-1-29-35
[20] Чижов И. В., Попова Е. А. Структурная атака на криптосистемы типа Мак-Элиса-Сидельникова, построенной на основе комбинирования случайных кодов с кодами Рида-Маллера // International Journal of Open Information Technologies. 2020. Т. 8, № 6. С. 24-33. EDN: NOIJEL
[21] Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era / M. E. Sabani [et al.] // Electronics. 2023. Vol. 12, issue 12. Article number: 2643. https://doi.org/10.3390/electronics12122643
[22] Karakaya A., Ulu A. A Review on Latest Developments in Post-Quantum Based Secure Blockchain Systems // 2023 11th International Symposium on Digital Forensics and Security (ISDFS). Chattanooga, TN, USA : IEEE Computer Society, 2023. P 1-6. https://doi.org/10.1109/ISDFS58141.2023.10131840
[23] CRYSTALS – Kyber: A CCA-Secure Module-Lattice-Based KEM / J. Bos [et al.] // 2018 IEEE European Symposium on Security and Privacy (EuroS&P). London, UK : IEEE Computer Society, 2018. P. 353-367. https://doi.org/10.1109/EuroSP.2018.00032
[24] The Ring-LWE Problem in Lattice-Based Cryptography: The Case of Twisted Embeddings / J. N. Ortiz [et al.] // Entropy. 2021. Vol. 23, issue 9. Article number: 1108. https://doi.org/10.3390/e23091108
[25] Yadav V. K., Verma S., Venkatesan S. An efficient and light weight polynomial multiplication for ideal lattice-based cryptography // Multimedia Tools and Applications. 2021. Vol. 80. P. 3089-3120. https://doi.org/10.1007/s11042-020-09706-8

Поступила 08.12.2023; одобрена после рецензирования 01.02.2024; принята к публикации 05.03.2024.

Об авторах:
Урбан Николай Алексеевич, магистрант кафедры информационных технологий, искусственного интеллекта и общественно-социальных технологий цифрового общества, ФГБОУ ВО «Российский государственный социальный университет» (129226, Российская Федерация, г. Москва, ул. Вильгельма Пика, д. 4, стр. 1), **ORCID: https://orcid.org/0000-0002-8047-1499,** urbannikolai@mail.ru
Мельникова Елена Анатольевна, доцент кафедры информационных технологий, искусственного интеллекта и общественно-социальных технологий цифрового общества, ФГБОУ ВО «Российский государственный социальный университет» (129226, Российская Федерация, г. Москва, ул. Вильгельма Пика, д. 4, стр. 1), кандидат физико-математических наук, доцент, **ORCID: https://orcid.org/0000-0003-1997-1846,** Ya.e.melnikova@yandex.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

References

[1] Mousa N., Shirazi F. A survey analysis of quantum computing adoption and the paradigm of privacy engineering. *Security and Privacy*. 2024;7(6):e419. https://doi.org/10.1002/spy2.419
[2] King A.D., et al. Quantum critical dynamics in a 5,000-qubit programmable spin glass. *Nature*. 2023;617:61-66. https://doi.org/10.1038/s41586-023-05867-2
[3] Kirichenko E.A. Quantum superiority as a threat to cybersecurity and post-quantum methods of cryptography. *IMSIT Bulletin*. 2021;(1):37-39. (In Russ., abstract in Eng.) EDN: KFKKBQ
[4] Lukashev A.V., et al. Quantum aspiration as a threat to information security. *International Journal of Information Technologies and Energy Efficiency.* 2023;8(6):97-101. (In Russ., abstract in Eng.) EDN: IQDQNH
[5] Nazarenko A.P., Dmitriev E.V. The current state of post-quantum cryptography in Russia and abroad. *Synchronization systems, signal generation and processing*. 2021;12(6):77-83. (In Russ., abstract in Eng.) EDN: FNKIVP

[6] Minbaleev A.V., Berestnev M.A., Evsikov K.S. Ensuring information security of mining industry equipment in the quantum era. *News of the Tula State University. Sciences of Earth.*. 2023;(1):567-584. (In Russ., abstract in Eng.) https://doi.org/10.46689/2218-5194-2023-1-1-567-584

[7] Dam D.-T., et al. A Survey of Post-Quantum Cryptography: Start of a New Race. *Cryptography.* 2023;7(3):40. https://doi.org/10.3390/cryptography7030040

[8] Malygina E.S., et al. Basic approaches to the construction of post-quantum cryptosystems: description, comparative characteristics. *Prikladnaya Diskretnaya Matematika. Supplement*. 2023;(16):58-65. (In Russ., abstract in Eng.) https://doi.org/10.17223/2226308X/16/16

[9] Kudryashov V.E., Fionov A.N. Problem of stability of modern cryptosystems against the background of the emergence of quantum computers. *Interexpo GEO-Siberia*. 2022;6:109-115. (In Russ., abstract in Eng.) https://doi.org/10.33764/2618-981X-2022-6-109-115

[10] Kurokawa T., et al. Selection Strategy of F4-Style Algorithm to Solve MQ Problems Related to MPKC. *Cryptography*. 2023;7(1):10. https://doi.org/10.3390/cryptography7010010

[11] Makarov A.O. Scheme of post-quantum aggregated signature with lazy verification based on multidimensional quadratic polynomials. *IT Security(Russia)*. 2023;30(3):30-50. (In Russ., abstract in Eng.) https://doi.org/10.26583/bit.2023.3.02

[12] Matveev G. Mathematical aspects of post-quantum cryptography. *Science and Innovation*. 2023;(8):52-56. (In Russ., abstract in Eng.) EDN: ELRJNN

[13] Bukovshin V.A., et al. Analysis of modern post-quantum encryption algorithms. *Scientific Review. Technical sciences.* 2019;(4):36-44. (In Russ., abstract in Eng.) EDN: VGXBXK

[14] Drzazga B., Krzywiecki Ł. Review of Chosen Isogeny-Based Cryptographic Schemes. *Cryptography*. 2022;6(2):27. https://doi.org/10.3390/cryptography6020027

[15] Bandara H., et al. On Advances of Lattice-Based Cryptographic Schemes and Their Implementations. *Cryptography.* 2022;6(4):56. https://doi.org/10.3390/cryptography6040056

[16] Nguyen T.-H., et al. A High-Efficiency Modular Multiplication Digital Signal Processing for Lattice-Based Post-Quantum Cryptography. *Cryptography*. 2023;7(4):46. https://doi.org/10.3390/cryptography7040046

[17] Camacho-Ruiz E., et al. Timing-Attack-Resistant Acceleration of NTRU Round 3 Encryption on Resource-Constrained Embedded Systems. *Cryptography*. 2023;7(2):29. https://doi.org/10.3390/cryptography7020029

[18] Orlov M.A., Nechaev K.A., Reznichenko S.A. Evaluation of statistical properties and cryptographic stability of random sequences obtained by an IBM quantum computer. *IT Security(Russia)*. 2023;30(1):14-26. (In Russ., abstract in Eng.) https://doi.org/10.26583/bit.2023.1.01

[19] Azman A.V., Rastamkhanov R.N., Tsukanov I.R. Authentication of the distribution of quantum keys using post-quantum cryptography. *Izvestiya Tula State University. Technical sciences.* 2023;(1):29-35. https://doi.org/10.24412/2071-6168-2023-1-29-35

[20] Chizhov I.V., Popova E.A. Structural Attack on Mceliece-Sidelnikov Type Public-Key Cryptosystem Based on a Combination of Random Codes with Reed-Muller Codes. *International Journal of Open Information Technologies.* 2020;8(6):24-33. (In Russ., abstract in Eng.) EDN: NOIJEL

[21] Sabani M.E., Savvas I.K., Poulakis D., Garani G., Makris G.C. Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era. *Electronics.* 2023;12(12):2643. https://doi.org/10.3390/electronics12122643

[22] Karakaya A., Ulu A. A Review on Latest Developments in Post-Quantum Based Secure Blockchain Systems. In: 2023 11th International Symposium on Digital Forensics and Security (ISDFS). Chattanooga, TN, USA: IEEE Computer Society; 2023. p. 1-6. https://doi.org/10.1109/ISDFS58141.2023.10131840

[23] Bos J., et al. CRYSTALS – Kyber: A CCA-Secure Module-Lattice-Based KEM. In: 2018 IEEE European Symposium on Security and Privacy (EuroS&P). London, UK: IEEE Computer Society; 2018. p. 353-367. https://doi.org/10.1109/EuroSP.2018.00032

[24] Ortiz J.N., de Araujo R.R., Aranha D.F., Costa S.I.R., Dahab R. The Ring-LWE Problem in Lattice-Based Cryptography: The Case of Twisted Embeddings. *Entropy.* 2021;23(9):1108. https://doi.org/10.3390/e23091108

[25] Yadav V.K., Verma S., Venkatesan, S. An efficient and light weight polynomial multiplication for ideal lattice-based cryptography. *Multimedia Tools and Applications*. 2021;80:3089-3120. https://doi.org/10.1007/s11042-020-09706-8

Submitted 08.12.2023; approved after reviewing 01.02.2024; accepted for publication 05.03.2024.

About the authors:

Nikolai A. Urban, Master degree student of the Chair of Information Technologies, Artificial Intelligence and Social Technologies of Digital Society, Russian State Social University (4 Wilhelma Pika St., building 1, Moscow 129226, Russian Federation), **ORCID: https://orcid.org/0000-0002-8047-1499,** urbannikolai@mail.ru

Elena A. Melnikova, Associate Professor of the Chair of Information Technologies, Artificial Intelligence and Social Technologies of Digital Society, Russian State Social University (4 Wilhelma Pika St., building 1, Moscow 129226, Russian Federation), Cand. Sci. (Phys.-Math.), Associate Professor, **ORCID: https://orcid.org/0000-0003-1997-1846,** Ya.e.melnikova@yandex.ru

All authors have read and approved the final manuscript.