CC BY

http://dx.doi.org/10.35596/1729-7648-2025-23-3-102-107

УДК 004.832.519.6

АЛГОРИТМ ШИФРОВАНИЯ ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ ДИСКРЕТНОЙ КВАНТОВОЙ КАРТЫ

А. В. СИДОРЕНКО, Е. А. ВЫСОЦКАЯ

Белорусский государственный университет (Минск, Республика Беларусь)

Аннотация. Разработан комплексный алгоритм шифрования на основе традиционных алгоритмов RSA (криптографический алгоритм с открытым ключом), SHA-3 (алгоритм хеширования переменной разрядности), а также дискретной квантовой карты. Описываются особенности предлагаемого алгоритма и разработанной компьютерной программы на языке C++. Для оценки работоспособности алгоритма было проведено тестирование на трех зашифрованных изображениях, различающихся объемом передаваемой информации. Сравнительный анализ полученных изображений с исходными показал эффективность алгоритма шифрования информации с применением дискретной квантовой карты. Также с помощью этого алгоритма можно выполнять дополнительные операции, связанные с включением информации внутрь зашифрованного изображения, что обеспечит дополнительный уровень защиты при передаче информации.

Ключевые слова: шифрование, алгоритм, дискретная квантовая карта.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Сидоренко, А. В. Алгоритм шифрования информации с применением дискретной квантовой карты / А. В. Сидоренко, Е. А. Высоцкая // Доклады БГУИР. 2025. Т. 23, № 3. С. 102–107. http://dx.doi.org/10.35596/1729-7648-2025-23-3-102-107.

INFORMATION ENCRYPTION ALGORITHM USING A DISCRETE QUANTUM MAP

ALEVTINA V. SIDORENKO, ELIZAVETA A. VYSOTSKAYA

Belarusian State University (Minsk, Republic of Belarus)

Abstract. A complex encryption algorithm has been developed based on traditional RSA (public key encryption algorithm), SHA-3 (hashing algorithm), and a discrete quantum map. The features of the proposed algorithm and the developed computer program in C++ are described. To evaluate the performance of the algorithm, testing was carried out on three encrypted images that differed in the volume of transmitted information. A comparative analysis of the obtained images with the original ones showed the efficiency of the information encryption algorithm using a discrete quantum map. This algorithm can also be used to perform additional operations related to including information inside the encrypted image, which will provide an additional level of protection when transmitting information.

Keywords: encryption, algorithm, discrete quantum map.

Conflict of interests. Authors declare no conflict of interests.

For citation. Sidorenko A. V., Vysotskaya E. A. (2025) Information Encryption Algorithm Using a Discrete Quantum Map. *Doklady BGUIR*. 23 (3), 102–107. http://dx.doi.org/10.35596/1729-7648-2025-23-3-102-107 (in Russian).

Введение

Интенсивное развитие информационных технологий, машинного обучения и искусственного интеллекта выдвигает на первый план вопросы, связанные с квантовой безопасностью. По мере расширения возможностей искусственного интеллекта растет число потенциальных уязвимостей, которыми могут воспользоваться злоумышленники [1, 2].

При эволюции квантовых компьютеров традиционные криптосистемы с публичным ключом и хеш-функции могут быть взломаны, и со временем их устойчивость снизится. Возникает необходимость обеспечения криптографической гибкости с помощью алгоритмов шифрования. Среди них – алгоритмы шифрования RSA (криптографический алгоритм с открытым ключом), ECDA (алгоритм с открытым ключом, использующийся для построения и проверки электронной цифровой подписи), SHA-3 (алгоритм хеширования переменной разрядности), SHA-256 (алгоритм криптографического хеширования), ECDH (протокол Диффи – Хеллмана на эллиптических кривых), DSA (алгоритм цифровой подписи). Даже на достаточно мощном квантовом компьютере конфиденциальная передача данных в перечисленных алгоритмах может быть нарушена алгоритмом Шора (квантовый алгоритм факторизации – разложение числа на простые множители) [3–7]. Следует отметить, что для ускорения генерации хеш-значений в системах с блокчейном квантовые алгоритмы могут использовать алгоритм Гровера (GSA, Grover Search Algorithm – квантовый алгоритм решения задачи перебора) [8]. GSA может быть адаптирован для детектирования хеш-коллизий и в то же время заменить блоки, формируемые в блокчейне, сохраняя интегрируемость передаваемой информации.

В статье представлен разработанный алгоритм шифрования и компьютерной программы на основе RSA, SHA-3 и дискретной квантовой карты. Выполнено тестирование программы с определением ее эффективности. Отмечены основные аспекты применения дискретной квантовой карты совместно с алгоритмами шифрования RSA и SHA-3 для обработки тестовых изображений.

Методы шифрования

Рассмотрим традиционные методы шифрования и шифрование с помощью дискретной квантовой карты. Так, RSA основан на задаче факторизации больших полупростых чисел. В алгоритме используются два ключа: открытый и закрытый. Открытый ключ известен всем, а закрытый хранится в секрете. Только авторизованные пользователи знают, как открыть сообщение. Размер блока, как правило, составляет 446 бит, а размер ключа – более 1024 бит. Для шифрования применяется только один цикл. В цикле шифрования используются три операции: генерация ключа, шифрование и расшифровка. Процесс генерации ключа состоит из следующих этапов.

1. Выбираются два случайных ключа заданного размера: p и q.

2. Вычисляется их произведение: $n = pq$.

3. Вычисляется значение функции Эйлера: $\varphi(n) = (p - 1)(q - 1)$.

4. Выбирается целое число e (простое), которое меньше значения функции Эйлера и является взаимно простым со значениями функции Эйлера, не имеющими общих делителей друг с другом, кроме 1: $1 < e < \varphi(n)$.

5. Вычисляется число d, обратное числу e по модулю $\varphi(n)$: $de \equiv 1(\mathrm{mod}\varphi(n))$.

6. После проведения вычислений получаем: (e, n) – открытый ключ; (d, n) – закрытый ключ [9].

Структурная схема алгоритма шифрования приведена на рис. 1. Для создания электронной подписи применяется алгоритм с использованием закрытого ключа DSA [10].

Дискретная квантовая карта представляет собой структуру элементов и способна обрабатывать данные, характеризущие квантовые процессы. На рис. 2 изображены стандартная и упрощенная двухкубитная схемы дискретной квантовой карты.

Квантовая карта состоит из квантового регистра памяти и квантового регистра данных [4]. В регистре памяти (рис. 2, *а*) находятся n_m кубит. Для ввода переменных в регистре памяти используется m_t кубит за время t. Регистр данных содержит в себе n_x кубит и используется для ввода памяти (скрытых переменных) x_t за время t.

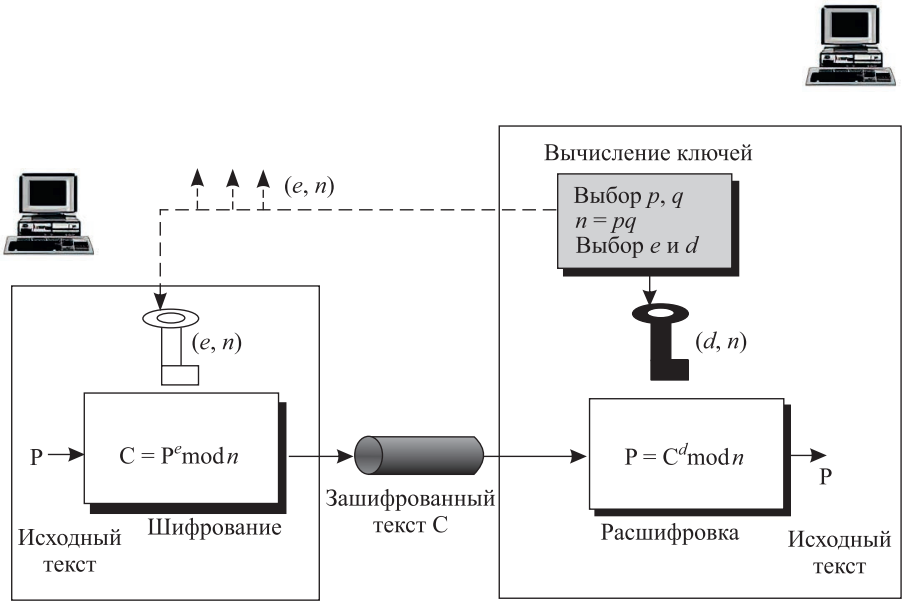


Рис. 1. Стандартная структура алгоритма RSA
Fig. 1. Standard structure of the RSA algorithm

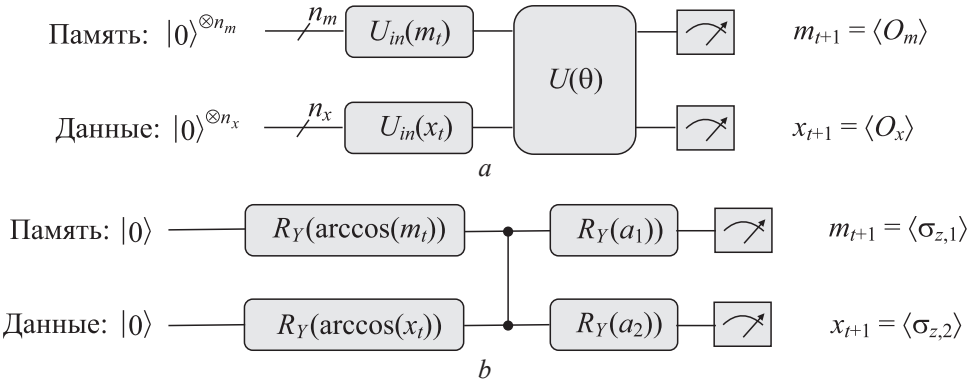


Рис. 2. Схема дискретной квантовой карты: *a* – стандартная; *b* – упрощенная двухкубитная
Fig. 2. Discrete quantum map diagram: *a* – standard; *b* – simplified two-qubit

Унитарный оператор $U(\theta)$ следует после слоя кодирования. Упрощенная двухкубитная схема (рис. 2, *b*) в регистре памяти использует функции $R_Y(\arccos(m_t))$ и $R_Y(\arccos(x_t))$ для кодирования, а также параметрические операторы $R_Y(a_1)$ и $R_Y(a_2)$. Следует отметить, что дискретная квантовая карта чувствительна к начальным условиям, то есть любое, даже небольшое, изменение в них приводит к образованию абсолютно различных текстовых последовательностей или изображений. Применение дискретной квантовой карты для шифрования позволяет обеспечить более высокий уровень безопасности благодаря квантовым свойствам карты. В частности, квантовые ключи, полученные с помощью карт, будут обладать такими параметрами, которые не позволят их копировать.

Процесс шифрования

Создание компьютерной программы включает в себя, прежде всего, разработку структурной схемы алгоритма для процесса шифрования (рис. 3). В схему включены блоки для выполнения дополнительных операций (например, перестановка значений используемой для шифрования последовательности, замена символов, перебор значений и т. д.) при подготовке и реализации процесса шифрования. Кроме того, в структурной схеме имеются блоки, реализующие алгоритмы SHA-3, RSA и дискретную квантовую карту. С их помощью получают зашифрованные данные. Поскольку шифрование в данном случае является обратимым процессом, расшифровка

происходит по той же схеме, но в обратном порядке. Зашифрованная последовательность снова подвергается процессу дополнительных операций, и на выходе получается расшифрованная исходная последовательность.

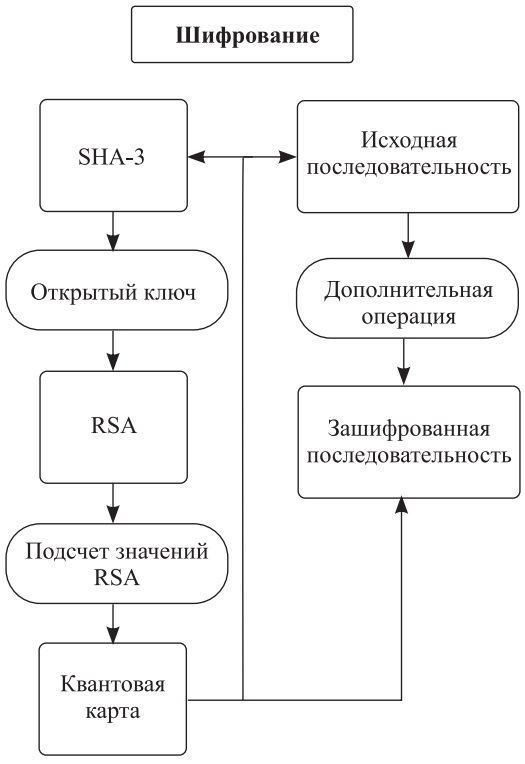


Рис. 3. Структурная схема алгоритма для процесса шифрования
Fig. 3. Block diagram of the algorithm for the encryption process

Реализация и тестирование разработанной компьютерной программы

Предлагаемая компьютерная программа разработана на языке C++. При этом дополнительные библиотеки не использовались. С помощью алгоритма SHA-3 получали хеш-значения информационной последовательности или изображения, которые в дальнейшем применялись для выполнения алгоритма RSA. После этого рассчитывались параметры для дискретной квантовой карты. При тестировании текстовой последовательности для создания ключей в разработанной программе использовали пять пар простых чисел. Результаты тестирования показали, что в случае применения алгоритма SHA-3 к анализируемой последовательности получаются 32 хеш-значения. Из этого ряда находили, что наилучшими параметрами среди простых чисел являются $p = 23$ и $q = 21$. Для создания открытого ключа использовали $e = 7$. Внедрение дискретной квантовой карты в разработанный алгоритм обеспечивало дополнительную защиту передаваемой зашифрованной последовательности или изображения. Последние позволили создать максимальную запутанность зашифрованных данных. Расширение возможностей для разработанной компьютерной программы продемонстрированы при шифровании трех тестовых изображений в формате .bmp (рис. 4).

Алгоритм работы компьютерной программы можно представить в виде выполнения следующих этапов.

1. Исходный файл изображения считывается в виде матрицы.

2. Матрица вводится в алгоритм SHA-3, на выходе которого получаются хеш-значения.

3. Хеш-значения вводятся в алгоритм RSA, где рассчитываются открытый и закрытый ключи, производятся шифрование и расшифровка переданной информации.

4. Рассчитанные ключи вводятся в дискретную квантовую карту, в которой осуществляется циклическая запутанность строк и столбцов матрицы. При этом нечетные строки смещаются влево, четные – вправо. Нечетные столбцы смещаются вверх, четные – вниз. Получается измененная матрица изображения.

a *b* *c*

Рис. 4. Тестовые изображения размерами, пиксель: *a* – 512×512; *b* – 256×256; *c* – 467×467
Fig. 4. Test images with dimensions, pixel: *a* – 512×512; *b* – 256×256; *c* – 467×467

5. Применение операции XOR (исключающее ИЛИ) к полученной матрице изменяет значения в ее строках и столбцах, что способствует большей запутанности и позволяет получить зашифрованное изображение.

6. Расшифровка повторяет этапы проведения зашифровки изображения в обратном порядке.

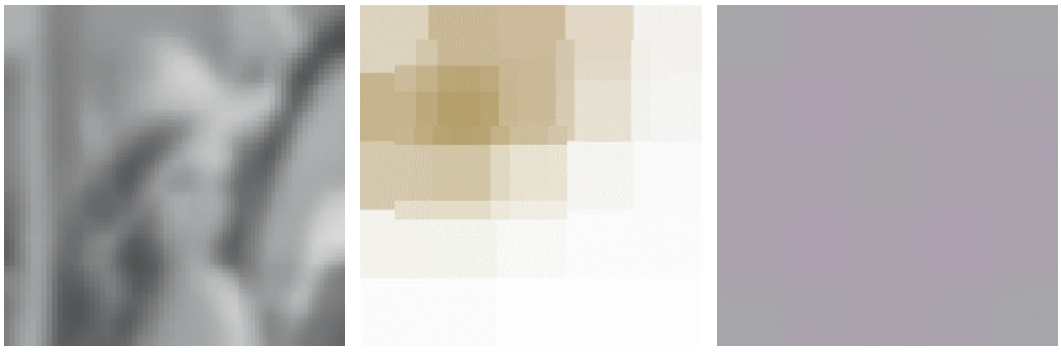
Результаты тестирования разработанной компьютерной программы с использованием тестовых изображений, приведенных на рис. 4, отражены в табл. 1.

Таблица 1. Результаты тестирования компьютерной программы на основе изображений на рис. 4
Table 1. Results of testing the computer program based on images in Fig. 4

Изображение на рис. 4	Размер, пиксель	Время, мс			Хеш-значение	Размер зашифрованных данных, Кб
		обработки матрицы	шифрования RSA	расшифровки RSA		
a	512×512	110	180	150	3a9f–7d8b	200
b	256×256	40	70	60	5f4a–9c2e	80
c	467×467	90	150	120	8c3d–b2f1	130

Как видно из табл. 1, время обработки матрицы передаваемого изображения увеличивается с ростом размера изображения, что связано с необходимостью обработки большего объема данных. Дискретная квантовая карта реализует процесс запутанности, необходимый при шифровании, а с помощью образованных алгоритмом ключей RSA изменяет порядок следования столбцов и строк изображения. Посредством алгоритма SHA-3 успешно получены хеш-значения для всех изображений с обеспечением целостности данных. Время зашифровки и расшифровки данных зависит от размеров передаваемого изображения и с их увеличением возрастает.

Зашифрованные изображения, полученные с использованием тестовых изображений на рис. 4, представлены на рис. 5. Сравнительный анализ тестовых и полученных изображений показал эффективнсть предложенного алгоритма.



a *b* *c*

Рис. 5. Зашифрованные изображения, соответствующие тестовым на рис. 4
Fig. 5. Encrypted images corresponding to the test images in Fig. 4

Заключение

1. Разработан комплексный алгоритм шифрования изображений на основе алгоритмов RSA (алгоритм шифрования с открытым ключом), SHA-3 (алгоритм хеширования) и дискретной квантовой карты. Предложенный алгоритм позволяет эффективно шифровать изображения, что подтверждает возможность сочетания традиционных методов шифрования и шифрования с использованием дискретной квантовой карты.

2. Алгоритм шифрования информации с применением дискретной квантовой карты позволит осуществлять дополнительные операции с изображениями (например, встраивать секретные изображения внутрь изначально зашифрованного). Это обеспечит дополнительный уровень защиты при передаче информации в виде изображений.

3. Работа выполнена в рамках Государственной программы научных исследований «Цифровые и космические технологии, безопасность общества и государства» (подпрограмма «Цифровые технологии и космическая информатика», задание 1.9.3.4).

Список литературы / References

1 Kiktenko E. O. (2018) Quantun Secured Blockchain. *ArXiv*. 3.
2 Bechzadan V. (2017) Vulnerability of Deep Reinforcement Learning to Policy. Induction Attacks. *ArXiv*.
3 Nai Sun Ping (2023) Quantum Discrete -Map. Based Recurrent Neural Networks. *University of Science and Technology of China*. (3), 1–11.
4 Guodong E., Kaivin J., Xiaoling H. (2021) Quantum Logistic Image Encryption Algorithm Based on SHA-3 and RSA. *Journal of Nonlinear Dynamics*. 104, 2807–2827.
5 Sidorenko A. V., Shishko M. S. (2020) Hashing Technical Algorithm Based on SHA-3 and Using Chaotic Maps. *Informatics*. 17 (1), 109–118 (in Russian).
6 Standard FIPS. 186-2. *Digital Signature Standard (DSS)*. 2000.
7 Grover L. A. (1996) First Quantum Mechanical Algorithm for Database Search. *Proc. of 28 Annual ACM Simposium on the Theory of Computing. Philadelphia. USA*. 212–219.
8 Shor P. W. (1992) Polynomial Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput*. 26, 1484–1509.
9 Calderbank H. (2007) *RCA Cryptosystem. History Algorithm. Primes*. Chicago, University of Chicago, Department of Mathematics. 1–7.
10 Jamak H. (2006) Digital Signature Algorithms. *Expert Conference Trends in the Development of Machinery and Associated Technology: 10th International Research*. 1–5.

Поступила 29.01.2025
Received: 29 January 2025

Принята в печать 11.04.2025
Accepted: 11 April 2025

Сведения об авторах

Сидоренко А. В., д-р техн. наук, проф., проф. каф. физики и аэрокосмических технологий, Белорусский государственный университет

Высоцкая Е. А., студент, Белорусский государственный университет

Адрес для корреспонденции

220030, Республика Беларусь,
Минск, просп. Независимости, 4
Белорусский государственный университет
Тел.: +375 29 339-14-30
E-mail: sidorenkoa@yandex.by
Сидоренко Алевтина Васильевна

Information about the authors

Sidorenko A. V., Dr. Sci. (Tech.), Professor, Professor at the Department of Physics and Aerospace Technology, Belarusian State University

Vysotskaya E. A., Student, Belarusian State University

Address for correspondence

220030, Republic of Belarus,
Minsk, Nezavisimosti Ave., 4
Belarusian State University
Tel.: +375 29 339-14-30
E-mail: sidorenkoa@yandex.by
Sidorenko Alevtina Vasilevna