УДК 004.056.55
DOI 10.33764/2618-981X-2022-6-109-115

Проблема устойчивости современных криптосистем на фоне появления квантовых компьютеров

В. Е. Кудряшов[1]*, *А. Н. Фионов*[1]
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: vadkud@inbox.ru

Аннотация. С каждым годом производство квантовых компьютеров становится все более продуктивным и дешевым, например, компьютер «Цучунцзы» использует 56 кубитов и способен решать проблемы, ставящие на первый план возможность квантового ускорения в течение нескольких часов, в то время как классические суперкомпьютеры требуют десятки тысяч лет. В настоящее время IBM дает возможность любому пользователю сети Интернет удаленно подключиться и поработать на реальном квантовом компьютере с мощностью в несколько кубитов. Современная криптография основана на том, что классическими алгоритмами трудно провести факторизацию целых чисел или дискретное логарифмирование. Но с применением алгоритма Шора на квантовом компьютере эти трудности легко обходятся. Некоторые из самых популярных криптографических систем - RSA (факторизация целых чисел), DH (дискретное логарифмирование) и ECDSA (эллиптические кривые над конечными полями) – с появлением продуктивных квантовых компьютеров больше не станут надежным инструментом для шифрования данных. В данной статье изучены постквантовые криптографические системы и проведено сравнение их с классической системой RSA.

Ключевые слова: шифрование, RSA, Мак-Элис, квантовый компьютер, NTPUEncrypt, постквановая криптография

Problem of stability of modern cryptosystems against the background of the emergence of quantum computers

V. E. Kudryashov[1]*, *A. N. Fionov*[1]
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: vadkud@inbox.ru

Abstract. Every year, the production of quantum computers is becoming more productive and cheaper - for example, “The Tsuchongzi” computer uses 56 qubits and is able to solve problems that highlight the possibility of quantum acceleration within a few hours, while classical supercomputers require tens of thousands of years. Currently, IBM allows any Internet user to remotely connect and work on a real quantum computer, albeit with a power of several qubits. Modern cryptography is based on the fact that it is difficult to carry out factorization of integers or discrete logarithm by classical algorithms. But with the use of Shor's algorithm on a quantum computer, these difficulties are easily bypassed. Some of the most popular cryptographic systems - RSA (integer factorization), DH (discrete logarithm), and ECDSA (elliptic curves over finite fields) - will no longer be a reliable tool for data encryption with the advent of productive quantum computers. In this article, post-quantum cryptographic systems are studied and compared with the classical RSA system.

Keywords: encryption, RSA, McEliece, quantum computer, NTPUEncrypt, post-quantum cryptography

Введение

В настоящее время безопасность информации зависит от защищенности современных криптосистем от различных векторов атак. Учитывая тот факт, что в области квантовой криптографии в последние годы замечается стремительный рост количества исследовательких работ, можно предположить, что появление реальных квантовых компьютеров уже не за горами. Такие компьютеры значительно превосходят по скорости обработки сложных операций обычные устройства за счет использования кубита (бит, который может одновременно принимать два значения). Благодаря этому свойству операции факторизации целых чисел или дискретного логарифмирования легко решаются с использованием алгоритма Шора [1]. А значит современные криптосистемы, использующие в своей работе перечисленные операции, становятся потенциально уязвимыми. Поэтому сейчас криптографами отдается приоритет разработке алгоритмов, которые не зависят от квантовых вычислений, а значит устойчивы к квантовым атакам. Криптография, которая учитывает возможности квантовых компьютеров, называется постквантовой [2].

Алгоритмы, основанные на алгебраических задачах факторизации целых чисел и дискретного логарифмирования [3]:

- распределение ключей (ECDH, DH);
- асимметричное шифрование (RSA);
- электронная подпись (ECDSA, DSA, ГОСТ Р 34.10-2012).

В настоящий момент исследования в этой области сосредоточены на шести основных подходах [4]:

– криптография, основанная на хеш-функциях;
– криптография, основанная на кодах исправления ошибок;
– криптография, основанная на решётках;
– криптография, основанная на многомерных квадратичных системах;
– шифрование с секретным сключом;
– шифрование с использованием суперсингулярной изогении.

Цель исследования: анализ существующих методов постквантовой криптографии.

Для достижения поставленной цели необходимо решить следующие задачи:

– анализ проблематики выбранной темы;
– сбор информации по методам современной и постквантовой криптографии и выбор трех из них для сравнения;
– сравнительный анализ выбранных криптосистем;
– выводы.

Были изучены такие методы постквантовой криптографи, как криптография, основанная на кодах исправления ошибок (система Мак-Элиса) и криптография, основанная на решетках (система NTRUEncrypt). На основе этих методов ученым удалось разработать множетсво криптосистем, например, систему Мак-Элиса или систему NTRUEncrypt. Сравнили эти системы с классическим RSA, чтобы понять, сущетствуют ли уже алгоритмы, способные обеспечить безопасность информации в постквантовом мире [5].

Криптография, основанная на кодах исправления ошибок (криптосистема Мак-Элиса) – подход к построению алгоритмов, стойкость которых основывается на предположении о вычислительной сложности задачи декодирования случайного линейного кода.

Криптосистема Мак-Элиса – система, разработанная Робертом Мак-Элисом в 1978 г. В шифровании используется пара открытого и закрытого ключа, а сама логика работы основана на кодах с исправлением ошибок. Роберт Мак-Элис был первым, кто использовал процесс рандомизации при шифровании [6].

Криптография, основанная на решетках – подход к построению алгоритмов асимметричного шифрования с использованием задач теории решёток, то есть задач оптимизации на дискретных аддитивных подгруппах.

Вместе с другими методами постквантовой криптографии она считается перспективной из-за способности квантового компьютера расшифровывать широко используемые системы асимметричной криптографии, основанные на двух типах задач теории чисел: задачах целочисленной факторизации и задачах дискретного логарифмирования. Сложность алгоритмов взлома, построенных на решетках, чрезвычайно высока, лучшие алгоритмы могут решить эту задачу с трудом за экспоненциальное время [7].

Постквантовая криптография на решётках основана на неосуществимых как для квантовых, так и для классических компьютеров задачах на решётках, таких как:

- нахождение кратчайшего вектора;
- нахождение идеального кратчайшего вектора;
- нахождение кратчайшего независимого вектора;
- поиск короткого целого решения.

Методы и материалы

Рассмотрим подробнее алгоритмы генерации ключей, шифрования и дешифрования в криптосистеме Мак-Элиса.

Алгоритм генерации ключей заключается в следующем.

1. Берется G – порождающая матрица размера (k, n) (n,k) линейного кода, исправляющего t ошибок.

2. Берется случайная невырожденная матрица S размера (k, k).

3. Берется случайная матрица перестановки P размера (n, n).

4. Публичный ключ – пара (SGP, t), где

$$SGP = G',$$

где G – начальная порождающая матрица.

5. Приватный ключ – тройка (S, G, P).

Алгоритм шифрования заключается в следующем.

1. Берется случайный вектор ошибки m длины n и веса w не больше t.

2. Шифротекст с получается по формуле:

$$c = mG' + e,$$

где m – взятый случайный вектор; G' – транспонированная порождающая матрица G; e – случайное слово (ошибочное).

Алгоритм дешифрования заключается в следующем.

1. Рассчитывается c' по формуле:

$$c' = cP^{-1},$$

где c – шифротекст; P^{-1} – обратная случайной матрице перестановки P.

2. Находится m' с помощью алгоритма Питерсона.

3. Находится исходный текст m по формуле:

$$m = m'S^{-1},$$

где m' – искомая величина из п.2; S^{-1} – обратная случайной невырожденной матрице S.

Далее рассмотрим алгоритмы генерации ключей, шифрования и дешифрования в криптосистеме NTRUEncrypt (основана на решетках).

Алгоритм генерации ключа заключается в следующем.

1. Задается 6 параметров: N, p, q, d, d_f, d_g.

2. Определяются наборы многочленов по формулам:

$$L_f = L(d_f, d_f - 1),$$

$$L_g = L(d_g, d_g),$$

$$L_r = L(d, d).$$

3. Из набора L_f выбирается произвольный многочлен $f(x)$.

4. Из набора L_f выбирается многочлен $g(x)$.

5. Вычисляются многочлены $f_q(x)$, $f_p(x)$, удовлетворяющие формулам:

$$f_p(x) * f(x) = 1 \bmod p,$$

$$f_q(x) * f(x) = 1 \bmod q.$$

6. Открытый ключ h(x) определяется по формуле:

$$h(x) = f_q(x) * g(x) \bmod q .$$

7. Секретный ключ – это пара *(f(x), f_p(x))*.

Алгоритм шифрования заключается в следующем.

1. Боб выбирает сообщение m и преобразует его в многочлен по формуле:

$$M(x) \in L_m ,$$

где L_m – множество многочленов (вводится пользователем).

2. Боб выбирает так называемый «ослепляющий» многочлен $r(x) \in L_r$ и вычисляет шифротекст *C(x)* по формуле:

$$C(x) = p * r(x) * h(x) + M(x) \bmod q ,$$

где *p, q* – заданные параметры системы; *r(x)* – «ослепляющий» многочлен; *h(x)* – открытый ключ; *M(x)* – преобразованное сообщение m.

Алгоритм дешифрования заключается в следующем [8].

1. Получив от Боба шифротекст *C(x)*, Алиса вычисляет *a(x)* по формуле:

$$a(x) = f(x) * C(x) \bmod q, a(x) \in (-\frac{q}{2}; \frac{q}{2}],$$

где *f(x)* – произвольный многочлен из набора L_f.

2. Алиса вычисляет *b(x)* по формуле:

$$b(x) = a(x) \bmod p .$$

3. Алиса восстанавливает исходное сообщение *M* по формуле:

$$M = b(x) * f_p(x) \bmod p .$$

Результаты

В табл. 1 представлено сравнение постквантовых систем и классической RSA.

Таблица 1

Сравнение постквантовых систем и RSA

Параметр сравнения	Система Мак-Элиса (n=2048, k=1718, t=30)	Система NTPUEncrypt (n=503, p=2, q=253)	Система RSA (e = 2^{16}+1)
Скорость шифрования	1025 мс	2320,63 мс	4555 мс
Скорость дешифрования	2311	8450 мс	6557176,5
Размер открытого ключа	429,5 Кбайт	69,2 Кбайт	0,5 Кбайт
Размер файла с шифротекстом относительно размера файла с начальным текстом	Больше	Равен	Равен

Криптостойкость к атакам алгоритмом Шора	+	+	-

После создания достаточно мощных квантовых компьютеров алгоритм RSA станет бесполезным, так как он основывается на операции дискретизации целых чисел. Однако такие системы, как система Мак-Элиса и NTPUEncrypt, сохранят свою криптостойкость и в постквантовом мире, так как на данные момент не существует алгоритмов, решающих, например, задачи кратчайшего вектора решетки. Они ничуть не уступают ни в скорости работы (работают даже быстрее), ни в удобстве использования.

К недостаткам системы Мак-Элиса можно отнести больший размер шифротекста и очень большой размер открытого ключа (больше в 1000 раз, чем у RSA).

К недостаткам системы NTPUEncrypt можно отнести большой размер открытого ключа (больше в 70 раз, чем у RSA) и необходимость использования рекомендуемых разработчиками входных параметров для обеспечения должной криптостойкости.

Основные недостатки постквантовых криптосистем (большой размер ключа) связаны с повышением уровня их криптостойкости. Поэтому сейчас их не используют.

Исследовательская группа постквантовой криптографии, спонсируемая Европейской комиссией, рекомендовала систему шифрования с открытым ключом Мак-Элиса в качестве кандидата для долгосрочной защиты от атак квантовых компьютеров [9].

Заключение

Стоимость создания квантовых сетей хотя бы на 50 пользователей оценивается в несколько миллионов долларов, а о квантовом общедоступном Интернете говорить и вовсе рано. Однако в ближайшие несколько лет вычислительная мощность квантовых компьютеров может достичь уровней, достаточных для того, чтобы представлять угрозу для современных криптосистем, основанные задачах факторизации целых чисел и задачах дискретного логарифмирования. В связи с этим возникает необходимость изучения методов постквантовой криптографии. Сложность взлома алгоритмов, например, построенных на решетках, крайне велика, самые лучшие алгоритмы могут решить эту задачу с трудом за экспоненциальное время [10].

На данный момент уже существуют постквантовые системы, которые не уступают в скорости и удобстве использования классическим системам криптографической защиты (например, RSA). Единственным недостатком таких систем является большой размер открытого ключа, но это и объясняется их криптостойкостью в постквантовом мире. Поэтому уже сейчас стоит изучать алгоритмы постквантового шифрования данных и заменять ими классические системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Дрон К.К. О перспективах совместного использования методов квантовой и классической криптографии. // Вестник Хакасского государственного университета им НФ Катанова. – 2018. – № 24. – С. 8-11.

2. Горев А. И., Симаков, А. А. Обеспечение Информационной Безопасности. – Москва: Мир, 2005. – 844 с.

3. Осмоловский, С. А. Стохастическая информатика. Инновации в информационных системах. – Москва: Горячая линия, 2012. – 322 с.

4. Буковшин В.А., Чуб П.А., Черкесова Л.В., Короченцев Д.А., Поркшеян В.М. Анализ современных пост-квантовых алгоритмов шифрования. – Научное обозрение №4: Технические науки, 2005. – 128 с.

5. Бабенко Л. К. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2006. – 376 с.

6. Адаменко М. Основы классической криптологии. Секреты шифров и кодов. – Москва: Машиностроение, 2014. – 256 с.

7. Авдошин С. Дискретная математика. Модулярная алгебра, криптография, кодирование. – Москва: СИНТЕГ, 2016. – 260 с.

8. Кузьмин Т. В. Криптографические методы защиты информации. – Москва: Огни, 2013. – 192 с.

9. Молдовян Д. Н. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // CyberLeninka: Научная электронная библиотека. — URL: https://cyberleninka.ru/article/n/novaya-kontseptsiya-razrabotki-postkvantovyh-algoritmov-tsifrovoy-podpisi-na-nekommutativnyh-algebrah/viewer (дата обращения: 10.05.2022).

10. Зубов А.Н. Математика кодов аутентификации. – М.: Гелиос АРВ, 2014. – 319 с.