УДК 004.056

ПОСТКВАНТОВЫЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПОВЫШЕНИЯ СТОЙКОСТИ ШИФРОВ

М.А. Солонович, А.А. Игнатенко
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В данной статье рассмотрены угрозы классическим криптографическим алгоритмам, которые представляют квантовые компьютеры. Обсуждаются симметричное и асимметричное шифрование. Описание алгоритмов Шора и Гровера. Использование искусственного интеллекта в повышении стойкости шифров: автоматизированный криптоанализ решеток и кодов, оптимизация параметров и генерация новых схем.
Ключевые слова: Криптография; квантовые компьютеры; постквантовые алгоритмы; алгоритм Шора; алгоритм Гровера; RSA; симметричное шифрование; асимметричное шифрование; искусственный интеллект; криптоанализ.

POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS AND THE APPLICATION OF ARTIFICIAL INTELLIGENCE TO ENHANCE THE STRENGTH OF CIPHERS

M.A. Solonovich, A.A. Ignatenko
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. This article examines the threats to classical cryptographic algorithms posed by quantum computers. Symmetric and asymmetric encryption are discussed. Shor's and Grover's algorithms are described. The use of artificial intelligence in increasing the security of ciphers: automated cryptanalysis of lattices and codes, parameter optimization, and the generation of new schemes.
Keywords: Cryptography; quantum computers; post-quantum algorithms; Shor's algorithm; Grover's algorithm; RSA; symmetric encryption; asymmetric encryption; artificial intelligence; cryptanalysis.

Введение

Криптография – это наука о защите информации путем преобразования исходных данных в шифр, обеспечивая конфиденциальность, целостность и аутентичность. Появление квантовых компьютеров создает угрозу классическим алгоритмам криптографии, основанным на факторизации числа и дискретном логарифмировании. Параллельно развитие искусственного интеллекта предоставляет как инструменты для атак, так и средства для проектирования стойких

постквантовых схем. Рассматриваются постквантовые криптографические алгоритмы и роль искусственного интеллекта в их разработке.

Основная часть

Криптография – это наука о защите информации путем преобразования исходных данных в шифр, обеспечивая конфиденциальность, целостность и аутентичность. В общем случае криптографическое преобразование позволяет преобразовать открытый текст в шифротекст при помощи некоторого алгоритма и секретного ключа.

Симметричный алгоритм шифрования - для шифровки и расшифровки используется одинаковый ключ.

Асимметричный алгоритм шифрования – для шифровки и расшифровки используются разные ключи: открытый ключ для шифрования, закрытый ключ для дешифровки.

В настоящее время криптография опирается на вычислительную сложность решения подбора ключей для расшифровки. Безопасность большинства асимметричных алгоритмов строится на том, что операции по созданию ключа выполнить легко, а для подбора ключа это будет крайне сложная задача. Например, произведение двух больших простых чисел n и q требует полиномиального времени, в то время как факторизация результирующего модуля имеет экспоненциальную сложность. На этой идее строится алгоритм шифрования RSA.

RSA относится к асимметричным алгоритмам шифрования, для шифрования информации используется открытый ключ, а для дешифровки используется закрытый ключ.

Вся безопасность данного алгоритма опирается на вычислительную сложность. Задача стоит только в том, чтобы разложить большое произведение на простые множители. И эта сложность актуальна только для обычных компьютеров.

Однако квантовые компьютеры при применении своих алгоритмов способны кардинально изменить ситуацию. Одним из них является Алгоритм Шора предназначен для факторизации целых чисел, позволяющий разложить число n на простые множители за $O(\log^3 n)$ операций, используя $O(\log n)$ кубитов.

Для атаки на симметричную криптографию используют алгоритм Гровера. В исходной постановке он позволяет отыскать в неупорядоченном списке из N элементов присутствующий в единственном экземпляре элемент с отличительным свойством за $O(\sqrt{N})$ шагов – итераций Гровера. Алгоритм Гровера может быть использован для ускорения атаки полным перебором.

В настоящее время на международном уровне ведется стандартизация постквантовых алгоритмов на решетках (Kyber), кодах (McEliece), хэшах (SPHINCS+), устойчивых к Шору/Гроверу. Злоумышленники уже реализуют стратегию «собери сейчас – расшифруй потом», накапливая зашифрованные данные для будущих квантовых атак.

На этом фоне особое значение приобретает применение методов искусственного интеллекта в постквантовой криптографии. Искусственный интеллект сильно ускоряет развитие постквантовой криптографии, беря на себя решение задач, ранее требовавших десятилетий ручного труда.

Нейронные сети анализируют сложные структуры решеток LWE и кодов McEliece, мгновенно выявляя критические уязвимости – короткие векторы или эквивалентные коды, на поиск которых у экспертов уходили месяцы. методы машинного обучения оптимизируют параметры алгоритмов. Генетические алгоритмы и градиентный спуск подбирают оптимальные значения q и β для Kyber и NTRU, обеспечивая минимальный размер ключей при сохранении требуемой стойкости против квантовых атак. Эволюционные алгоритмы и генеративно-состязательные сети (GAN) создают и тестируют модификации SPHINCS+ и Ring-LWE, автоматически проверяя устойчивость к алгоритмам Шора и Гровера.

Заключение

Существующие сегодня и повсеместно применяемые асимметричные алгоритмы уязвимы к квантовым атакам. Стоит отметить, что симметричные остаются частично стойкими при условии увеличения длины ключа. Постквантовая криптография предлагает новые математические основы. Искусственный интеллект полезен в постквантовой криптографии: он помогает автоматизировать и улучшать разработку постквантовых алгоритмов.

Список использованных источников

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие. – 2-е изд., испр. и доп. – М.: Гелиос АРВ, 2002. – 480 с.

2. Малыгина Е. С., Куценко А. В., Новоселов С. А., Колесников Н. С., Бахарев А. О., Хильчук И. С., Шапоренко А. С., Токарева Н. Н. Постквантовые криптосистемы: открытые вопросы и существующие решения. Криптосистемы на решетках // Дискретный анализ и исследование операций. – 2023. – Т. 30, № 4. – С. 46–90. – DOI: 10.33048/daio.2023.30.771.

References

1. Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V. Osnovy kriptografii [Fundamentals of cryptography]. 2nd ed. Moscow: Gelios ARV, 2002. 480 p. (In Russ.).

2. Malygina E. S., Kutsenko A. V., Novoselov S. A., Kolesnikov N. S., Bakharev A. O., Khilchuk I. S., Shaporenko A. S., Tokareva N. N. Post-quantum cryptosystems: open questions and existing solutions. Lattice-based cryptosystems. *Diskretnyi analiz i issledovanie operatsii* [Discrete Analysis and Operations Research], 2023, vol. 30, no. 4, pp. 46-90. (In Russ.) DOI: 10.33048/daio.2023.30.771.

Сведения об авторах

Солонович М.А., курсант, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», maxnest77max@icloud.com.

Игнатенко А.А. магистр, преподаватель, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», a.ignatenko@bsuir.by.

Information about the authors

Solonovich M.A., Cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", maxnest77max@icloud.com.

Ignatenko A.A., Master, lecturer, Educational Institution "Belarusian State University of Informatics and Radioelectronics", a.ignatenko@bsuir.by.