УДК 004.056.55

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ: ПОЧЕМУ НАМ ПОРА МЕНЯТЬ МЕТОДЫ ЗАЩИТЫ

Д.С. Таран, В.А. Федоренко
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье обсуждается, как развитие квантовых компьютеров ставит под удар привычную защиту данных. Старые алгоритмы (RSA, ECC), на которых держится почти весь интернет, скоро могут стать бесполезными из-за алгоритма Шора. Автор объясняет, почему нужно переходить на «постквантовые» методы защиты уже сейчас, и рассматривает один из самых крутых вариантов – криптографию на решетках. Также даются простые советы, как начать внедрять новую защиту в реальные системы.
Ключевые слова: криптография; квантовый компьютер; защита информации; шифрование; постквантовые алгоритмы; решетки; цифровая подпись; информационная безопасность; хакеры; алгоритм Шора.

POST-QUANTUM CRYPTOGRAPHY: WHY IT'S TIME TO CHANGE PROTECTION METHODS

D.S. Taran, V.A. Fedorenko,
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The article discusses how the development of quantum computers threatens traditional data protection. Old algorithms (RSA, ECC), which support almost the entire

Internet, may soon become useless due to Shor's algorithm. The author explains why it is necessary to switch to "post-quantum" protection methods now and considers one of the coolest options – lattice-based cryptography. Simple tips are also given on how to start implementing new protection into real systems.
Keywords: cryptography; quantum computer; information security; encryption; post-quantum algorithms; lattices; digital signature; information security; hackers; Shor's algorithm.

Введение

Сегодня вся наша безопасность в сети – пароли, банковские карты, переписки – держится на криптографии. Мы привыкли думать, что это надежно, потому что обычному компьютеру нужны тысячи лет, чтобы подобрать ключ. Но скоро все изменится. Появляются квантовые компьютеры. Для них наши сложные математические задачи – это пустяк. Если мы не хотим, чтобы в один день все секреты мира были раскрыты, нам нужно срочно придумывать новые способы защиты – постквантовую криптографию.

Основная часть

Главная проблема в том, что квантовые компьютеры работают по другим законам физики. С помощью алгоритма Шора они могут мгновенно разламывать современные цифровые замки.

Что с этим делать? Математики предлагают использовать задачи, которые не под силу даже квантовому компьютеру. Самый перспективный вариант – это криптография на решетках.

Если говорить просто, то мы прячем секрет в огромной многомерной паутине из точек. Чтобы найти правильную точку, нужно решить уравнение:

$$As + e = b, \tag{1}$$

где A – матрица, s – секретный вектор, e – ошибка, b – правильная точка

В этой формуле вектор e играет роль намеренно внесенного шума. Даже небольшое отклонение делает невозможным использование стандартных методов решения линейных уравнений. Чтобы взломать такую защиту, злоумышленнику пришлось бы найти кратчайший вектор в многомерной решетке, что является NP-трудной задачей.

Помимо решеток, рассматриваются и другие методы защиты: криптография на основе хеш-функций, кодовая криптография.

Криптография на основе хеш-функций использует деревья Меркла для создания цифровых подписей. Стойкость здесь зависит только от надежности самой хеш-функции, а не от сложности теоретико-числовых задач. Это делает такие системы очень предсказуемыми и безопасными.

Кодовая криптография основана на использовании кодов, исправляющих ошибки (например, схема Мак-Элиса). Сообщение маскируется под случайный набор данных, и только владелец секретного ключа знает, как «исправить» этот шум и прочитать исходный текст.

В настоящее время Национальный институт стандартов и технологий (*NIST*) уже завершает отбор алгоритмов, которые станут мировыми стандартами. Фаворитами выступают такие системы, как *CRYSTALS-Kyber* (для шифрования) и *CRYSTALS-Dilithium* (для цифровых подписей).

Переход на постквантовую защиту осложняется несколькими факторами. Во-первых, это размер ключей. Если классический ключ *RSA* может занимать 256–512 байт, то постквантовые ключи часто исчисляются килобайтами. Это создает дополнительную нагрузку на сетевые протоколы, такие как *TLS*, используемые при просмотре веб-страниц.

Во-вторых, возникает вопрос производительности. Постквантовые алгоритмы требуют больше оперативной памяти и ресурсов процессора. Это особенно критично для устройств интернета вещей (*IoT*) и мобильных гаджетов с ограниченным энергопотреблением.

Учитывая риски, эксперты предлагают использовать гибридный подход. Суть его в том, что данные шифруются одновременно двумя способами: старым (классическим) и новым (постквантовым). Если один из методов будет взломан, данные все равно останутся защищены вторым слоем. Это позволяет плавно внедрять новые технологии, не отказываясь от проверенных десятилетиями стандартов, пока квантовые компьютеры не стали массовой реальностью.

Заключение

Квантовая угроза – это не сюжет из кино, а реальность ближайших лет. Чтобы не остаться беззащитными, нужно уже сейчас тестировать гибридные системы (старая защита + новая). Это позволит плавно перейти на новые стандарты безопасности и не бояться появления мощных квантовых вычислителей.

Список использованных источников

1. Alagic, G. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process / G. Alagic [et al.] // NIST Internal Report 8413. – 2022. – 54 p.

2. Алферов, А. П. Основы криптографии : учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – Москва : Гелиос АРВ, 2005. – 480 с.

References

1. Alagic, G. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process / G. Alagic [et al.] // NIST Internal Report 8413. – 2022. – 54 p.

2. Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V. (2005) Fundamentals of Cryptography: Tutorial. Moscow, Helios ARV (in Russian).

Сведения об авторах

Таран Д.С., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ulefol58@gmail.com

Федоренко В.А., начальник цикла кафедры связи, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», v.fedorenko@bsuir.by

Information about the authors

Taran D.S., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", ulefol58@gmail.com

Fedorenko V.A., Head of the cycle of the Department of Communications, Educational Institution "Belarusian State University of Informatics and Radioelectronics", v.fedorenko@bsuir.by