ОБЗОР И КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННЫМ СИСТЕМАМ СО СТОРОНЫ КВАНТОВЫХ АЛГОРИТМОВ

Крупенич Е. Г., Вергель И. В.
Кафедра программного обеспечения информационных технологий, Факультет компьютерных систем и сетей,
Центр информатизации и инновационных разработок,
Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: {s.nesterenkov, e.krupenich, i.vergel}@bsuir.by

В статье рассматриваются квантовые алгоритмы, представляющие угрозу современным криптографическим системам. Среди них особое место занимают алгоритм Шора, позволяющий эффективно решать задачу факторизации целых чисел и вычисления дискретного логарифма, и алгоритм Гровера, обеспечивающий квадратичное ускорение поиска в неструктурированных массивах данных. Также предложен один из возможных вариантов классификации квантовых угроз по типу криптографического примитива, характеру воздействия, горизонту актуализации и степени критичности для инфраструктуры.

Введение

Квантовый алгоритм представляет собой классический алгоритм, который задает последовательность унитарных операций с указанием, над какими именно кубитами их надо совершать. Результат работы квантового алгоритма носит вероятностный характер. За счёт небольшого увеличения количества операций в алгоритме можно сколь угодно приблизить вероятность получения правильного результата к единице. Множества задач, допускающих решение на квантовом компьютере и на классическом, совпадают. Квантовый компьютер, таким образом, не увеличивает число алгоритмически разрешимых задач. Весь смысл применения квантового компьютера в том, что некоторые задачи он способен решить существенно быстрее, чем любой из классических.

I. Квантовые угрозы

ддВ последние годы появились конкретные алгоритмы, представляющие угрозу существующим средствам защиты информации. Наибольшую известность получили алгоритм Шора, подрывающий безопасность асимметричных криптосистем, и алгоритм Гровера, снижающий стойкость симметричных шифров и хэш-функций. Кроме того, в практику входят атаки типа «собери сейчас – расшифруй потом», что делает проблему ещё более актуальной. Подобные угрозы приобретают стратегический характер, поскольку затрагивают критическую инфраструктуру, системы электронных платежей, защищённые каналы связи и цифровые подписи.

II. Алгоритм Шора

Алгоритм Шора – это алгоритм разложения числа на простые множители, позволяющий разложить число M за $O(log^3 N)$, используя $O(\log N)$ логических кубитов. Его применение представляет угрозу для криптографических систем с открытым ключом, безопасность которых основана на сложности задач факторизации и вычисления дискретного логарифма. К таким системам относятся широко используемые алгоритмы RSA, Diffie–Hellman и криптография на эллиптических кривых (ECC). Именно они лежат в основе протоколов TLS/SSL, VPN, цифровых подписей и инфраструктуры открытых ключей (PKI). При этом другие классы асимметричных алгоритмов, использующие иные математические основы (например, решётки или кодовые конструкции), не подвержены воздействию алгоритма Шора.

Алгоритм Шора сводит задачу факторизации числа к задаче нахождения периода (порядка) функции.

1. Выбираем случайное число a, где $1 < a < N$.
2. Вычисляем $R = gcd(a,N)$.
   - Если K, то это нетривиальный делитель числа $N \neq 1$, а второй равен N/K. Алгоритм завершен.
3. Иначе используем квантовую подпрограмму, чтобы найти порядок r числа a.

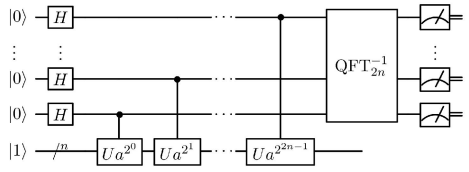

Рис. 1 – Квантовая подпрограмма в алгоритме Шора

4. Если r нечетное, возвращаемся к шагу 1.
5. Вычисляем $g = gcd(N,a^{r/2}+1)$
   - Если g нетривиален, то другой делитель равен N/g. Алгоритм завершен.
   - Иначе возвращаемся к шагу 1.

Алгоритм с высокой вероятностью успешно разложит N на множители после первого вызова квантовой подпрограммы, хотя теоретически может потребоваться несколько повторов.

III. Алгоритм Гровера

Алгоритм Гровера – это квантовый алгоритм поиска, позволяющий найти искомый элемент в неструктурированной базе данных из N элементов за $O(\sqrt{N})$ шагов вместо $O(N)$, требуемых классическим перебором. Для его реализации необходимо $O(\log N)$ кубитов. С его помощью становится возможным ускоренный перебор ключей и поиск предобразов для хэш-функций, что снижает криптостойкость симметричных алгоритмов шифрования и функций хэширования. В первую очередь под угрозой оказываются такие алгоритмы, как AES и SHA-2/SHA-3, что может привести к компрометации систем аутентификации и целостности данных.

Алгоритм Гровера основан на многократном применении так называемого оператора инверсии амплитуды, который усиливает вероятность правильного ответа:

1. Инициализируем систему до равномерной суперпозиции по всем состояниям.

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

2. Применяем оператор U_ω.
3. Измерь полученное квантовое состояние в вычислительном базисе.

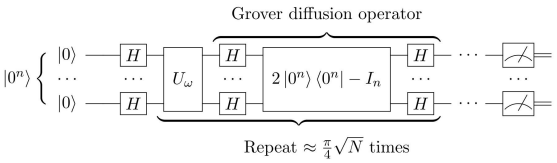

Рис. 2 – Представление алгоритма Гровера в виде квантовой схемы

После порядка $\frac{\pi}{4}\sqrt{N}$ итераций вероятность нахождения искомого элемента становится близкой к единице.

IV. Классификация угроз

Для систематизации квантовых угроз информационной безопасности можно выделить несколько ключевых признаков. Один из них связан с типом криптографического примитива: асимметричные алгоритмы, основанные на задачах факторизации и вычисления дискретного логарифма, оказываются уязвимыми перед алгоритмом Шора, тогда как симметричные шифры и хэш-функции подвержены ускоренному перебору с помощью алгоритма Гровера.

Другим важным признаком является характер воздействия: если Шор полностью разрушает математическую указанных алгоритмов, то Гровер лишь снижает их эффективную стойкость, уменьшая длину ключа или сложность поиска предобраза.

Важен и временной горизонт угроз: атаки на асимметричные системы строго доказаны и станут критичными с появлением масштабных квантовых компьютеров, тогда как атаки на симметричные примитивы возможны уже при меньших ресурсах.

Наиболее критичны для инфраструктуры системы обмена ключами, подписей и доверенных каналов, тогда как симметричные шифры и хэш-функции сохраняют стойкость при увеличении параметров.

Сводное распределение существующих криптографических систем по выделенным признакам представлено в таблице 1.

1. M. Ekerå. On completely factoring any integer efficiently in a single run of an order-finding algorithm. / M. Ekerå // Quantum Information Processing. – 2021, – Vol. 205, № 20, P. 1-14.
2. Bernstein D. J. Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? / D. J. Bernstein // Conference Proceedings for Special-purpose Hardware for Attacking Cryptographic Systems. – 2021. – №9. – P. 105-117.
3. Sinitsyn N. Topologically protected Grover's oracle for the partition problem. / N. Sinitsyn, B. Yan // Physical Review A. – 2023. – Vol. 108.
4. Bernstein D. J. Post-quantum RSA. / D. J. Bernstein, N. Heninger, P. Lou; L. Valenta // Luke Post-Quantum Cryptography. Lecture Notes in Computer Science. – 2017. – Vol. 10346. – P. 311-329.
5. Exman I., Pérez-Castillo R., Piattini M., Felderer M. Quantum Software: Aspects of Theory and System Design. / I. Exman, R. Pérez-Castillo, M. Piattini, M. Felderer // Springer Nature. — 2024. ISBN 978-3-031-64136-7.

Таблица 1 – Классификация угроз информационной безопасности со стороны квантовых алгоритмов

Класс системы	Примеры	Алгоритм	Эффект
Асимметричные	RSA, ECC, Diffie–Hellman	Шор	Полная уязвимость
Симметричные	AES-128/192/256	Гровер	Сокращение эффективной длины ключа
Хеш-функции	SHA-2, SHA-3	Гровер	Быстрый поиск коллизий
Инфраструктурные протоколы	TLS/SSL, VPN, PKI	Шор + Гровер	Ослабление защиты
Квантовая криптография	QKD (BB84, E91)	Шор/Гровер	Устойчивы
Асимметричные (постквантовые)	NTRU, Kyber, McEliece	Шор/Гровер	Устойчивы