Безопасность квантовых вычислений

Голубович Тимур Б01-110

1 ноября 2024 г.

Содержание

1 Введение

Безопасность квантовых вычислений становится критически важной из-за угроз, которые представляют квантовые технологии для традиционных методов защиты информации. С увеличением вычислительных мощностей квантовые компьютеры смогут эффективно факторизовать большие числа с помощью алгоритма Шора, что ставит под сомнение надежность криптографических алгоритмов, таких как RSA.

В ответ разрабатываются новые методы защиты, включая квантовое распределение ключей (QKD) и постквантовые криптографические алгоритмы, устойчивые к квантовым атакам. Эти технологии необходимы для обеспечения безопасности данных в будущем.

Таким образом, комплексный подход к безопасности квантовых вычислений, учитывающий технические аспекты, становится важным для специалистов в области информационной безопасности.

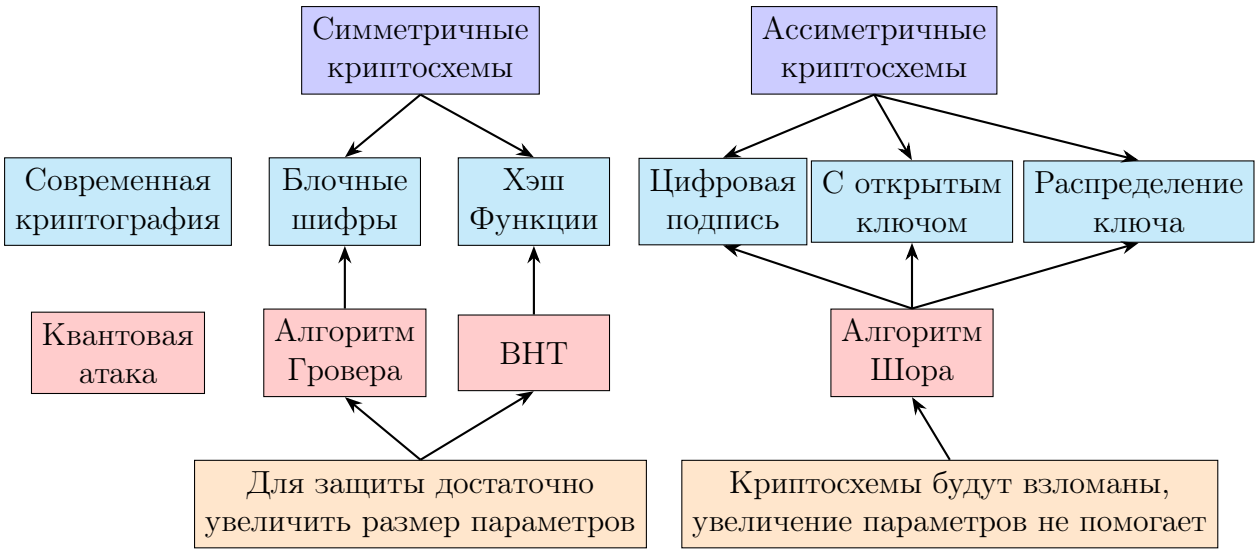

Рис. 1: Постквантовые криптографические механизмы

2 Квантовые алгоритмы и криптография

Квантовые компьютеры могут угрожать традиционной криптографии. Например, алгоритм Шора позволяет эффективно факторизовать большие числа, что ставит под угрозу безопасность систем, основанных на RSA и других алгоритмах, использующих факторизацию. Это означает, что данные, защищенные с помощью таких методов, могут быть уязвимы к атакам с использованием квантовых компьютеров. Давайте подробней рассмотрим, как он работает.

2.1 Факторизация целых чисел

Для начала, факторизация натурального числа есть его разложение в произведение простых множителей. Существование и единственность (с точностью до порядка следования множителей) такого разложения следует из основной теоремы арифметики. Очевидный алгоритм разложения числа на простые множители такой:

Algorithm 1: Факторизация на классическом компьютере

Input: число $n \in \mathbb{N}$, которое необходимо факторизовать
Output: первый простой делитель d
$N \leftarrow [\log_2 n] + 1$ Количество символов в двоичном представлении
if n *простое* **then**
  return n Факторизация не требуется
for *каждое* a *от* 2 *до* $\sqrt{n}$ **do**
  if $n \mod a = 0$ **then**
    $d \leftarrow a$ Находим первый простой делитель **return** d

Рис. 2: Примитивный алгоритм факторизации целового числа

Вопрос о существовании алгоритма факторизации с полиномиальной сложностью на классическом компьютере является одной из важных открытых проблем современной теории чисел. В то же время факторизация с полиномиальной сложностью возможна на квантовом компьютере с помощью алгоритма Шора (класс BQP).

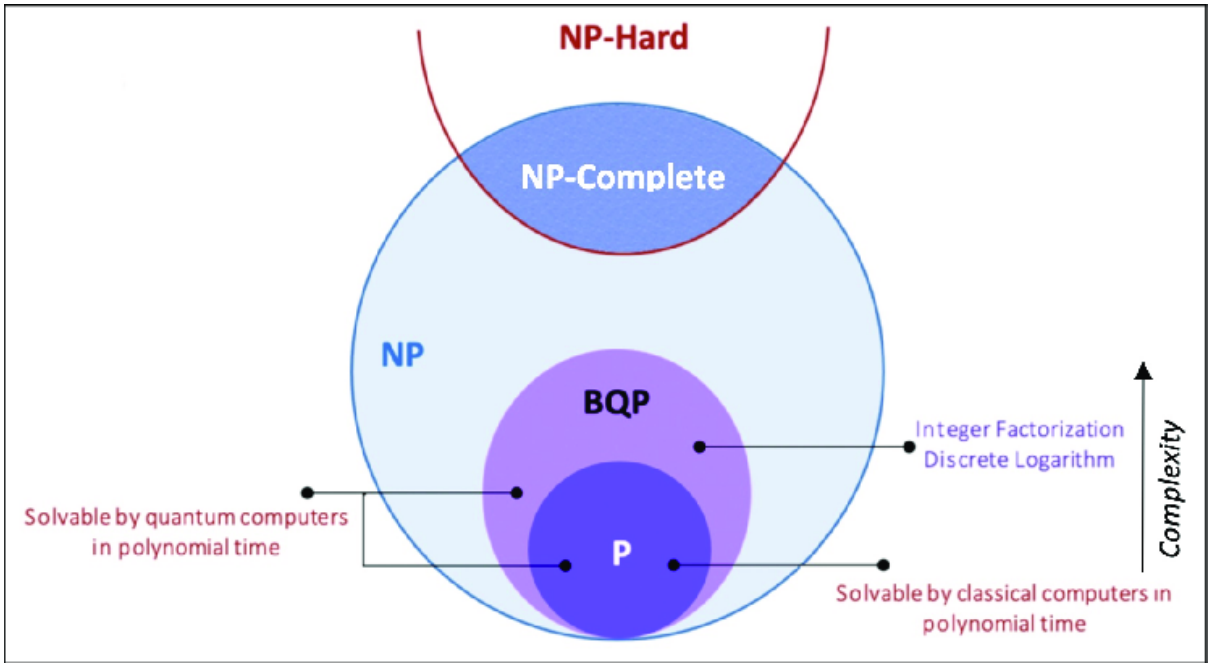

Рис. 3: Предположительная сложность задачи факторизации

2.2 Алгоритм Шора

Алгоритм Шора позволяет выполнить решение задачи факторизации за полиномиальное время. Это осуществляется за счет использования свойства квантового параллелизма и сведения задачи к поиску периода функции.

Допустим, нам необходимо разложить на множители некоторое число N. Изначально выберем произвольное число $a < N$ и рассмотрим функцию $f_a(x) = a^x \mod N$.

Функция $f_a(x)$ является периодической с периодом r. Период r является порядком числа a: $a^r \equiv 1 \mod N$ и $\forall i < r \Rightarrow a^i \not\equiv 1 \mod N$. Если число N простое, то период r будет равен $N-1$. Этот случай весьма простой и легко реализуется проверкой на простоту классическими методами. В общем случае $f_a(x+r) = f_a(x)$. Если период r известен, то разложение на множители числа N легко можно определить классическими методами. В частности, если период r является четным числом, то из соотношения $a^r - 1 \equiv 0 \mod N$ можно записать:

$$(a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \mod N$$

Так как $(a^{r/2} - 1)(a^{r/2} + 1)$ делится на N, то оба сомножителя имеют общие с N делители. Эти делители можно определить классическим алгоритмом Евклида по поиску наибольшего общего делителя. Если же период r является нечетным или $(a^{r/2} - 1)(a^{r/2} + 1)$ вырождается в ноль, то следует выбрать другое число a. Для больших чисел N это случается редко.

Квантовый алгоритм Шора предназначен для быстрого поиска периода r. Для реализации алгоритма необходимо использовать квантовый компьютер с двумя квантовыми регистрами размера n. Причем размер должен быть таким, что $M = 2^n > N$, $M \approx N^2$.

Algorithm 2: Алгоритм Шора для факторизации числа N

Input: Целое число N для факторизации
Output: Непростые множители числа N
while *не найден делитель* **do**
  Выбрать случайное число a такое, что $1 < a < N$
  if *gcd*$(a, N) \neq 1$ **then**
    return *gcd*(a, N) *Найден делитель*
  $r \leftarrow$ *find_period*(a, N) *Квантовый алгоритм для нахождения периода*
  if *r нечетный* ***или*** $a^{r/2} \equiv -1 \mod N$ **then**
    Период не подходит, продолжаем с другим a
  $x_1 \leftarrow a^{r/2} \mod N$
  $x_2 \leftarrow N - x_1$
  if *gcd*$(x_1, N) \neq 1$ **then**
    return *gcd*(x_1, N) *Возвращаем делители*
  if *gcd*$(x_2, N) \neq 1$ **then**
    return *gcd*(x_2, N) *Возвращаем делители*
  return *Не удалось найти делители* Если делители не найдены

Рис. 4: Алгоритм Шора

2.3 Квантовый отжиг

Квантовый отжиг (*Quantum Annealing*) — это метод решения оптимизационных задач, который использует квантовые эффекты для поиска низкоэнергетических состояний системы. Он основан на классическом отжиге, где система охлаждается для достижения минимальной энергии, но в отличие от классического подхода, квантовый отжиг применяет суперпозицию и туннелирование, что позволяет избегать локальных минимумов. Процесс включает в себя несколько этапов:

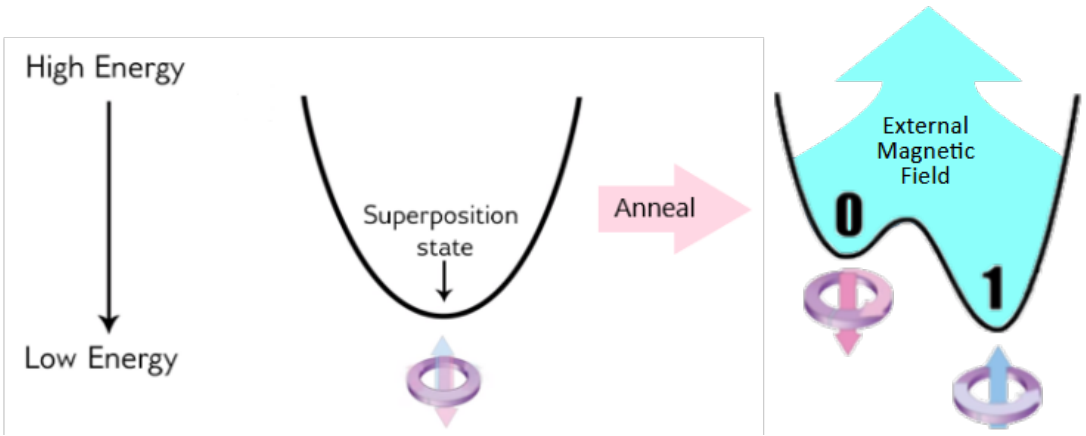

Рис. 5: Энергетическая диаграмма процесса отжига

1. **Инициализация**: Кубит есть основная единица квантовой информации в квантовом процессоре $D-Wave(QPU)$. Он может находиться в состоянии 0, 1 или одновременно в обоих состояниях (суперпозиция). Система начинается с кубитов в состоянии суперпозиции, соответствующем одному минимуму энергии.

2. **Энергетический ландшафт**: По мере эволюции процесса отжига энергетический ландшафт изменяется, создавая множество минимумов. Цель состоит в том, чтобы направить систему к состоянию с наименьшей энергией.

3. **Процесс отжига**: Система переходит от начального гамильтониана к конечному гамильтониану, стремясь оставаться в состоянии с наименьшей энергией на протяжении всего процесса.

4. **Измерение**: В конце процесса отжига каждый кубит оказывается в классическом состоянии (0 или 1), представляя решение задачи.

Квантовый отжиг находит применение в различных областях, таких как комбинаторные задачи оптимизации, машинное обучение и логистика. Технологии, такие как квантовые процессоры от *D-Wave*, специально разработаны для работы с такими задачами. Несмотря на то, что квантовый отжиг находится на ранних стадиях развития, он уже демонстрирует многообещающие результаты в решении сложных оптимизационных задач. Таким образом он представляет угрозу для симметричной криптографии, особенно для потоковых шифров. Существуют шифры, устойчивые к классическим атакам, но они уязвимы к квантовому отжигу. Среди них находится Grain-128a, основная схема финалиста NIST Lightweight Cryptography Grain-128AEAD. Стандартизированные шифры широко используются как в военной, так

и в гражданской отраслях. Стандартизация шифра с такой уязвимостью позволит внедрить угрозу во многие сектора:

– обработка секретных данных;

– устройства Интернета вещей;

– телекоммуникации.

Задачи для квантового отжига формулируются в виде **QUBO** или **Ising** модели. Рассмотрим задачу QUBO.

2.4 QUBO

Определение: QUBO (Quadratic Unconstrained Binary Optimization) — это задача оптимизации, в которой необходимо найти бинарный вектор x (состоящий из 0 и 1), минимизирующий квадратичную функцию. Формально задача может быть записана как:

$$\min_{x \in \{0,1\}^n} f(x) = x^T Q x$$

где Q — симметричная матрица, а x — бинарный вектор.
Основные характеристики:

- **Бинарные переменные:** Переменные x_i могут принимать значения только 0 или 1.
- **Квадратичная функция:** Целевая функция состоит из линейных и квадратных членов.
- **Решение:** Задачи решаются классическими (методы ветвей и границ, генетические алгоритмы) и квантовыми алгоритмами (например, квантовым отжигом).

3 Устойчивость к квантовым атакам

Устойчивость к квантовым атакам — это важная тема в области криптографии, особенно с учетом развития квантовых компьютеров, которые могут угрожать традиционным криптографическим алгоритмам. Квантовые компьютеры обладают способностью решать определенные задачи гораздо быстрее, чем классические компьютеры. Это означает, что если квантовые компьютеры достигнут достаточной мощности, они смогут легко взломать многие существующие криптографические схемы.

3.1 Постквантовая криптография

В ответ на эту угрозу разрабатываются новые криптографические алгоритмы, которые устойчивы к квантовым атакам. Эти алгоритмы называются постквантовыми и включают в себя:

1. **Криптография на основе решеток:** Алгоритмы, основанные на математических структурах, называемых решетками, считаются одними из самых перспективных для создания устойчивых к квантовым атакам систем. Примеры включают схемы шифрования NTRU и схемы цифровой подписи на основе решеток.

2. **Криптография на основе многочленов:** Использует задачи, связанные с многочленами, которые трудно решать даже для квантовых компьютеров.

3. **Криптография на основе кодов:** Алгоритмы, использующие ошибки коррекции кодов, также рассматриваются как потенциально устойчивые к квантовым атакам. Примером является система McEliece.

3.2 Квантовые алгоритмы

Квантовые алгоритмы продолжают развиваться, и помимо алгоритма Шора, стоит упомянуть:

- **Алгоритм Гровера:** Этот алгоритм позволяет ускорить поиск в неупорядоченной базе данных, находя элемент в базе данных из N элементов за $O(\sqrt{N})$ времени.

- **Квантовые алгоритмы для симуляции квантовых систем:** Эти алгоритмы позволяют моделировать квантовые системы и процессы, что может быть полезно в химии, физике и других областях.

- **Квантовые алгоритмы для оптимизации:** Разрабатываются алгоритмы, которые используют квантовые свойства для решения задач оптимизации, такие как алгоритмы QAOA (Quantum Approximate Optimization Algorithm).

4 Заключение

В заключение, развитие квантовых технологий представляет собой процесс, который одновременно открывает новые горизонты и создает угрозы для существующих систем безопасности. Квантовые алгоритмы, такие как алгоритм Шора или алгоритм квантового отжига, демонстрируют, что традиционные методы криптографии, основанные на факторизации или оптимизационных задачах, могут оказаться уязвимыми в условиях появления мощных квантовых компьютеров. В ответ на эти вызовы развивается квантовая криптография.

Тем не менее, на данный момент мощности квантовых компьютеров все еще остаются ограниченными, что дает время для исследования и разработки новых постквантовых криптографических алгоритмов, способных защитить данные от потенциальных квантовых атак. Это создает надежду на то, что мы сможем адаптироваться к изменениям в области вычислительных технологий и сохранить безопасность цифровых коммуникаций в будущем. Важно продолжать инвестировать в исследования и разработки в этой области, чтобы обеспечить защиту данных в эпоху квантовых вычислений.

Список литературы

[1] Thirty Years Later, a Speed Boost for Quantum Factoring

[2] Постквантовый переход

[3] Factorization of Integers

[4] Алгоритм Шора

[5] A Tutorial on Formulating and Using QUBO Models

[6] What is Quantum Annealing?

[7] The possible impact of quantum annealing on cybersecurity

[8] Quantum tunneling breakthrough

[9] Квантовая атака

[10] Безопасность квантовых технологий в сфере IT