Федеральное государственное образовательное бюджетное учреждение
высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»
(Финансовый университет)

Колледж информатики и программирования

Реферат

На тему: «Квантовый алгоритм Шора»

Студент группы 3ОИБАС-*1220*
Чигарёв Иван Александрович «6» июня 2023 г.

Основная профессиональная образовательная программа по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Форма обучения очная

Проверили: _____ Рой А.В.,

_____ Рой О.В.

Москва
2023

Американский математик Питер Шор разработал квантовый алгоритм для целочисленной факторизации, позже названный в его честь, в 1994 году. Алгоритм использует метод определения периода функции и может быть настроен для решения задач вычисления дискретного логарифма в конечной группе или группе точек эллиптических

На квантовом компьютере, к фактору целое число N, пробеги алгоритма Шора в многочленное время (потраченное время является полиномиалом в регистрации N, который является размером входа). Определенно это занимает время и квантовые ворота заказа), использование быстрого умножения, демонстрируя, что проблема факторизации целого числа может быть эффективно решена на квантовом компьютере и находится таким образом в классе сложности BQP. Это существенно быстрее, чем самый эффективный известный классический алгоритм факторинга, общее решето числового поля, которое работает в подпоказательное время — о. Эффективность алгоритма Шора происходит из-за эффективности кванта, который Фурье преобразовывает, и модульное возведение в степень повторным squarings.

Если квантовый компьютер с достаточным числом кубитов мог бы работать, не уступая шуму и другому кванту decoherence явления, алгоритм Шора мог использоваться, чтобы нарушить схемы криптографии открытого ключа, такие как широко используемая схема RSA. RSA основан на предположении, что большие количества факторинга в вычислительном отношении тяжелы. Насколько известен, это предположение действительно для классического (неквант) компьютеры; никакой классический алгоритм не известен, который может фактор в многочленное время. Однако алгоритм Шора показывает, что факторинг эффективен на идеальном квантовом компьютере, таким образом, может быть выполнимо победить RSA, строя большой квантовый компьютер. Это был также сильный фактор мотивации для проектирования и строительства квантовых компьютеров и для исследования новых квантовых компьютерных алгоритмов. Это также облегчило исследование в области новых cryptosystems, которые безопасны от квантовых компьютеров, коллективно названной постквантовой криптографии.

Работоспособность алгоритма Шора была показана в 2001 году на примере факторизации числа 15 на квантовом компьютере из 7 кубитов.

В случае создания квантового компьютера достаточной мощности алгоритм Шора позволит эффективно (за время, лишь ненамного превосходящее требующееся для зашифрования) взламывать большинство используемых сейчас асимметричных криптографических схем (RSA, DSA, EdDSA, ГОСТ Р 34.10-2012 и других).

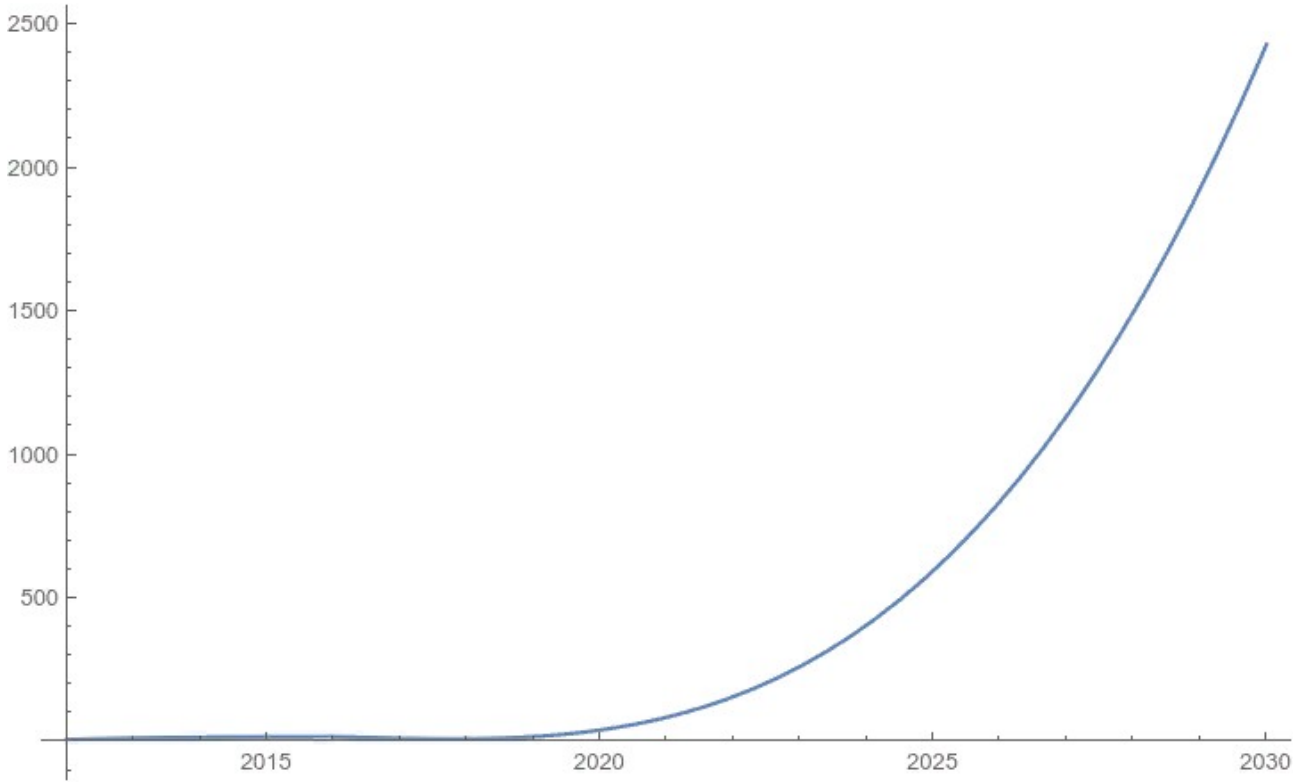
В таблице ниже приведены актуальные на начало 2021 года рекорды по факторизации чисел, используемых в качестве открытого ключа в наиболее

распространенной криптосистеме с открытым ключом RSA. Для сравнения также даны рекорды факторизации достигнутые на классических компьютерах.

Год	Число (квантовый компьютер)	Число (классический компьютер)
2012	143 (8 битов)	RSA-768 (768 битов)
2014	56135 (16 битов)	-
2016	200 099 (18 битов)	-
2019	291 311 (18 битов)	RSA-240 (795 битов)
2020	1 099 551 473 989 (41 бит)	RSA-250 (829 битов)

Отметим также, что некоторые из указанных в таблице рекордов по факторизации чисел получены при помощи квантовых компьютеров, реализующих модели, которые ранее считались не вполне подходящими для решения задач криптоанализа, таких как модель квантового отжига, реализованного в квантовых вычислителях производства компании D-Wave.

На стойкость симметричных шифров (AES, Кузнечик и других) и хэш-функций (SHA, Стрибог и других) алгоритм Шора не оказывает влияния, поскольку для их анализа применяются другие, не столь эффективные алгоритмы (метод Гровера, Саймона, BHT и другие), для успешной защиты от которых достаточно увеличить размер параметров в 2-3 раза.
На рисунке приведен график построенной по второй колонке этой таблицы экстраполирующей функции (по оси X — год, по оси Y — количество битов в числах RSA, факторизуемых квантовым вычислителем). Учитывая, что современные зарубежные рекомендации по защите информации предполагают использование в криптосистеме RSA чисел размера не менее 2048 битов (рекомендовано 3072), можно сделать вывод о том, что квантовые компьютеры, способные эффективно решать задачи криптоанализа используемых сейчас криптосистем, будут доступны в диапазоне 2028-2033 годов.



Тем не менее, поскольку в современных телекоммуникационных сетях симметричные алгоритмы практически всегда используются в связке с асимметричными (как, например, в протоколе TLS), возможная реализация алгоритма Шора представляет реальную угрозу всему существующему криптографическому ландшафту. Злоумышленник может уже сегодня сохранять зашифрованные традиционными методами данные, а с появлением у него доступа к квантовому компьютеру дешифровать их.

Для противодействия квантовой угрозе усилиями мирового криптографического сообщества, в том числе и команды QApp, ведется деятельность по разработке и внедрению квантово-устойчивых криптографических алгоритмов.

Алгоритм Шора — квантовый алгоритм факторизации (разложения числа на простые множители), позволяющий разложить число M за время $O(\log^3 M)$, используя $O(\log M)$ логических кубитов.

Алгоритм Шора был разработан Питером Шором в 1994 году. Семь лет спустя, в 2001 году, его работоспособность была продемонстрирована группой специалистов IBM. Число 15 было разложено на множители 3 и 5 при помощи квантового компьютера с 7 кубитами.

Значимость алгоритма заключается в том, что с его помощью (при использовании квантового компьютера с несколькими тысячами логических кубитов) становится возможным взлом криптографических систем с открытым ключом. К примеру, RSA использует открытый ключ M, являющийся произведением двух больших простых чисел. Один из способов взломать шифр

RSA — найти множители M. При достаточно большом M это практически невозможно сделать, используя известные классические алгоритмы. Наилучшие из известных классических детерминированных доказанных алгоритмов факторизации, такие как метод квадратичных форм Шенкса и алгоритм Полларда — Штрассена, требуют времени порядка $M^{1/4}$. Также метод квадратичных форм Шенкса может работать за время порядка $M^{1/4}$, если верна Гипотеза Римана. Среди вероятностных алгоритмов лидером факторизации является специальный метод решета числового поля, который способен с вероятностью 1/2 найти простой делитель за субэкспоненциальное время $\exp\left(\left(\frac{32}{9}*\log M\right)^{1/3}*(\log\log M)^{2/3}\right)$. Алгоритм Шора, используя возможности квантовых компьютеров, способен произвести факторизацию числа не просто за полиномиальное время, а за время, не намного превосходящее время умножения целых чисел (то есть практически так же быстро, как происходит само шифрование). Таким образом, реализация масштабируемого квантового компьютера поставит крест на большей части современной криптографической защиты. Речь не только о схеме RSA, прямо опирающейся на сложности факторизации, но и о других сходных схемах, которые квантовый компьютер способен взломать аналогичным образом.

Алгоритм Шора имеет вероятностный характер. Первый источник случайности встроен в классическое вероятностное сведе́ние разложения на множители к нахождению периода некоторой функции. Второй источник появляется из необходимости наблюдения квантовой памяти, которое также даёт случайные результаты.

Алгоритм Шора состоит из следующих частей:

- Преобразование проблемы факторизации в задачу нахождения периода. Эта часть может быть реализована классическими средствами.

- Нахождение квантового периода с помощью квантового преобразования Фурье, которое отвечает за квантовое ускорение и использует квантовый параллелизм.

Основа алгоритма Шора: способность информационных единиц квантовых компьютеров — кубитов — принимать несколько значений одновременно и находиться в состоянии «квантовой запутанности». Поэтому он позволяет проводить вычисления в условиях экономии кубитов. Принцип работы алгоритма Шора можно разделить на 2 части: первая — классическое сведе́ние разложения на множители к нахождению периода некоторой функции, вторая — квантовое нахождение периода этой функции. Пусть:
M — число, которое мы хотим разложить на множители (оно не должно быть целой степенью нечётного числа);

N — размер регистра памяти, который используется (не считая свалки). Битовый размер этой памяти $n = log_2 N$ примерно в 2 раза больше размера M. Точнее, $M^2 < N = 2^n < 2M^2$;
t — случайный параметр, такой что $1 < t < M$ и $gcd(t, M) = 1$(где — gcd наибольший общий делитель).
Отметим, что t, N, M — фиксированы. В алгоритме Шора используется стандартный способ сведения задачи разложения к задаче поиска периода r функции для случайно подобранного числа t.

Квантовая часть алгоритма

Для осуществления квантовой части алгоритма вычислительная схема представляет собой **2** квантовых регистра ***X*** и ***Y***. Первоначально каждый из них состоит из совокупности кубитов в нулевом булевом состоянии |0).

Регистр **X** используется для размещения аргументов x функции $\int(x)$. Регистр **Y** (вспомогательный) используется для размещения значений функции $\int(x)$ с периодом r, подлежащим вычислению.

Квантовое вычисление состоит из 4 шагов:

- **Первый шаг.** На первом шаге с помощью операции Уолша — Адамара которая представляет собой преобразование кубита с помощью оператора $H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$, первоначальное состояние |0) регистра X переводится в равновероятную суперпозицию всех булевых состояний N. Второй регистр ***Y*** остаётся в состоянии |0). В итоге получается следующее состояние для системы двух регистров:
  $\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}$.
- **Второй шаг.** Пусть U_f— унитарное преобразование, которое переводит | x,0) в | $\int(x)$). На втором шаге применяется унитарное преобразование к системе двух регистров. Получается следующее состояние системы:

$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x,0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x,t^x \bmod M\rangle$, то есть между состояниями обоих регистров образуется определённая связь.

- **Третий шаг**. Квантовое Фурье-преобразование представляет собой унитарное преобразование состояния квантового регистра, описываемого N-мерным вектором состояния вида $\sum_{x=0}^{N-1} f(x)|x\rangle$, в другое состояние $\sum_{k=0}^{N-1} \tilde{f}(k)|k\rangle$:

  $\mathrm{QFT}_N : \sum_{x=0}^{N-1} f(x)|x\rangle \Rightarrow \sum_{k=0}^{N-1} \tilde{f}(k)|k\rangle$, где амплитуда Фурье-преобразования $f(x)$ имеет вид

  $$\tilde{f}(k) = \frac{1}{N}\sum_{x=0}^{N-1} \exp(2\pi\, i\, kx/N) f(x).$$

  В двумерной x,k-плоскости преобразование Фурье соответствует повороту осей координат на 90°, которое приводит к преобразованию шкалы x в шкалу k. На третьем шаге над состоянием первого регистра производится преобразование Фурье, и получается

  $$\frac{1}{N}\sum_{x=0}^{N-1}\sum_{k=0}^{N-1} \exp(2\pi\, i\, kx/N)|k, t^x \bmod M\rangle.$$

- **Четвёртый шаг**. На четвёртом шаге выполняется измерение первого регистра X относительно ортогональной проекции вида:
  $|0,0\rangle \otimes I, \quad |1,1\rangle \otimes I, \quad \ldots, \quad |N-1,N-1\rangle \otimes I$, где I — тождественный оператор на гильбертовом пространстве второго регистра Y.

В результате получается $|k, t^k \bmod M\rangle$ с вероятностью[6]

$$\left|\frac{1}{N}\sum_{x:\, t^x \equiv t^k \bmod M} \exp(2\pi\, i\, kx/N)\right|^2.$$

На оставшейся части прогона работает классический компьютер:

- Находится наилучшее приближение (снизу) к $\frac{k}{N}$ со знаменателем $r' < M < \sqrt{N}$:

  $$\left|\frac{k}{N} - \frac{d'}{r'}\right| < \frac{1}{2N}.$$

- Пробуем r' в роли r:
  - Если $r' \equiv 0 \bmod 2$, то следует вычислить $\gcd(t^{\frac{r'}{2}} \pm 1, M)$.
  - Если r' нечётно или если r' чётно, но собственный делитель M не обнаружен, то следует повторить прогон $O(\log\log M)$ раз с тем же самым t. В случае отказа изменить t и начать новый прогон алгоритма[3][4].

В некоторой степени определение периода функции с помощью преобразования Фурье аналогично измерению постоянных решётки кристалла методом рентгеновской или нейтронной дифракции. Чтобы определить период r, не требуется вычислять все значения $f(x)$. В этом смысле задача похожа на задачу Дойча, в которой важно знать не все значения функции, а только некоторые её свойства[6].

Существующие атаки

Для примера, рассмотрим атаку, которая нацелена именно на алгоритм RSA. Суть этой атаки заключается в поиске ключа путем факторизации большого числа (алгоритм Шора для этого как раз заточен!). Если мы сможем вычислить простые числа, которые использовались для генерации конкретного ключа, то фактически получим значение этого ключа.

Итак, мы должны перебрать большой набор чисел. Это очень сложно сделать, но теперь в наших руках грозное оружие — алгоритм Шора. Если наш процесс пройдёт успешно, у нас будет возможность атаковать систему RSA. Фактически, вся сложность состоит во времени, которое нужно для перебора чисел.

По существующим оценкам учёных, при наличии квантовых компьютеров нам потребуется около 20 миллионов физических кубитов для ключа размером 2048 бит. Вы удивитесь, но даже и при таком огромном количестве кубитов нам нужно будет ждать 8 часов.

Если у нас в распоряжении не такие мощные квантовые компьютеры, то оценки показывают, что с 13436 квантовыми единицами информации мы должны будем потратить 177 дней. Сегодня мы не располагаем такой возможностью. Хорошо это или плохо? Поговорим в следующем разделе.

Перспективы развития

Адаптируя стратегию "если ты не можешь кого-то победить, присоединяйся к ним", сейчас начинается гонка за право использования тех же квантовых вычислений. Возможно, эта гонка ведётся даже за мощь "квантового Интернета", который приведёт к созданию новых, более сложных процедур шифрования. Конечная цель — постквантовая криптография.

Можно выделить несколько перспективных методов, на которых основана постквантовая криптография:

- Схемы шифрования McEliece и Niederreiter
- Криптография на решётках
- Обмен ключами с использованием суперсингулярных изогений
- Многомерная криптография

Эти подходы не являются решением на века, но способны составить большую конкуренцию квантовым протоколам взлома. Заинтересовавшиеся могут ознакомиться подробнее по ссылкам выше.

Стоит отметить, что проблема массового исчезновения информационной безопасности не нова. Шифрование, созданное немецкими военными машинами Enigma во время Второй мировой войны, в конечном итоге было взломано союзниками, но на этом криптография не закончилась. А в 1977 году в ходе публичного конкурса был нарушен современный стандарт шифрования данных (DES).

Сегодня особого внимания требует предупреждение Питера Шора о своевременном выполнении решений. Очевидно, что давление оказывается потому, что технологии шифрования глубоко встроены во многие различные системы. По этой причине их взлом и внедрение новых может занять много времени.

Не все предсказывают, что гонка завершится через несколько лет. Например, Роджер Граймс, специалист по обеспечению безопасности KnowBe4, объявил, что 2021, вероятно, станет первым публичным признанием квантового криптографического взлома, когда квантовые компьютеры будут способны взламывать традиционные криптографические ключи с открытым ключом. Как мы можем наблюдать, этого пока не случилось.

Алгоритм составлен из двух частей. Первая часть алгоритма превращает проблему факторинга в проблему нахождения периода функции и может быть осуществлена классически. Вторая часть находит период, используя квант, который преобразовывает Фурье, и ответственно за квантовое ускорение.

Получение факторов с периода

Целые числа меньше, чем N и coprime с N формируют конечную группу Abelian под модулем умножения N. Размер дан функцией totient Эйлера.

К концу шага 3 у нас есть целое число в этой группе. Так как группа конечна, необходима конечный приказ r, самое маленькое положительное целое число, таким образом что

:

Поэтому, N делит (также письменный |) − 1. Предположим, что мы в состоянии получить r, и это ровно. (Если r странный, посмотрите шаг 5.) Теперь квадратный корень 1 модуля, отличающегося от 1. Это вызвано тем, что заказ модуля, таким образом, еще заказ в этой группе был бы. Если, шагом 6 мы должны перезапустить алгоритм с различным случайным числом.

В конечном счете мы должны совершить нападки, заказа в, такой что. Это вызвано тем, что таков квадратный корень 1 модуля, кроме 1 и, чье существование гарантируется китайской теоремой остатка, так как не главная власть.

Мы утверждаем, что это - надлежащий фактор, то есть. Фактически, если, то делится, так, чтобы, против строительства. Если, с другой стороны, то личностью Безута есть целые числа, таким образом что

Умножая обе стороны на мы получаем

С тех пор делится, мы получаем, который делится, так, чтобы, снова противореча строительству.

Таким образом необходимый надлежащий фактор.

Нахождение периода
Находящий период алгоритм Шора полагается в большой степени на способность квантового компьютера быть во многих государствах одновременно.

Физики называют это поведение «суперположением» государств. Чтобы вычислить период функции f, мы оцениваем функцию во всех пунктах одновременно.

Квантовая физика не позволяет нам получать доступ ко всей этой информации непосредственно, все же. Измерение приведет к только одной из всех возможных ценностей, уничтожая всех других. Если бы не никакая теорема клонирования мы могли сначала измерить f (x), не имея размеры x, и затем сделать несколько копий получающегося государства (который является

суперположением государств все имеющие тот же самый f (x)). Измерение x на этих государствах обеспечило бы различные ценности x, которые дают тот же самый f (x), приводя к периоду. Поскольку мы не можем сделать точные копии квантового состояния, этот метод не работает. Поэтому мы должны тщательно преобразовать суперположение к другому государству, которое даст правильный ответ с высокой вероятностью. Это достигнуто квантом, который преобразовывает Фурье.