КВАНТОВЫЕ АЛГОРИТМЫ И ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ

Кубиты (или квантовые биты) способны принимать уже не два а большее количество состояний, обычно представляемых на т.н. сфере Блоха. Система кубитов вместе с каждым значением хранит его амплитуду (векторное значение вероятности).

Квантовый процессор – вычислительное устройство, в основе которого лежат унитарные операции (экспоненты некоторых Эрмитовых операторов, сохраняют скалярное произведение) с кубитами.

Например, 64-разрядный квантовый регистр может хранить до 2^{64} значений в одном месте [7,8], а квантовый компьютер может все эти значения одновременно обрабатывать [7].

Квантовый компьютер – вычислительное устройство на основе квантовых процессоров, способное работать по программе (трудно реализовать, пока носит лабораторный характер, (Цзючжан -2020 (аналоговый бозонный сэмплер), Сикамор-2019 (53 кубита на основе сверхпроводников) проблема исправления ошибок, связанная с невозможностью копирования состояния, влиянием кубитов и их содержания друг на друга, проблема считывания состояния, неустойчивость физических устройств и вычислений).

Квантовая арифметика связана с тригонометрическими суммами, выражающими амплитуды состояний. Унитарные преобразования повышают вероятность (квадрат модуля амплитуды) искомых состояний. Эти состояния и считываются с наибольшей вероятностью в итоговом состоянии.

[7] Andrew M. Steane, Eleanor G. Rieffel Beyond Bits: The Future of Quantum // Information Processing. 2000, Computer 33 (1): 38-45 DOI: 10.1109/2.816267

[8] Eleanor Rieffel An Introduction to Quantum Computing for Non-Physicists // 2000, ACM Computing Surveys 32 (3) 48p. DOI: 10.1145/367701.367709

Ситуация с квантовым компьютером сейчас отличается от ситуации с обычным компьютером в середине 20 века и ранее. Первые компьютеры хоть и медленно, но работали (например, суммирующая машина Паскаля 1642г. осуществляла арифметические преобразования пятизначных десятичных чисел (около 50 сделано, 15 из них было продано), разностная машина Беббиджа 1822г. вычисляла значения многочленов до 7 степени, ЭВМ “Bombe”, “Colossus” 1940-43г. осуществляли взлом немецких шифровальных машин Enigma и Lorenz), а первые квантовые - нет.

Если $1/k^s$ это вероятность успешного срабатывания одного кубита в s шагах программы для n кубитного процессора (вычисляющего функцию от n битного аргумента). Тогда для того, чтобы получить хотя бы один правильный (по всем кубитам) результат нам понадобиться в среднем произвести k^{sn} квантовых шагов. При $k^s > 2$, это больше, чем количество всех возможных аргументов данной задачи. Значительного выигрыша по сравнению с обычным компьютером, последовательно обрабатывающим эти аргументы, мы не получаем.

Квантовый компьютер --- спец-вычислитель (ранее известны векторные машины, SAT-solvers), основанный на природных (физических, биологических) принципах или автоматах, который некоторые задачи может решать эффективнее обычных компьютеров, а для некоторых других не может быть эффективно применен. Какие алгоритмы принципиально нельзя так ускорить пока не ясно.

Достоверность одного шага квантового компьютера **(Fidelity) зависит от числа кубитов и от номера шага (не исследовано)**.

Технология **«Выстрел»**: **Одна квантовая операция** с последующим анализом результатов на обычном компьютере. Уменьшаются проблемы с нагревом, количеством ошибок, проще создать идеальные условия.

Для реализации конкретных практических задач **не нужен полноценный квантовый компьютер. (Jiuzhang 2020** фотоны более стабильны, не требуют охлаждения, лучше масштабируются**)**

КВАНТОВОЕ ДЕШИФРОВАНИЕ

Пусть блочный шифр осуществляет взаимно однозначное отображение открытого текста t в шифрованный текст той же длины при ключе k той же длины: $F(k,t)=c$. Пусть при разных k в один и тот же шифртекст преобразуются разные t . И пусть нам удалось реализовать расшифрование при помощи унитарного преобразования: $F^{-1}(k,c) = t$. Тогда, сравнивая статистику результата со статистикой случайного осмысленного текста в языке (что-то вроде каппа-теста), мы получаем открытый текст t .

Примеры важных для криптографии алгоритмов для квантового компьютера

Алгоритм Дойча-Йожа (решение задачи разделения случаев, когда некоторая булева функция от нескольких булевых переменных является сбалансированной (то есть в половине случаев принимает значение 0, а в половине 1) или константой). Это исторически первый алгоритм для квантовых вычислителей (1992г.). Его выполнение требует **одного** фазового запроса на вычисление соответствующей функции [9].

Алгоритм Бернштейна-Вазерани: Дана как чёрный ящик функция f(x) = (x, s) - скалярное произведение двоичных векторов длины n. Найти s за минимальное число запросов. Этот алгоритм является модификацией предыдущего (1993). Достаточно **O(1)** обращений к квантовому компьютеру [10].

[9] David Deutsch and Richard Jozsa Rapid solution of problems by quantum computation. // Proceedings of the royal society A math., phyz., eng. Sci., 1992, v.439, issue 1907

https://royalsocietypublishing.org/doi/10.1098/rspa.1992.0167

[10] Jack D. Hidary. Quantum Computing: An Applied Approach // Springer International Publishing, 2019, С. 104—107. — ISBN 978-3030239213. — doi:10.1007/978-3-030-23922-0
https://epubs.siam.org/doi/10.1137/S0097539796300921

1. Практическая возможность реализации квантовых операций определяет используемый математический аппарат.

We now give certain properties of quantum computation that will be useful. These facts are not apparent from the definition of quantum Turing machine or quantum circuit, and they are very useful for constructing algorithms for quantum machines.

Fact 1: A deterministic computation is performable on a quantum computer if and only if it is reversible [BV]. From results on reversible computation [Benn, BV], this means that we can compute any polynomial time function $f(a)$ as long as we keep the input, a, on the machine. To erase a and replace it with $f(a)$ we need in addition that f is one-to-one and that a is computable in polynomial time from $f(a)$; i.e., that both f and f^{-1} are polynomial.

Fact 2: Any polynomial size unitary matrix can be approximated using a polynomial number of elementary unitary transformations [Deu2, BV, Yao] and thus can be approximated in polynomial time on a quantum computer. Further, this approximation is good enough so as to introduce at most a bounded probability of error into the results of the computation.

2. Унитарные преобразования полиномиального размера можно реализовать и на обычном компьютере. Создание начального заполнения и дискретное преобразование Фурье делаются в алгоритме Шора с помощью полиномиальной последовательности квантовых операций, кратно увеличивающих число состояний системы. Причем при создании начального заполнения амплитуды не имеют векторной составляющей. При современных способах реализации, с фиксированной долей ошибки это приводит к случайному результату. Поэтому алгоритм Шора на данном этапе является непрактическим. А защита информации все равно необходима.

Алгоритм Шора факторизации M:

Преобразование Фурье: $\sum_{x=1}^{N} e^{2\pi i x \frac{r}{N}} = \begin{cases} 0 \text{ при } r \neq N \\ N \text{ при } r = N \end{cases}$

Регистры памяти (аргумент, значение ф-ии) = (x, t^x (mod M))

Если r четное и $t^{\frac{r}{2}} \neq -1 \pmod{M}$ **, то НОД(**$t^{\frac{r}{2}} + 1$ **, M) – нетривиальный.**

Шаги: 1. Начальное заполнение

2. QFT = DFT экспоненциального размера = композиция полиномиального числа DFT полиномиального размера

$$a_{ks} = e^{2\pi i \frac{ks}{q_1}}, b_{uv} = e^{2\pi i \frac{uv}{q_2}}, c_{mn} = e^{2\pi i \frac{mn}{q_1 q_2}} \rightarrow c_{(s_1 q_2 + s_2 q_1),(t_1 q_2 + t_2 q_1)} = a_{s_1 t_1} b_{s_2 t_2}$$

При $(q_1, q_2) = 1$,

$\text{DFT}_{q_1 q_2}$ **является перестановкой тензорного произведения** $\text{DFT}_{q_1} \otimes \text{DFT}_{q_2}$

3. Измерение

Given x and n, to find r such that $x^r \equiv 1 \pmod{n}$, we do the following. First, we find a smooth q with $5n^2 < q \leq 10n^2$. Next, we choose a random number $a \pmod{q}$. This leaves our machine in state

$$\frac{1}{q^{1/2}} \sum_{a=0}^{q-1} |a\rangle .$$

As in the algorithm for discrete log, we will not write x and n in the state of our machine, because we never erase these values.

Next, we compute x^a. We then map $a \to c$ with amplitude $\frac{1}{q^{1/2}} \exp(2\pi iac/q)$. This leaves our machine in state

$$\frac{1}{q} \sum_{a=0}^{q-1} \exp(2\pi iac/q) \, |c, x^a\rangle .$$

We now compute the probability that our machine ends in this state. Writing $a = br + k$, we obtain that this probability is

$$\left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k)/r \rfloor} \exp(2\pi i(br+k)c/q) \right|^2 .$$

Using the same argument as in the algorithm for discrete log, if $\{rc\}_q$ is small relative to q, all the amplitudes will point in nearly the same direction, giving a big probability. This

Алгоритм Шора дискретного логарифмирования: (a, b, $g^a x^{-b} = g^k \pmod{p}$)

Использование аппарата цепных дробей:

The probability of seeing a given state $\left|c, x^k \pmod n\right\rangle$ will thus be at least $1/3r^2$ if

$$\frac{-r}{2} \leq \{rc\}_q \leq \frac{r}{2}, \tag{5.11}$$

i.e., if there is a d such that

$$\frac{-r}{2} \leq rc - dq \leq \frac{r}{2}. \tag{5.12}$$

Dividing by rq and rearranging the terms gives

$$\left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q}. \tag{5.13}$$

We know c and q. Because $q > n^2$, there is at most one fraction d/r with $r < n$ that satisfies the above inequality. Thus, we can obtain the fraction d/r in lowest terms by rounding c/q to the nearest fraction having a denominator smaller than n. This fraction can be found in polynomial time by using a continued fraction expansion of c/q, which

Квантовый алгоритм Шора [4, 12] (1994) факторизации целых чисел, позволяющий разложить число n на простые множители за $O(\log^3 n)$ операций, используя $O(\log n)$ кубитов.

Для эллиптических кривых квантовый алгоритм дискретного логарифмирования может быть построен при помощи замены в алгориме Шора выражений вида

$g^a x^{-b} = g^k$ на $\Phi_a(P) + \Phi_{-b}(X) = \Phi_k(P)$,

где $\Phi_n(P)$ – многочлены деления (координата n-кратной точки nP на эллиптической кривой).

[4] Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM J. Comput. 1997. Vol. 26, № 5, P. 1484–1509

[12] Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on — IEEE, 1994. — P. 124–134. — ISBN 0-8186-6580-7 — doi:10.1109/SFCS.1994.365700

Выводы

- При использовании произвольных унитарных операций необходимо обеспечить полное (или близкое к полному, то есть с асимптотически малой долей) исправление ошибок. В противном случае (при фиксированной доле ошибок), из-за экспоненциального роста их количества, даже при полиномиальном числе запросов к квантовому вычислителю, результат работы по программе будет носить случайный характер.
- Для решения криптографически значимых задач на квантовом компьютере, допускающем некоторое количество ошибок, необходимо предложить квантовые алгоритмы, с количеством запросов меньшим константы (такие как алгоритмы Дойча-Йожи, Бернштейна-Вазерани)
- Для получения практических алгоритмов было бы полезно перечислить все возможные квантовые операции, существенно затрагивающие экспоненциально большое количество амплитуд.
- В противном случае разрозненные усилия физиков и математиков будут наполнять знаниями международную базу знаний, увеличивая риски ее использования в деструктивных целях.

Ориентировочные размеры параметров в байтах (V уровень стойкости)

Название	Тип	Длина с.к.	Длина о.к.	Длина ш.т. (подписи)
Lepton	Ш	80	4128	5557
Three Bears	Ш, ВОК	40	1584	1697
qTESLA	П	4128	6432	5920
Classic McEliece	Ш	13908	1047319	22
LEDAcrypt	ВОК/Ш	40	18016	9008
DILITHIUM	П	3856	760	3366
FrodoKEM	ВОК	31272	15632	15768
RQC	ВОК, Ш	3510	3510	3574
NTRU	Ш	6130	6734	140
NewHope	ВОК	3680	1824	2208
SIKE	ВОК	826	726	766
Rainbow	П	1319000	871000	118
LUOV	П	32	39300	4700
SPHINCS	П	1024	1024	41800
Picnic	П	256	512	209474
WalnutDSA	П	1040	634	7704
pqRSA	Ш, П	25769803776	8589934592 (8 Тб!)	8589934592
RSA, FF-DLP	П, Ш, ВОК	3 / 1920	1920	1920
EC-DLP	П, Ш, ВОК	64	128	128

Коды — решетки — изогении — многочлены — хэш — прочее

Crypto AG

Питер Дженкс (АНБ): «Электронноя система, будучи разработанной хитроумным математиком-криптологом, может делать вид, что выдает бесконечные потоки случайных символов, но при этом , на самом деле, повторять выходные данные через достаточно небольшие интервалы с тем, чтобы эксперты АНБ и их мощные компьютеры могли бы их взломать.»

Вплоть до 2018г. более 50 лет, ЦРУ вносила критические изменения в шифровальную продукцию швейцарской фирмы Crypto AG для чтения секретной переписки правительств Ирана, Индии, Пакистана, стран Латинской Америки, Аргентины и Ватикана.

8 лет (2006-2014) стандарт NIST Dual_EC_DRBG на псевдослучайную последовательность использовался и приносил информацию тем, кто владел секретным ключом. Стандарт отозван после появления открытой публикации о его вскрытии.

На прошедших выборах в ГД осенью 2021г. Была использована блокчейн платформа фирмы Waves с эллиптической кривой secp256k1 , построенной для схемы Bitcoin. Электронное голосование проводилось через интернет в системе «Госуслуги». Все это категоритчески запрещено ФЗ-20 «О государственной автоматизированной системе РФ «Выборы», а также УК РФ ст.142.2. и Законом о защите персональных данных.

Новые реалии: Большие сетевые трафики. Много каналов утечки информации.

Криптография в новых условиях.

- Децентрализованное распределение ключей (хеш старого ключа с новой общей секретной информацией).
- Децентрализованное шифрование (разделение при помощи пороговых схем с последующей отправкой разными маршрутами через списки доверия)
- Децентрализованная аутентификация (каждый подписывает весь свой цифровой след в интернете).

В децентрализованной системе методы защиты информации те-же, но квантовый компьютер «к каждому не приставишь» (принцип распараллеленной защиты: чтобы сломать общую защиту надо сломать защиту каждого).

СПАСИБО ЗА ВНИМАНИЕ!