УДК 004.27:004.056.55

П. Г. Ключарев

КВАНТОВЫЙ КОМПЬЮТЕР И КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ СОВРЕМЕННЫХ СИСТЕМ ШИФРОВАНИЯ

Рассмотрены квантовые алгоритмы, которые могут быть использованы в задачах криптоанализа, и то влияние, которое могут оказать квантовые компьютеры на информационную безопасность, когда появятся их практические образцы.

Криптографические алгоритмы имеют большое значение в задачах обеспечения информационной безопасности. Стойкость многих современных криптоалгоритмов в настоящее время считается более чем достаточной. Однако положение серьезнейшим образом изменится после разработки практических образцов квантовых компьютеров.

Современные криптоалгоритмы. Современные алгоритмы шифрования можно подразделить на симметричные и асимметричные (алгоритмы с открытым ключом). Симметричный алгоритм шифрования (например, AES, RC6 и др.) считается достаточно стойким, если не известны способы взлома этого криптоалгоритма, более быстрые, чем полный перебор. Сложность полного перебора (для атаки с известным шифротекстом) можно оценить как $O(2^k)$, где k — длина ключа в битах. Учитывая, что в 2002 г. с помощью любительской сети распределенных вычислений distributed.net была продемонстрирована возможность взлома 64-битного ключа методом грубой силы, сейчас нормой считается длина ключа 128 бит, а максимальная длина ключа, поддерживаемая большинством симметричных криптоалгоритмов, равна 256 битам.

Для асимметричных криптоалгоритмов известны способы криптоанализа, работающие значительно быстрее полного перебора. Из-за этого асимметричные криптографические алгоритмы имеют длину ключа, значительно бóльшую, по сравнению с симметричными. Наиболее часто применяются алгоритм RSA, основанный на вычислительной сложности задачи о факторизации целых чисел, и алгоритм Эль-Гамаля, основанный на вычислительной сложности задачи дискретного логарифмирования. Причем используются версии алгоритма Эль-Гамаля для различных полей. В частности, большое значение имеет алгоритм Эль-Гамаля над группой точек эллиптической кривой [3] (табл. 1).

Квантовые вычисления. Квантовые компьютеры смогут решать задачи криптоанализа значительно эффективнее по сравнению с классическими. Кратко рассмотрим основные положения теории квантовых вычислений. Более обстоятельное введение можно найти, например, в работе [1].

Таблица 1

Сопоставление длины ключей симметричных и асимметричных шифров при одинаковой криптостойкости.

Длина ключа симметричного криптоалгоритма	Длина ключа алгоритма RSA	Длина ключа алгоритма Эль-Гамаля над группой точек эллиптической кривой
80	1024	163
112	2048	224
128	3072	283
192	7680	409
256	15360	571

Квантовые компьютеры основаны на квантовых регистрах, которые состоят из квантовых битов. Квантовый бит — это простейшая квантовая система, имеющая два выделенных состояния. Одно из его выделенных состояний будем обозначать $|0\rangle$, а другое $|1\rangle$. Состояние квантовой системы можно измерить. При этом квантовый бит может иметь такое состояние, что измерение может с некоторой вероятностью показать $|0\rangle$, а с некоторой другой показать $|1\rangle$. Будем описывать состояние такой системы как линейную комбинацию выделенных состояний: $(a\,|0\rangle + b\,|1\rangle)$, где a и b — комплексные числа, такие что $|a|^2 + |b|^2$=1. Тогда измерение состояния $(a\,|0\rangle + b\,|1\rangle)$ с вероятностью $|a|^2$ покажет состояние $|0\rangle$, а с вероятностью $|b|^2$ покажет состояние $|1\rangle$.

Квантовый регистр, состоящий из n квантовых битов, имеет 2^n выделенных состояний, соответствующих n разрядным двоичным числам от $|00\ldots0\rangle$ до $|11\ldots1\rangle$. Состояние квантового регистра записывается в виде линейной комбинации всех этих выделенных состояний:

$$\sum_{x=0}^{2^n-1} a_x\,|x\rangle.$$

При этом выполняется условие нормировки

$$\sum_{i=0}^{2^n-1} |a_i|^2 = 1.$$

Коэффициенты a_x являются комплексными числами. Они называются амплитудами соответствующих состояний $|x\rangle$.

Состояние системы, состоящей из n квантовых битов, описывается вектором единичной длины в 2^n-мерном комплексном унитарном пространстве (скалярное произведение состояний $|a\rangle = |a_1\ldots a_n\rangle$ и $|b\rangle = |b_1\ldots b_n\rangle$ обозначается как $\langle a|b\rangle$ и вводится обычным образом: $\langle a|b\rangle = \sum\limits_i a_i b_i^*$). Таким образом, квантовый регистр длины n может представлять различные значения n-битного слова одновременно.

Чтобы извлечь из квантового регистра информацию, надо провести измерение. При этом измерить можно любой набор квантовых битов. Кроме того, поскольку квантовые состояния образуют евклидово пространство, измерения можно проводить в различных базисах. Однако проведение измерения приводит к переходу системы в базисное состояние, соответствующее результатам измерения.

Квантовый компьютер может осуществлять преобразования над квантовым регистром. Квантовым преобразованием будем называть отображение унитарного пространства, образуемого квантовой системой, в себя. С квантовыми системами можно производить только линейные унитарные преобразования, причем любое линейное унитарное преобразование допустимо. В силу линейности, квантовые преобразования полностью определяются их действием на базисные векторы.

Некоторые важнейшие элементарные преобразования (квантовые вентили) приведены в табл. 2

Криптоанализ симметричных шифров. Один из известных квантовых алгоритмов — алгоритм Гровера. Обычно его описывают как алгоритм поиска в неупорядоченном массиве. Однако небольшая модификация превращает его в алгоритм для восстановления ключа симметричного алгоритма шифрования по тексту сообщения и шифротексту. При использовании классического компьютера для этого требуется полный перебор, имеющий сложность $O(2^m)$, где m — длина ключа. Для квантового компьютера эту сложность можно сильно уменьшить.

Будем рассматривать функцию $y = c(k, x)$. Эта функция шифрует сообщение x на ключе k; x и y — целые числа в диапазоне $x, y \in [0, 2^n - 1]$, где n — длина блока. Пусть нам известна пара сообщение–шифротекст: x_1, y_1. Рассмотрим функцию $f(k)$, которая принимает значение единицы, если $c(k, x_1) = y_1$, и нуля в противном случае. Требуется найти значение аргумента, при котором функция равна единице.

Рассмотрим следующий квантовый алгоритм:

приводим квантовый регистр в состояние $\frac{1}{\sqrt{2^m}} \sum\limits_{t=0}^{2^m-1} |t\rangle$;

вычисляем функцию f от этого регистра $\frac{1}{\sqrt{2^m}} \sum\limits_{x=0}^{2^m-1} |t\rangle\,|f(t)\rangle$.

Повторяем $\frac{\pi}{4}\sqrt{2^m}$ раз процедуру увеличения амплитуды всех t_i, для которых $f(t_i) = 1$ (эта процедура описывается далее).

Измеряем состояние регистра. Результат будет равным искомому ключу с вероятностью около 2^{-n}. Если результат все-таки оказался неверным (это легко проверить), весь алгоритм следует выполнить заново.

Процедура увеличения амплитуды состоит из двух этапов: 1) изменение амплитуды с a_j на $-a_j$ для всех t_i, таких, что $f(t_i) = 1$. Эта операция представляет собой преобразование Z над последним

Преобразования квантовых вентилей

Название, обозначение и краткое описание квантового вентиля	Действие на базовые состояния	Матрица
Тождественное преобразование I	$\|0\rangle \to \|0\rangle$ $\|1\rangle \to \|1\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Отрицание X	$\|0\rangle \to \|1\rangle$ $\|1\rangle \to \|0\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Фазовый сдвиг Z	$\|0\rangle \to \|0\rangle$ $\|1\rangle \to -\|1\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Фазовый сдвиг с отрицанием Y	$\|0\rangle \to -\|1\rangle$ $\|1\rangle \to \|0\rangle$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
Controlled-NOT CNOT Прибавляет ко второму биту первый по модулю 2	$\|00\rangle \to \|00\rangle$ $\|01\rangle \to \|01\rangle$ $\|10\rangle \to \|11\rangle$ $\|11\rangle \to \|10\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Controlled-Controlled NOT (Вентиль Тофолли) Прибавляет к третьему биту произведение двух первых (по модулю два).	$\|000\rangle \to \|000\rangle$ $\|001\rangle \to \|001\rangle$ $\|010\rangle \to \|010\rangle$ $\|011\rangle \to \|011\rangle$ $\|100\rangle \to \|100\rangle$ $\|101\rangle \to \|101\rangle$ $\|110\rangle \to \|111\rangle$ $\|111\rangle \to \|110\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$
Преобразование Адамара H:	$\|0\rangle \to \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $\|1\rangle \to \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

квантовым битом регистра; 2) инверсия относительно среднего. Это преобразование можно записать следующим образом:

$$\sum_i |t_i\rangle \to \sum_i (2a_{\text{ср}} - a_i)\,|t_i\rangle,$$

где $a_{\text{ср}}$ — средняя амплитуда.

Инверсию относительно среднего можно записать в виде матрицы

$$D = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{pmatrix}.$$

Как показал Л. Гровер в работе [2], это преобразование может быть эффективно реализовано на квантовом компьютере, а сложность всего алгоритма оценивается как $O\left(2^{n/2}\right)$.

Таким образом, появление квантовых компьютеров приведет к снижению эффективной длины ключа в два раза. Это говорит о том, что уже сейчас следует использовать симметричные шифры с длиной ключа не менее 256 битов.

Кроме того, аналогичный алгоритм может быть использован для взлома хэш-функций, в связи с чем следует использовать хэш-функции с длиной блока не менее 256 битов.

Криптостойкость системы RSA. Стойкость системы асимметричного шифрования RSA основывается на сверхполиномиальной вычислительной сложности факторизации натуральных чисел. Однако существует квантовый алгоритм, сложность которого полиномиальна.

Поставим задачу следующим образом: по натуральному числу N, имеющему ровно два простых делителя, найти эти делители. Заметим, что для некоторого числа a его порядок по модулю N (т.е. минимальное число r такое, что $a^r = 1 \pmod N$) четен. Тогда мы можем выражение $a^r = 1 \pmod N$ записать в виде

$$\left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right) = 0 \pmod N.$$

То есть, зная r, мы можем эффективно найти делители числа N. Заметим, что порядок r фактически является периодом функции $a^x \pmod N$.

Для нахождения периода функции существует следующий квантовый алгоритм.

Пусть у нас есть периодическая функция $f(x)$. Область определения и область значений этой функции — множество целых чисел, причем $0 \leqslant x \leqslant 2^n - 1$ и $0 \leqslant f(x) \leqslant 2^m - 1$. Для того, чтобы найти период этой функции, нам нужен квантовый регистр, состоящий из $n + m$ квантовых битов. Приведем его в состояние

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, 0\rangle.$$

Теперь вычислим от него функцию f, так чтобы у нас получилось состояние

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle.$$

Затем проведем измерение последних m квантовых битов (т.е. квантовых битов, относящихся к $f(x)$). После него наш квантовый регистр перейдет в состояние

$$\sum_{x:f(x)=u} |x, u\rangle.$$

Теперь проведем квантовое преобразование Фурье (алгоритм которого приведен ниже), в результате чего мы получим состояние

$$\sum_j c_j \left| j\frac{2^n}{r} \right\rangle,$$

где c_j равны нулю при всех j, не кратных $2^n/r$. Если период r не делит 2^n, преобразование выполняется не точно, причем бóльшая амплитуда сосредоточена вблизи целых значений, кратных $[2^n/r]$.

Наконец, измерим полученное состояние. Измерение даст число v.

Если период равняется степени двойки, то $v = j\frac{2^n}{r}$. А поскольку в большинстве случаев j и r взаимно просты, то сокращение дроби $\frac{v}{2^n}$ даст дробь, знаменатель которой и есть период. В общем случае либо придется прогнать весь алгоритм несколько раз, пока мы не получим правильное значение периода (ему соответствует максимальная амплитуда, а следовательно, максимальная вероятность), либо воспользоваться известным из теории чисел разложением в бесконечную дробь [6].

Квантовое преобразование Фурье определяется так:

$$U_{QFT}\left(|x\rangle\right) = \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} e^{\frac{2\pi i c x}{2^m}} |c\rangle.$$

Как показал П. Шор в работе [6], такое преобразование можно построить с использованием только $m(m+1)/2$ квантовых вентилей двух типов. Один из них представляет собой преобразование Адамара, примененное к j-му квантовому биту (обозначим его H_j). Другой вентиль реализует двухбитное преобразование вида

$$S_{j,k} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\frac{\pi}{2^{k-j}}} \end{pmatrix}.$$

Согласно работе [6], квантовое преобразование Фурье можно задать следующим образом:

$$H_0 S_{0,1} \ldots S_{0,m-1} H_1 \ldots H_{m-3} S_{m-3,m-2} S_{m-3,m-1} H_{m-2} S_{m-2,m-1} H_{m-1} = \\ = \prod_{k=0}^{m-1} H_k \prod_{t=k+1}^{m-1} S_{k,t}. \quad (1)$$

После этого преобразования следует изменить порядок битов на противоположный. Это можно сделать либо соответствующей квантовой схемой, либо, если сразу после квантового преобразования Фурье происходит измерение, классическим способом.

Рассмотренный квантовый алгоритм факторизации имеет сложность $O(n^3)$. В то же время, лучший классический алгоритм факторизации — алгоритм решета числового поля [4] — имеет сложность $O(\exp(c(\log n)^{1/3}(\log\log n)^{1/3}))$, где $c = \sqrt[3]{\frac{64}{9}}$.

Криптостойкость системы Эль-Гамаля. Система Эль-Гамаля основана на трудности вычисления дискретного логарифма, т.е., если g — образующий элемент конечной группы G, то зная $a \in G$, надо найти $r \in G$ такой, что $a = g^r$. Наиболее часто эта схема применяется для группы Z_p и для группы точек эллиптической кривой.

Существует квантовый алгоритм Шора для вычисления дискретного логарифма. Приведем здесь его оригинальную версию, которая предназначена для группы Z_p (где p — простое).

Сначала найдем q — степень двойки, чтобы $p < q < 2p$. Приведем квантовый регистр в состояние

$$\frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}\left|a, b, g^a x^{-b} \,(\mathrm{mod} p)\right\rangle. \tag{2}$$

Применим теперь преобразование Фурье к первой и второй частям регистра, в результате чего регистр перейдет в состояние

$$\frac{1}{q(p-1)}\sum_{c=0}^{q-1}\sum_{d=0}^{q-1} e^{\frac{2\pi i}{q}(ac+bd)}\left|c, d, g^a x^{-b} \,(\mathrm{mod} p)\right\rangle. \tag{3}$$

Теперь измеряем состояние квантового регистра. В результате измерения с вероятностью не менее $\frac{1}{480}$ мы получим c и d такие, что

$$-\frac{1}{2q} \leqslant \frac{d}{q} + r\left(\frac{c(p-1) - \{c(p-1)\}_q}{(p-1)q}\right) \leqslant \frac{1}{2q}(\mathrm{mod} 1), \tag{4}$$

где $\{x\}_q$ — число, удовлетворяющее соотношениям $\{x\}_q \equiv x \,(\mathrm{mod} q)$ и $-\frac{q}{2} < \{x\}_q \leqslant \frac{q}{2}$.

Для того чтобы получить кандидата на r, надо округлить $\frac{d}{q}$ до ближайшего числа, кратного $\frac{1}{p-1}$, затем разделить по модулю $p-1$ на $\frac{(p-1)c - \{(p-1)c\}_q}{q}$. В работе .[6] сложность этого алгоритма оценивается как $O(n^3)$. В то же время, лучший классический алгоритм для дискретного логарифма имеет сверхполиномиальную сложность.

Несмотря на то, что долгое время считалось, что алгоритм Шора не подходит для вычисления дискретного логарифма в группе точек эллиптической кривой, в работе [5] приводится вариант алгоритма Шора

для группы точек эллиптической кривой над полем GF(p), обладающий сложностью $O(n^3)$, а также высказывается гипотеза, что аналогичный алгоритм существует также и для эллиптических кривых над другими полями.

Заключение. Несмотря на большие успехи, которых достигла криптология, необходимо отметить, что появление действующих образцов квантовых компьютеров приведет к тому, что многие криптосистемы, прежде всего асимметричные, станут не стойкими, что приведет к невозможности безопасного предоставления многих услуг, в том числе интернет-банкинга и электронной торговли. Перестанут быть безопасными электронные подписи и схемы распределения ключей. Из этого следует, что необходимы новые асимметричные криптоалгоритмы.

СПИСОК ЛИТЕРАТУРЫ

1. Ключарев П. Г. Основы квантовых вычислений и квантовой криптографии // Вестник МГТУ им. Н.Э. Баумана. Серия "Приборостроение". – 2006. – № 2. – С. 36–46.
2. Grover L. K. Quantum Mechanics Help in Searching for a Needle in a Haystack. / Phys. Rev. Lett. – 1997. –V. 78(2). – P. 325–328.
3. Hankerson D. R., Vanstone S. A. & Menezes A. J. Guide to elliptic curve cryptography. – New York: Springer, 2003. – XX. – 311 p.
4. Pomerance C. A Tale of Two Sieves. / Not. Amer. Math. Soc., 1996. – P. 43.
5. Proos J. A. Shor's discrete logarithm quantum algorithm for elliptic curves. Waterloo, Ont.: Faculty of Mathematics University of Waterloo. 2003. – P. 35.
6. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. / Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.

Статья поступила в редакцию 27.12.2006

Петр Георгиевич Ключарёв родился в 1980 г., окончил МГТУ им. Н.Э. Баумана в 2004 г. Аспирант кафедры "Информационная безопасность". Автор шести научных работ в области информационной безопасности.

P.G. Klyucharyov (b. 1980) graduated from the Bauman Moscow State Technical University in 2004. Post-graduate of "Information Security" department of the Bauman Moscow State Technical University. Author of 6 publications in the field of information security.