МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Криптостойкость RSA, задача факторизации, квантовый компьютер

Чернышев М.Н.
гр. 016

2004 г.

Введение

Алгоритм RSA является самым распространенным алгоритмом шифрования с открытым ключом. Фирмой RSA Data Security, Inc. было продано около 450 миллионов лицензий на программный продукт, реализующий данный алгоритм. Его популярность вполне объяснима. С бурным развитием телекоммуникационных технологий возникла потребность в быстром и безопасном обмене данными. Симметричные системы шифрования плохо решали эти задачи из-за проблемы безопасной передачи ключей.

Впервые идея криптографии с открытым ключом была предложена в 1976 г У. Диффи (Whitefield Diffie) и М. Хеллманом (Martin Hellman). Основным тезисом их концепции было предложение использовать два типа ключей: ключи для шифрования и ключи для расшифрования. Причем ключ расшифрования нельзя найти по ключу шифрования.

С 1976 года было создано большое количество подобных алгоритмов. Многие из них оказались нестойкими, многие стойкие оказались труднореализуемыми из-за слишком большой длины ключа или криптотекста. И лишь очень небольшая часть алгоритмов оказались достаточно защищенными и пригодными для практической реализации. Как правило, эти алгоритмы основываются на решении трудных математических задач. В частности, в алгоритме RSA (Ron Rivest, Adi Shamir, Leonard Adleman) такой задачей является разложение больших чисел на простые множители.

В настоящее время алгоритм RSA применяется практически во всех программных продуктах, использующих передачу данных по незащищенным каналам связи. RSA является стандартом де-факто, принятым практически во всем мире. Поэтому вопрос стойкости данного алгоритма является очень актуальным. Открытие достаточно эффективных методов криптоанализа данного алгоритма повлечет за собой очень тяжелые последствия для телекоммуникационной индустрии, платежных систем, средств электронной коммерции и т.д.

Описание алгоритма RSA

Для генерации ключей (открытого и секретного) применяются два случайных простых числа p и q. Для обеспечения необходимой безопасности они должны быть достаточно большими и иметь равную длину. Затем рассчитывается произведение n=pq

После этого случайным образом выбирается число e, взаимно простое с (p-1)(q-1). Пара чисел e и n является открытым ключом (ключом шифрования). Теперь с помощью расширенного алгоритма Евклида вычисляется секретный ключ (ключ расшифрования) d, такой, что:

$$ed = 1(\mathrm{mod}(p-1)(q-1))$$

Для шифрования сообщение разбивается на цифровые блоки, размерами меньше n.
Криптотекст c будет состоять из блоков той же длины
Шифрование происходит по следующей формуле:

$$c_i = m_i^e \bmod n$$

Расшифровка происходит так:

$$m_i = c_i^d \bmod n$$

$$c_i^d \bmod n = m_i^{ed} \bmod n = m_i^{k(p-1)(q-1)+1} \bmod n =$$

$$= m_i m_i^{k(p-1)(q-1)} \bmod n = m_i \cdot 1 \bmod n = m_i$$

Стойкость алгоритма RSA.

До сих пор математически не доказано, что для восстановления m по e и n обязательно нужно раскладывать число n на множители. Но если будет открыт метод криптоанализа RSA, позволяющий получить d, то этот метод можно будет также

использовать для разложения на простые множители числа n. Такие алгоритмы в настоящее время не найдены. Существует несколько достаточно эффективных способов взлома, но они работают только при выборе определенных параметров n, e и d, а также при неосторожном обращении с секретными ключами. Грамотным выборов параметров и четкой системой использования секретных ключей эффективность подобного рода атак сводится к нулю. Таким образом, считается, что стойкость рассматриваемого алгоритма полностью зависит от трудоемкости разложения на множители больших чисел.

Задача факторизации.

Задача разложения на простые множители является одной из древнейшей задач теории чисел. Все существующие алгоритмы не очень сложны, но их выполнение занимает много времени. На настоящее время самым лучшим алгоритмом факторизации считается метод «Общее решето числового поля». Эвристическая оценка времени его выполнения такова:

$$e^{(1,923+o(1))(\ln(n))^{\frac{1}{3}}(\ln(\ln(n)))^{\frac{2}{3}}}$$

В таблице приведены рекорды разложения на множители чисел RSA-k. Каждое число RSA-k имеет k десятичных разрядов и состоит из двух близких простых множителей.

Число	Дата	Сложность, MIPS-лет	Алгоритм
RSA-100	Апрель 1991	7	Квадратичного решета
RSA-110	Апрель 1992	75	Квадратичного решета
RSA-120	Июнь 1993	830	Квадратичного решета
RSA-129	Апрель 1994	5000	Квадратичного решета
RSA-130	Апрель 1996	500	Обобщенного квадратичного решета
RSA-140	Февраль 1999	2000	Обобщенного квадратичного решета
RSA-155	Август 1999	8000	Обобщенного квадратичного решета

Данные о трудности проекта RSA – 140 позволяют спрогнозировать сложность разложения более длинных чисел:

Разрядность (бит)	512	768	1024
Сложность (относительно RSA-140)	6.5	$4 \bullet 10^4$	$49 \bullet 10^6$
Требуемая оперативная память (относительно RSA-140)	2.5	$2 \bullet 10^2$	$7 \bullet 10^3$

Таким образом, 512-битные ключи уже не обеспечивают хорошей защищенности (группа ученых за несколько месяцев, используя большой вычислительный кластер, потратив несколько миллионов долларов, могут вскрыть наше сообщение). Но вскрытие 1024-битных ключей все еще недоступно современной вычислительной технике. Дальнейшее развитие алгоритмов факторизации приведет, по видимому, к уменьшению константы 1,923 в показателе экспоненты сложности. При уменьшении этого показателя до 1,5 уже сегодня можно раскладывать на множители 1024-битные числа. Тем не менее из-за экспоненциальности сложности данной задачи стойкость можно обеспечить выбором достаточно длинного ключа. Современные алгоритмы позволяют эффективно получать простые числа практически любой длины (до миллиона десятичных разрядов).

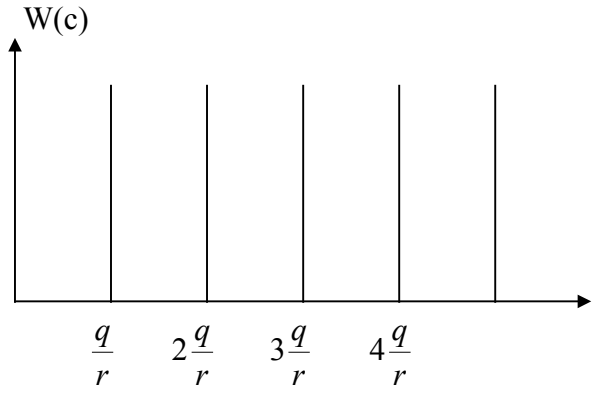
Квантовый компьютер.

Задача факторизации, вычислительно трудная для современной компьютерной техники, могла бы быть легко решена при использовании устройств, называемых квантовыми компьютерами. Кратко рассмотрим их устройство.

Память или регистры квантового компьютера, так же как и в случае обычного компьютера, состоят из двухуровневых ячеек. Простейшим примером такой квантовой ячейки является частица со спином $\frac{1}{2}$. Проекция спина на выбранное направление может принимать значения $-\frac{1}{2}$ и $\frac{1}{2}$. По аналогии с обычной классической ячейкой памяти обозначим одно из состояний нулем, а другое – единицей. Фундаментальным отличием квантовой ячейки от классической является то, что состояние квантовой ячейки является вероятностным. Это означает, что квантовая ячейка может принимать не только «чистые» состояния $|0>$ и $|1>$, но «смешанные» состояния $\psi = \alpha|0> + \beta|1>$, где $|\alpha|^2$ и $|\beta|^2$ определяют вероятность обнаружить систему в нулевом единичном состоянии соответственно. Таким образом, квантовый регистр, состоящий из L квантовых ячеек, имеет 2^L базисных состояний. Именно возможность принимать смешанные значения придает квантовому компьютеру его уникальные свойства.

Допустим, у нас есть квантовый регистр, находящийся в некотором состоянии, например, |10110001010010…> = |a>, состояния всех его бит являются чистыми. Осуществляя некоторую вычислительную процедуру $|a,0> \rightarrow |a,f(a)>$ над двумя регистрами, мы находим значение некой функции от содержимого рассматриваемого регистра. В этом случае квантовый компьютер ничем не отличается от классического и не проявляет своих уникальных свойств. Переведем теперь исходный регистр |a> в состояние, при котором каждый квантовый бит будет равновероятно принимать значения нуля и единицы, т.е. $\psi_1 = \frac{1}{\sqrt{2}}|0> + \frac{1}{\sqrt{2}}|1>$. При этом состояние всего регистра будет описываться следующим образом: $\psi = \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a>, \quad q = 2^L$. Проведя ту же самую вычислительную процедуру, на выходе мы получим уже значение функции для всевозможных значений входного аргумента: $\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a,0> \rightarrow \frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a,f(a)>$. Таким образом, за один такт работы квантовый компьютер параллельно выполняет экспоненциально большой объем вычислений.

В качестве примера использования квантового параллелизма рассмотрим задачу нахождения периода последовательности f(0), f(1), … , f(q-1). Для этого введем операцию квантового дискретного преобразования Фурье: $|a> \rightarrow \frac{1}{\sqrt{q}}\sum_{c=0}^{q-1} e^{2\pi i ac/q}|c,a>$. Проведя данное преобразование над суперпозицией $\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a,f(a)>$, получим: $\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a,f(a)> \rightarrow \frac{1}{q}\sum_{a=1}^{q-1}\sum_{c=0}^{q-1} e^{2\pi i ac/q}|c,f(a)>$. Пусть последовательность f(a) имеет период r, то есть f(a + r) = f(a), тогда при суммировании по a конструктивная интерференция происходит при условии, что $\frac{c}{q}$ кратно $\frac{1}{r}$. При всех других значениях $\frac{c}{q}$ происходит в большей или меньшей степени деструктивная интерференция. Таким образом, распределение вероятностей состояний регистра с будет носить следующий характер:



Одиночное вычисление и измерение с даст нам случайное значение, соответствующее одному из пиков максимума вероятности W(c). Таким образом, решение задачи нахождения периода последовательности носит вероятностный характер. Но ничто не мешает сделать эту вероятность сколь угодно близкой к единице.

При решении подобной задачи с помощью обычного компьютера, нам понадобилось бы вычислить, по крайней мере, r значений функции f. То есть, объем вычислений экспоненциально увеличивается при увеличении разрядности входных данных. При решении же данной задачи на квантовом компьютере разрядность входных данных слабо влияет на длительность вычислений (полиномиально).

Перейдем теперь к интересующей нас задаче факторизации чисел. Мы хотим факторизовать число N. Выберем некоторое число x, взаимно простое с N. Взаимную простоту можно установить с помощью достаточно эффективного алгоритма Евклида. Рассмотрим последовательность, образованную функцией $f(a) = x^a \bmod N$. Последовательности $\{x^a\}$ и $\{x^a (\bmod N)\}$ имеют следующий вид:

$\{x^a\} = \{1, x, ..., x^{r-1}, x^r, x^{r+1}, ...\}$

$\{x^a \bmod(N)\} = \{1, x, ..., x^{r-1}, 1, x, ..., x^{r-1}, 1, x, ...\}$

r-минимальная степень, для которой $x^r = 1 \bmod N$

Видно, что последовательность $\{x^a (\bmod N)\}$ имеет периодическую структуру. При использовании стандартных алгоритмов задача нахождения периода длинной последовательности является трудной. Но применив квантовый компьютер, мы можем достаточно быстро найти ее период r.

Далее подбираем такое значение x, что последовательность $\{x^a (\bmod N)\}$ имеет четный период r.

$x^r = 1 \bmod N;$

$(x^{r/2})^2 - 1 = 0 (\bmod N);$

$(x^{r/2} + 1)(x^{r/2} - 1) = 0 (\bmod N);$

Это означает, что произведение в левой части равенства кратно N, то есть одна из скобок должна иметь общий множитель с N. Для завершения факторизации вычислим НОД каждого из сомножителей с N (эта процедура достаточно эффективна). Найденный общий делитель и будет решением задачи.

В качестве примера реализации данного алгоритма разложим на множители число 133. Примем x=2 .

$\{2^a \bmod(133)\} = \{1,2,4,8,16,32,64,128,123,113,93,53,106,79,25,50,100,67,1,...\}$

Период последовательности r =18.

$(x^{r/2} + 1) = 513$

$(x^{r/2} - 1) = 511$

Находим НОД(513, 133):

$513 = 133 \bullet 3 + 114$

$133 = 114 \bullet 1 + 19$

$114 = 19 \bullet 6 + 0$

$НОД(513,133) = 19$

$133 \div 19 = 7 \Rightarrow 133 = 19 \bullet 7$

Таким образом, мы нашли делители исходного числа и тем самым, решили поставленную задачу.

Заключение

Уже доказано, что теоретических преград на пути конструирования квантового компьютера нет. Но технологически эта задача очень сложна. И трудности заключаются в чрезвычайной подверженности квантовых систем к внешнему воздействию. Достаточно всего мизерного нежелательного воздействия (поглощение одного кванта электромагнитного излучения или кратковременное включение сверхслабого магнитного поля), чтобы коренным образом исказить результаты вычислений. В настоящее время высшим результатом в этой области является создание 4-битного подобного устройства в исследовательской лаборатории компании IBM. Программирование устройства осуществлялось электромагнитными импульсами, а считывание данных ЯМР-сканером. Этот прототип квантового компьютера смог разложить на простые множители число 15. Но технологии не стоят на месте, и возможно, в скором будущем эти устройства станут достаточно совершенными, чтобы быстро решать задачу факторизации больших чисел.

Литература

1. Брюс Шнайер. «Прикладная криптография». М. «Издательство Триумф», 2003 г. Bruce Schneier «Applied Cryptography»
2. Харин Ю.С., Берник В.И, Матвеев Г.В., Агиевич С.В. «Математические и компьютерные основы криптологии». Минск, «Издательство «Белорусский Дом печати», 2003 г.
3. С. Браунштейн (Samuel L. Braunstein) «Квантовые вычисления: учебное руководство»
4. Л. Федичкин «Квантовые компьютеры» http://phys.web.ru/db/msg.html?mid=1168929&uri=page1.html