Эссе

Impact of Quantum Theory on Cryptography

Выполнил студент 916 группы
Шевченко Евгений

Введение

Технический прогресс не стоит на месте. И тем, что вчера казалось чудом сегодня уже мало кого удивишь. Однако научные открытия могут иметь кроме позитивных, ещё и негативные последствия. Одним из таких открытий является квантовый компьютер. С его помощью можно проводить вычисления, которые не реализуемы на сегодняшних (классических) компьютерах. Всё бы хорошо, но вот именно на вычислительной сложности основаны все основные системы шифрования, так широко используемые сегодня. В чём же основная идея квантового компьютера ?
В данном эссе я не буду уделять особого внимание принципам работы квантовых компьютеров , потому как у меня другая цель. В общих словах, всё выглядит примерно так.

Квантовый бит или кубит — это вектор единичной длины в 2-мерном комплексном векторном пространстве, в котором зафиксирован некоторый базис {|0>, |1>}. Ортонормированный базис |0> и |1> может соответствовать поляризациям фотона или состояниям «спин вверх», «спин вниз» электрона. Когда речь идёт о кубитах и квантовых вычислениях вообще, базис {|0>, |1>}, для которого проводятся все рассуждения, выбирается заранее. Мы будем далее считать, если особо не оговорено обратное, что этот базис одновременно является базисом измерения.
В квантовых вычислениях базисные состояния обозначаются |0> и |1>, чтобы «соответствовать» значениям классического бита 0 и 1. Но, в отличие от классического бита, кубиты могут находиться в суперпозиции |0> и |1>, например, a|0> + b|1>, где a и b — комплексные числа, такие что |a|^2 + |b|^2 = 1. В случае с поляризацией фотона, если такая суперпозиция измеряется в базисе {|0>, |1>}, то вероятность того, что измерение даст |0> равна |a|^2, а вероятность того, что измерение даст |1> — |b|^2.
Хотя квантовый бит может находиться в бесчисленном множестве суперпозиций состояний, путём измерения из него можно извлечь только один бит классической информации. Измерение кубита заменяет его состояние на базисное.
Существует набор, так называемых “квантовых вентилей” (аналоги логических AND NOT OR и так далее) при помощи которых организуются квантовые алгоритмы.
Мощность квантовых компьютеров объясняется ***квантовый параллелизмом***. Если мы применяем преобразование к суперпозиции исходных данных. Мы на выходе получаем суперпозицию результатов. Таким способом возможно вычислить *f(x)* для *n* значений аргумента *x* при однократном применении *Uf(преобразования)*.
Кроме того, как мы уже убедились, состояния кубита можно представить вектором в двумерном комплексном векторном пространстве, порождённом |0> и |1>. В классической физике возможные состояния системы из *n* частиц, в которой состояние каждой частицы задается вектором в 2-мерном пространстве, образуют 2*n-мерное векторное пространство. Однако, в квантовой системе общее пространство состояний гораздо больше: система из *n* кубитов имеет пространство состояний размерности 2^n. Именно этот экспоненциальный рост пространства состояний в зависимости от числа частиц даёт экспоненциальное преимущество в скорости вычислений на квантовых компьютерах в сравнении с классическими.

В 1994 году Питер Шор, вдохновленный работой Даниеля Саймона (опубликованной позже [Саймон 1997]), открыл ограниченно- вероятностный алгоритм разложения на множители n-разрядных чисел за полиномиальное время на квантовом компьютере. Начиная с семидесятых, люди ищут эффективные алгоритмы для разложения целых чисел. Наиболее эффективным классическим алгоритмом, известным на сегодняшний день, является алгоритм Ленстра и Ленстра [Ленстра и Ленстра 1993], который экспоненциален по размеру входа. Вход — это набор цифр числа M, имеющий размер

n ~ logM. Люди были настолько уверены в том, что эффективного алгоритма разложения не существует, что были созданы криптографические системы, например RSA, которые опираются на сложность этой проблемы. Результат Шора был ошеломляющим для большинства учёных, побудив их к широкомасштабным исследованиям в области квантовых вычислений.
При разбиении больших чисел на множители с помощью обычного компьютера добавление каждого разряда практически приводит к удвоению времени, которое необходимо на нахождение множителей. В отличие от этого, при использовании для решения этой задачи квантового компьютера, с добавлением еще одного разряда время возрастает лишь на постоянную величину.

Алгоритм Шора

В большинстве алгоритмов, включая алгоритм Шора, используется стандартный способ ведения задачи разложения к задаче поиска периода функции. Шор использует квантовый параллелизм для получения суперпозиции всех значений функции за один шаг. Затем он производит квантовое преобразование Фурье, результатом которого, как для классического преобразовании Фурье, является функция, аргумент которой кратен величине, обратной периоду. С высокой вероятностью измерение состояния возвращает период, который в свою очередь, служит для разложения целого числа M. Все что было сказано выше, раскрывает суть квантового алгоритма, но в очень упрощённом виде. Наибольшая трудность заключается в том, что квантовое преобразование Фурье основано на быстром преобразовании Фурье и, таким образом, дает только приблизительный результат в большинстве случаев.

Для начала мы опишем квантовое преобразование Фурье, а затем дадим подробное описание алгоритма Шора.

Квантовое преобразование Фурье

В общем случае преобразования Фурье переносят данные из временной в частотную область. Так, преобразования Фурье преобразуют функции с периодом r в функции, у которых значения, отличные от нуля, появляются только в значениях кратных частоте Дискретное преобразование Фурье (DFT,ДПФ) действует на N равноудаленных выборок в полуинтервале [0, 2П) для некоторого N, и выдает функцию, чья область определения — это целые числа от 0 до N-1. Дискретное преобразование Фурье функции периода r- это функция, сконцентрированная около значений, кратных N/r. Если период r делит N без остатка, то результатом будет функция, у которой значения, отличные от нуля, имеются только в точках, кратных N/r. В противном случае результат будет приближённым, и отличные от нуля члены появятся в числах, близких к кратным N/r.

Быстрое преобразование Фурье (FFT,БПФ) является разновидностью DFT, где N - степень двойки. Квантовое преобразование Фурье (QFT, КПФ) является вариантом DFT, где, также, как и в FFT, используются степени двойки. Квантовое преобразование Фурье действует на амплитуды квантового состояния, как:

$$\sum_x g(x)|x\rangle \to \sum_c G(c)|c\rangle,$$

где G(c) — это дискретное преобразование Фурье g(x), а x и c варьируются, как целые числа от 0 до N - 1 (в двоичном представлении). Если бы состояние измерили после того, как преобразование Фурье выполнено, то вероятность того, что результат |c), была бы |G(c)|^2.

Применяя квантовое преобразование Фурье к периодической функции g(x) с периодом r, мы предполагали закончить с

$\sum_c G(c)|c\rangle$, где $G(c)$
, где G(c) равно нулю везде кроме значений, кратных N/r. Таким образом, когда состояние измерено, результатом являются значения, кратные N/r, например j*N/r . Но, как уже было замечено выше, квантовые преобразования Фурье дают лишь приблизительный результат для периодов, которые не являются степенью двух, т.е. периодов, которые не делят N. Однако чем больше степень двойки, использована в качестве базы преобразования, тем точнее аппроксимация. Квантовое преобразование Фурье Uqft с базой N = 2^m определяется как

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

Для того, чтобы алгоритм Шора был полиномиальным, необходимо чтобы квантовое преобразование Фурье вычислялось эффективно. Шор показывает, что квантовое преобразование Фурье с базой 2^m можно построить с использованием только (m+1)*m/2 преобразований. Это построение использует 2 типа вентилей. Один — для реализации преобразования Адамара H:

$$H : |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

(через Hj обозначим преобразование Адамара, применяемое к j-му биту), другой — для реализации двубитного преобразования вида

$$S_{j,k} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta_{k-j}} \end{pmatrix},$$

где $\theta_{k-j} = \pi/2^{k-j}$ Это преобразование воздействует на k-ый и j-ный биты большого регистра. Квантовое преобразование Фурье задается выражением

$H_0 S_{0,1} \ldots S_{0,m-1} H_1 \ldots H_{m-3} S_{m-3,m-2} S_{m-3,m-1} H_{m-2} S_{m-2,m-1} H_{m-1},$

за которым следует обращение битов. Если за FFT следует измерение, как в алгоритме Шора, то обращение битов выполняется классическим способом. Все детали выполнения алгоритма можно найти в работе автора алгоритма [Шор 1997].

Подробности алгоритма Шора

Последовательные шаги алгоритма Шора детально представлены в нижеследующем примере, где мы разлагаем на множители число M = 21.

Шаг 1. **Квантовый параллелизм**. Произвольно выбираем число **a**. Если **a** не является взаимно простым с **M**, то значит мы уже нашли делиттель **M**. В противном случае применяем оставшуюся часть алгоритма.

Пусть m будет таким, что M^2<=2^m <= 2M^2 . Этот выбор был сделан таким образом, чтобы аппроксимации, применяемой в шаге 3 для функций, чей период не является степенью двойки, будет вполне достаточно, чтобы оставшаяся часть алгоритма работала. Используем квантовый параллелизм для вычисления f(x)= a^x mod M для всех целых чисел от 0 до 2^m - 1. Получим, таким образом

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

ПРИМЕР. Предположим a = 11 было выбрано случайно. Т.к. M^2 = =441 <= 2^9 < 882 = 2*M^2, то мы находим m = 9. Таким образом, всего 14 кубитов, 9 для x и 5 для f(x), требуются для вычисления суперпозиции.

Шаг 2. **Состояние, чья амплитуда имеет тот же период, что и f**. Квантовое преобразование Фурье воздействует на функцию амплитуды, связанной с входным состоянием. Чтобы использовать квантовое преобразование Фурье для получения периода функции f, необходимо составить состояние, чья функция амплитуды имеет тот же период, что и f.

Для составления такого состояния, измеряем последние [log2 M] кубиты состояния (*), которые относятся к f(x). Получаем случайное значение **u**. Само по себе значение **u** никакого интереса не представляет; нас интересует только воздействие измерения на наше множество суперпозиций. Это измерение проектирует пространство состояний на подпространство данной измеренной величины, поэтому состояние после измерения становится

$$C\sum_x g(x)|x, u\rangle,$$

с точностью до некоторого множителя C, где

$$g(x) = \begin{cases} 1, & \text{если } f(x) = u, \\ 0, & \text{в противном случае.} \end{cases}$$

Отметим, что иксы, которые появились в сумме, те, что с g(x)!=0, отличаются от друг от друга числом, кратным периоду, следовательно, g(x) это и есть та функция, которую мы ищем. Если бы мы могли измерить два полученных икса в сумме, мы могли бы иметь период. Но к сожалению, законы квантовой физики позволяют нам провести только одно измерение.

ПРИМЕР. Предположим, что случайное измерение суперпозиции уравнения (*) выдает 8. Состояние после этого измерения (На рисунке представлено только 9 битов; биты f(x) известны из измерения) ясно демонстрирует нам периодичность **f**.

Шаг 3. **Применение квантового преобразования Фурье.** Часть состояния |u> больше использоваться не будет, поэтому мы ее не записываем. Применим квантовое преобразование Фурье к состоянию, полученному на шаге 2.

$$U_{QFT} : \sum_x g(x)|x\rangle \to \sum_c G(c)|c\rangle$$

Из стандартного анализа Фурье получаем, что, когда период **r** функции **g(x),** определенной в шаге 2, есть степень двойки, то результат квантового преобразования Фурье есть

$$\sum_j c_j |j\frac{2^m}{r}\rangle,$$

где амплитуда равна нулю, кроме точек, кратных 2m/r. Когда период r не делит 2^m , преобразование выполняется точно, причём большая амплитуда сосредоточена в близи целых значений, кратных 2^m/r.

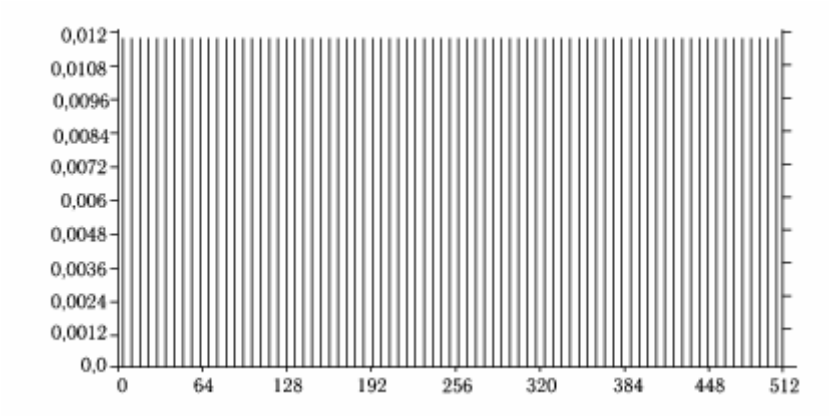

рис.2

Вероятности для различных x при измерении состояния $C \sum_{x \in X} |x, 8\rangle$ полученного в шаге 2, где $X = \{x | 211^x \mod 21 = 8\}\}$

Распределение вероятности квантового состояния после преобразования Фурье.

ПРИМЕР. На рисунке 2 отображён результат применения квантового преобразования Фурье к состоянию, полученному в шаге 2. Необходимо отметить, что рисунок 2 - это график Быстрого Преобразования Фурье функции, показанной на рисунке 1. В этом частном случае период функции f не делит 2^m.

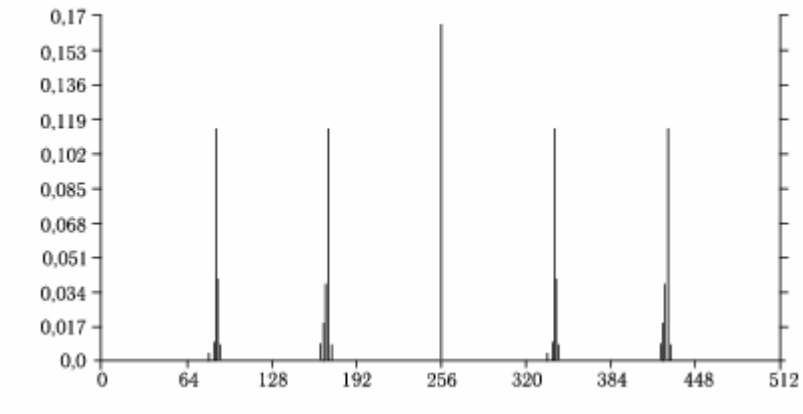

рис 2

Шаг 4- **Извлечение периода.** Измеряем состояния в стандартном базисе и получаем результат v. В случае, когда период является степенью двойки, квантовое преобразование дает точные значения, кратные 2m/r, и извлечь период не сложно. В этом случае v = j*(2^m)/r - для некоторого j. В большинстве случаев j и r будут взаимно просты, и в этом случае сокращение дроби v/(2^m)(= j/r) даст дробь, чей знаменатель q есть период r. Дело в том, что в общем случае квантовое преобразование Фурье даёт кратные значения основной частоты только приблизительно, что усложняет выяснение периода по результату измерения. Когда период не является степенью двойки, может быть получена хорошая оценка периода, если использовать так называемое разложение в бесконечную дробь v/(2^m).

ПРИМЕР. Допустим, что измерение состояния даёт величину v = 427. Поскольку v и 2^m взаимно просты, период **r** скорее всего не будет делить 2^m и поэтому можно применить разложение в бесконечную дробь. Следующая таблица прослеживает алгоритм, разложения.

i	a_i	p_i	q_i	ε_i
0	0	0	1	0.8339844
1	1	1	1	0.1990632
2	5	5	6	0.02352941
3	42	211	253	0.5

который заканчивается числом 6 = q2 < M <=q3. Таким образом, q = 6 наверняка является период функции **f**.

Шаг 5. **Нахождение делителя M**. Когда полученный период q чётный, используем алгоритм Евклида для эффективной проверки, имеют ли a^(q/2)+1 или a^(q/2)-1 отличный от единицы общий делитель с M. Причина, по которой a^(q/2)+1 или a^(q/2)-1 могут иметь общий отличный от единицы делитель с M следующая. Если q действительно является периодом функции f(x) = a^x mod M, то a^q = 1 mod M, поскольку a^q*a^x = a^x для всех x. Если q - четно, мы можем записать

$$(a^{q/2}+1)(a^{q/2}-1) = 0 \mod M.$$

Следовательно, поскольку ни a^(q/2)+1 ни a^(q/2)-1 не являются кратными значениями M, a^(q/2)+1 или a^(q/2)-1 имеют отличный от единицы общий с M делитель.

ПРИМЕР. Поскольку 6 чётное число, то либо a^(6/2) - 1 =1330, либо a^(6/2)+1= 1332 будут иметь общий с M делитель. В этом частном примере мы находим два делителя НОД(21,1330)=7 и НОД(21,1332)=3.

Шаг 6. **При необходимости повторяем алгоритм**. Некоторые действия могут выполняться неточно, поэтому процесс может не дать делитель M:

(1) Значение v не достаточно близко к кратному (2^m)/r

(2) Период r и сомножитель j могут иметь общий множитель, а при этом знаменатель q является делителем периода, а не самим периодом.

(3) Шаг 5 выдаёт M, как делитель M.

(4) Период функции f(x) = a^x mod M является нечётным.

Шор показал, что небольшое число повторений алгоритма дает множитель M с высокой вероятностью.

Комментарий к шагу 2 алгоритма Шора.

Оказывается, измерения на шаге 2 можно полностью опустить. Бернштейн и Вазирани [Бернштейн и Вазирани 1997] показали, что измерений в середине алгоритма можно всегда избежать. Если исключить измерение на шаге 2, то состояние будет состоять из суперпозиций нескольких периодических функций. Каждая из них имеет один и тот же период. Вследствие линейности квантовых алгоритмов, применяемое квантовое преобразование Фурье приводит к суперпозиции преобразований Фурье этих функций. Каждое из этих преобразований запутано с соответствующим **u** и, следовательно, они не интерферируют друг с другом. Измерение дает значение одного из этих преобразований. Понимание того, как это утверждение можно обобщить, иллюстрирует некоторые тонкости работы с квантовыми суперпозициями. Применим тензорное произведение квантового преобразования

2ге-1

Фурье и оператора идентичности, $U_{QFT} \otimes I$, к $C \sum_{x=0}^{2^n-1} |x, f(x)\rangle$ получив

$$C' \sum_{x=0}^{2^n-1} \sum_{c=0}^{2^m-1} e^{\frac{2\pi i x c}{2^m}} |c, f(x)\rangle,$$

что равно

$$C' \sum_{u} \sum_{x|f(x)=u} \sum_{c} e^{\frac{2\pi i x c}{2^m}} |c, u\rangle \qquad (**)$$

для **u** в диапазоне f(x). То, что получилось, есть суперпозиция результатов, полученных в шаге 3, для всех возможных **u**. Квантовое преобразование Фурье применяют к семейству отдельных функций g_u, индексируемых по u, где

$$g_u = \begin{cases} 1, & \text{если } f(x) = u, \\ 0, & \text{в противном случае,} \end{cases}$$

причём у всех одинаковый период. Необходимо отметить, что амплитуды в состояниях с различными **u** никогда не интерферируют (складываются или взаимоуничтожаются) друг с другом. Преобразование $U_{QFT} \otimes I$ можно записать как

$$U_{QFT} \otimes I : C \sum_{u \in R} \sum_{x=0}^{2^n-1} g_u(x)|x, f(x)\rangle \to C' \sum_{u \in R} \sum_{x=0}^{2^n-1} \sum_{c=0}^{2^n-1} G_u(c)|c, u\rangle,$$

где $G_u(c)$ — это дискретное преобразование Фурье $g_u(x)$, а R - диапазон f(x).
Измеряем с и повторяем шаги 4 и 5 как прежде.

Заключение

Как видно, с появлением квантовых компьютеров современную криптографию ожидают большие изменения. Конечно, это будет большой удар по классической криптографии. Но уже сейчас существуют квантовые криптоалгоритмы. Которые на порядок надёжнее сегодняшних, и основаны не на математической сложности, а на физических свойствах системы. Основами для этих алгоритмов служит *теорема неклонируемости*
Неизвестное квантовое состояние не может быть клонировано.
Эта теорема говорит о том, что нельзя получить точные копии квантового состояния до тех пор, пока оно не определено (т. е. пока не получена классическая информация, характеризующая данное состояние).
Доказательство:
Для получения копии квантового состояния |a> необходимо подвергнуть пару квантовых систем эволюции, описываемой как: U(|a>|0>) = |a>|a>, где U - унитарный оператор эволюции. Если это условие выполняется для любого состояния, то оператор U не должен зависеть от a и, следовательно, U(|b>|0>) = |b>|b> для |b> != |a>. Однако для состояния |c> = (|a> + |b>)/($2^{1/2}$) получим U(|c>|0>) = (|a>|a> + |b>|b>)/($2^{1/2}$) != |c>|c>, а следовательно, операция клонирования не выполняется. Этот вывод применим к любому предложенному методу клонирования (Wooters and Zurek 1982, Dieks 1982).
Так же эти алгоритмы базируются на **Парадоксе Эйнштейна-Подольского-Розена (EPR)**.

Но, пожалуй, самым важным вопросом остаётся создание квантового компьютера. Существует большое множество предложений по созданию такого компьютера с использованием ионных ловушек, ядерного магнитного резонанса (ЯМР), оптики и твёрдого тела. Все текущие предложения сводятся к решению проблемы увеличения числа кубитов. Необходим качественно новый уровень вычислений, чтобы обрабатывать не десятки, а сотни кубитов информации.
На сегодняшний день технологии с использованием ЯМР и ионных ловушек являются наиболее разрабатываемыми, однако использование оптики и твёрдого тела также подаёт надежды.
В квантовых компьютерах с ионной ловушкой [Ширак и Золлер 1995; Стин 1996] линейная последовательность ионов, представляющих кубиты, ограничена электрическим полем. Для того, чтобы произвести однокубитовые квантовые операции, лазеры направляются на отдельные ионы. Двухкубитовые операции осуществляются при использовании лазера, направленного на отдельный кубит для создания колебания, которое распространяется по цепи ионов до второго кубита, где другой лазер останавливает движение и завершает двухкубитовую операцию. При данном методе требуется, чтобы ионы находились в предельно чистом вакууме при максимально низких температурах.

Преимущество метода использования ЯМР заключается в том, что его можно применять при комнатной температуре. Тем более, что технология ЯМР в целом уже добилась некоторого успеха. Суть метода в том, чтобы использовать макроскопическое количество материи и закодировать квантовый бит в среднем состоянии спина большего количества ядер. Состояниями спина можно управлять посредством магнитных полей, а среднее состояние спина можно измерить при помощи техники ЯМР. Основная проблема при использовании этого метода заключается в трудностях при увеличении квантового регистра. Мощность измеряемого сигнала падает как 1/(2^n), где n — число кубитов. Однако, недавнее предложение [Шульман и Визарини (1998)] вероятно сможет разрешить эту проблему. Не так давно было успешно завершено создание трёхкубитового ЯМР компьютера [Корни и др. 1998; Вандерзипен и др. 1999; Гершенфельд и Чуанг 1997; Лафлам и др. 1997]. Основной проблемой при создании квантового компьютера является отсутствие когерентности и разрушение квантового состояния из-за взаимодействия с окружающей средой. Некоторое время существовали опасения, что квантовый компьютер нельзя будет создать, т. к. изолировать его от внешней среды не представляется возможным. Решение этой проблемы пришло скорее с алгоритмической, чем с физической стороны: были придуманы приёмы квантовой коррекции ошибок. Сначала учёные думали, что квантовая коррекция ошибок будет неосуществима из-за невозможности надёжного копирования неизвестных квантовых состояний. Но, оказывается, вполне возможно разработать коды, которые обнаруживают определённые виды ошибок и в состоянии восстановить когерентное квантовое состояние.

На сегодняшний день есть конкретные результаты. Так IBM продемонстрировала использование созданного в лабораториях компании семикубитового квантового компьютера для факторизации чисел по алгоритму Шора. Хотя решённая им задача вряд ли способна поразить воображение (компьютер верно определил, что делителями числа 15 являются числа 5 и 3), это самое сложное вычисление за всю историю квантовых компьютеров.
Химики IBM изобрели и создали новую молекулу, которая имеет семь ядерных спинов – молекулу, состоящую из пяти атомов фтора и двух атомов углерода. Эти атомы могут взаимодействовать между собой как кубиты, их можно программировать при помощи радиочастотных импульсов, а также определять их состояние посредством инструментов по измерению ядерного магнитного резонанса (NMR) – подобные инструменты широко используются в госпиталях и химических лабораториях.
Ученые IBM получили целую пробирку (миллиард миллиардов – 1018) таких молекул. В результате они смогли реализовать алгоритм Шора и правильно определить 3 и 5 как множители 15.

Литература:

1. **Э. Риффель, В. Полак "Основы квантовых вычислений" // "Квантовый компьютер и квантовые вычисления", т. 1, № 1, 2000**
2. http://www.qubit.org/
3. http://www.milketoast.com/school/cryptanalysis.htm
4. Polynomial-Time Algorithms For Prime Factorization and Discrete Logorithms on a Quantum Computer - P. Shor