Квантовые вычисления и их возможное влияние на алгоритмы шифрования

А.В. Коренюшкин

24 апреля 2007 г.

Эссе по курсу "Защита информации", кафедра радиотехники,
Московский физико-технический институт (ГУ МФТИ),
http://www.re.mipt.ru/infsec

1 Введение

В данном эссе рассматриваются основные принципы квантовых вычислений, а также их возможные приложения к криптографическим задачам и возможное влияние на существующие криптотехнологии.

Под квантовыми вычислениями (КВ) понимается особая модель вычислений, базирующаяся на принципах квантовой механики. Эта модель оперирует не с классической информацией, известной из теории Шеннона, но с принципиально иным объектом, квантовой информацией (КИ), которая может переводиться в классическую, однако не сводима к ней. То есть квантовую систему, несущую какое-то количество КИ, не возможно эквивалентно смоделировать классической системой. Именно этот факт и заставил исследователей обратить свои взоры на данный предмет, т.к. исследование таких систем может открыть принципиально иные, невыразимые в терминах теории информации и классической физики закономерности.

Первым идею гипотетической возможности КВ высказал Ричард Фейнман в [2]. Мне кажется, что при этом он руководствовался мантрой Норберта Винера «лучшей моделью кошки будет другая кошка, однако предпочтительнее, чтобы это была та же самая кошка», т.к. фактически Фейнман в этой статье развил сле-

дующую идею. Раз квантовые системы так плохо моделируются на классических компьютерах, нужно создать другой вычислитель, который будет их моделировать хорошо. И таким вычислителем будет другая квантовая система, ведь у нее нет иного выбора, как подчиняться квантовомеханическим закономерностям, а следовательно, и моделировать их.

Более строгое и формальное исследование КВ не заставило себя ждать. За работой Фейнмана последовали исследования других авторов. Была даже высказана идея о принципиальной возможности описания природных систем с помощью универсальных моделей, полученная как обобщение известного в теории алгоритмов тезиса Черча–Тьюринга и превратившаяся уже в «закон Черча–Тьюринга», который предлагается добавать к основым постулатам квантовой механики, рассматривать как ее фундамент:

> Изменение любой реальной конечной физической системы может быть как угодно точно сымитировано на вычислительной машине, работающей с универсальными моделями, за конечное число шагов.

Однако если возможности КВ для моделирования квантовых системы были очевидны a priori, если не сказать по определению, то их отличие от классических алгоритмов в решении других математических задач было осознано далеко не сразу. Первым были алгоритмы Дойча (1985) и Дойча-Джоза (1992) (последний – обобщение первого). Они решали за полиномиальное время чисто формальные, оторванные от каких-либо приложений задачи, на которые классическому компьютеру требовалось экспоненциальное время. И настоящим прорывом в области КВ были алгоритмы Питера Шора [3] (1994) факторизации и дискретного логарифмирования, справлявшиеся с этими задачами также за полиномиальное время! Надо ли говорить, что на вычислительной сложности этих задач базируются современные алгоритмы несимметричного шифрования (например, RSA и Эль Гамаля) и цифровой подписи (например, Эль Гамаля). Создание системы, способной быстро решать эти задачи неминуемо сделает данные алгоритмы непригодными для использования.

Однако в данный момент специалисты воздерживаются от оптимистических прогнозов по поводу скорого создания устройства, реализующего КВ, квантового компьютера (КК). Поэтому

пользователи упомянутых систем пока могут спать спокойно. К тому же в перспективе использование КИ для реализации передачи ключа с помощью квантовой криптографии, гарантирующей невозможность его перехвата, может избавить от необходимости использования алгоритмов несимметричного шифрования.

2 Физические основы квантовых вычислений

Идея КВ базируется на принципах квантовой механики. Существуют разные подходы к их формулированию, ниже представлен один из них:

1. Состояние изолированной системы Q выражается посредством вектора $|\psi\rangle$ в гильбертовом пространстве.
2. Такие переменные, как положение и импульс называются наблюдаемыми величинами и представляются посредством эрмитовых операторов.
3. Вектор состояния подчиняется уравнению Шредингера.
4. Постулат об измерениях.

Интерпретации последнего постулата разнятся, физики пока не пришли по нему к общему мнению, однако в большинстве случаев его можно выразить так: некоторые физические взаимодействия в системе распознаются как «измерения», и их суть заключается в том, что они переводят вектор состояния в собственное состояние измеряемой переменной $|k\rangle$, причем выбор k случаен с вероятностью $p \propto |\langle k|\psi\rangle|$.

Также важным в контексте КВ является парадок Эйнштейна-Подольского-Розена (ЭПР), заключающийся в следующем (из Wikipedia):

> Допустим, две одинаковые частицы A и B образовались в результате распада третьей частицы C. В этом случае, по закону сохранения импульса, их суммарный импульс должен быть равен исходному импульсу третьей частицы, то есть, импульсы двух частиц должны быть связаны. Это дачт нам возможность измерить импульс

> одной частицы и по закону сохранения импульса рассчитать импульс второй, не внося в еч движение никаких возмущений. Поэтому, измерив координату второй частицы, мы сумеем получить для этой частицы значения двух неизмеримых одновременно величин, что по законам квантовой механики невозможно.

Ответ на этот выпад сейчас примерно следующий: меряя импульс одной частицы мы необходимо вносим неопределенность в координату обоих частиц, как бы далеко они не находились, поэтому соотношение неопределенностей выполняется. Однако это на первый взгляд противоречит специальной теории относительности: нечто очень похожее на взаимодействие передается не со скоростью света, а мгновенно! Например, гипотетически можно реализовать систему, генерирующую в отстоящих друг от друга точках случайные последовательности со 100% корелляцией. Это можно представить себе так: Алиса и Боб научились подкидывать монетку так, что у обоих всегда выпадает одно, т.е. либо два орла, либо две решки. Затем они разъезжаются в разные концы страны (Земли, Солнечной системы, галактики...) и начинают вот так вот подкидывать монетки. Заметим, что передать с их помощью классическую информацию невозможно, однако при этом их подкидывания каким-то образом «синхронизированы»! Именно этот псевдотупик и привел исследователей к введению понятия КИ.

3 Квантовая информация

Рассмотрим квантовую систему с двумя состояниями (спин). Ее особенности таковы: она описывается волновой функцией (вектором в гильбертовом пространстве) $a|0\rangle+b|1\rangle$, поэтому хранит в себе бесконечное кол-во классической информации ($a, b \in R$), но при этом число возможных результатов измерения — лишь два. После долгих попыток описать такой феномен с позиций теории информации, исследователи наконец пришли к радикальном решению и стали рассматривать концепцию КИ, элементарной единицей которой является кубит – КИ, заключенная в квантовой системе с двумя состояниями. Конечно, при этом были доказаны некоторые свойства, подтверждающие корректность

такого определения и позволяющие такой величине носить гордое имя информации. А именно, для любой квантовой системы существует неким образом минимальная по количеству система кубитов, эквивалентно моделирующая ее. Количество этих самых кубитов — это и есть количество КИ, заключенной в системе.

С математической точки зрения квантовая система содержит n кубитов, если она содержит 2^n мерное гильбертово пространство. При этом она обладает 2^n взаимно ортогональными состояниями.

По аналогии с логическим гейтами были введены квантовые гейты — унитарные операции над кубитами. Также как и любая логическая функция n переменных может быть представлена как комбинация конечного числа, например, функций И-НЕ от пар переменных, так и любой квантовый гейт может быть представлен в виде комбинации гейтов из некого множества универсальных квантовых гейтов. Такие множества известны и применяются в разработке квантовых алгоритмов, которые обычно представляются в виде сетевой модели, показывающей последовательное и параллельное применение квантовых гейтов к тем или иным парам кубитов.

Из особенностей КИ хотелось бы отметить доказанную невозможность клонирования состояния кубита без необходимого разрушения этого состояния. Однако мы можем сделать это с разрушение, что называется квантовой телепортацией, которая происходит мгновенно, т.е. с бесконечной скоростью.

4 Квантовая криптография

Темой, сильно кореллирующей с топиком данного эссе, является квантовая криптография. Это механизм передачи ключа, гарантирующий невозможность его перехвата третьей стороной. Механизм весьма тривиален в теории. Рассмотрим Алису и Боба. Алиса хочет иметь ключ такой, чтобы кроме нее и Боба его никто не знал. Тогда она начинает генерировать кубиты в следующих состояниях $|0\rangle$ и $|1\rangle$, $|+\rangle$ и $|-\rangle$, где $|+\rangle = |0\rangle + |1\rangle$ и $|-\rangle = |0\rangle - |1\rangle$ (нормировочные коэффициенты опущены). Данные состояния образуют два базиса $\{|0\rangle, |1\rangle\}$ и $\{|+\rangle, |-\rangle\}$. Выбор того или иного базиса делается случайно. Боб, получая кубиты,

измеряет их по одному из базисов, выбирая их также случайно. После передачи оба публикуют протоколы выбора базисов, в которых в среднем совпадут $N/2$ записей из N. Предположим злоумышленник присоединился к каналу и прослушивает его. Но что значит прослушивать такой канал? Это значит, что он измеряет кубиты по одному из базисов. Но ведь он не знает, по какому базису будет отправлен следующий кубит, поэтому в половине случаев ошибется с выбором базиса, что приведет к тому, что Боб, угадав базис Алисы, в вероятностью $1/2$ измерит неправильное значение кубита из-за промежуточного измерения, сделанного злоумышленником. Поэтому для проверки секретности передачи Бобу с Алисой достаточно опубликовать и сверить половину из кубитов, для которых у них совпал базис. В случае отсутствия различий, они могу быть совершенно уверенными в секретности передачи и использовать оставшиеся $N/4$ кубитов, переведенных в обычные биты, в качестве ключа.

Конечно, все так просто только в теории, а на практике невозможно добиться передачи кубитов без искажений, поэтому помехи будут возникать и без участия злоумышленника. Однако эти трудности были успешно преодолены и коммерческие системы, работающие на принципах квантовой криптографии, уже в продаже.

5 Универсальный квантовый компьютер

Итак, квантовый компьютер. Согласно [1] это:

> Квантовый компьютер представляет множество, состоящее из n кубитов, для которого практически определены следующие операции:
>
> 1. Каждый кубит может быть представлен в какомлибо известном состоянии $|0\rangle$.
> 2. Каждый кубит может быть измерен по базису $\{|0\rangle, |1\rangle\}$.
> 3. Универсальный квантовый гейт (или множество гейтов) может воздействовать на любое ограниченное подмножество кубитов.
> 4. Состояние кубитов не изменяется кроме как посредством выше- вышеуказанных преобразований.

И такая штука сможет моделировать любую квантовую систему, воплощая «закон Черча-Тьюринга» в жизнь, лишь бы кубитов было достаточно, а именно с этим сейчас проблемы. Самый «многокубитовый» КК был сделан IBM в 2001 году, он состоял из 7 кубитов. Его работа была продемонстрирована успешным разложением числа 15 на простые множители по алгоритму Шора.

Создание же более мощного КК пока наталкивается на технические трудности. Если, конечно, не считать канадской компании D-Wave, уже создавшей 16-кубитовый процессой Orion и собирающейся наращивать мощности буквально стахановскими темпами: даешь 1024-кубитовый КК в 2008 году! На сайте компании http://www.dwavesys.com/ можно найти обещания быстрого (правда, приближенного) решения ни много, ни мало NP-полных задач! Единственным недостатком этого предприятия является то, что оно происходит в обстановке строгой секретности, никто из мировых специалистов по КК «в живую» Orion'а не видел, а поэтому все они выражают очень сильное сомнение в его работоспособности. Что ж, так это или нет, покажет время.

6 Квантовые алгоритмы

Как уже было отмечено выше, первым и на данный момент самым ярким прорывом в области создания алгоритмов для КК были алгоритмы Шора факторизации и дискретного логарифмирования. Оба они работают за полиномиальное от входных данных число шагов, точнее говоря, их время работы пропорционально кубу логарифма числа. Что делает возможным решение этих задач для огромных по сегодняшним меркам чисел.

Также нельзя не отметить алгоритм Гровера поиска в неупорядоченной базе данных. Он позволяет осуществлять его за время $O(\sqrt{N})$, где N – количество элементов, против $O(N)$ у классического компьютера. Это может снизить сложность решения полным перебором задач класса NP: эти задачи допускают проверку правильности решения за полиномиальное время, а перебор всех вариантов решения фактически и является поиском в неупорядоченной базе данных. Поэтому алгоритм Гровера позволяет несколько снизить сложность, но при этом экспоненциальный характер асимптотики никуда не денется, поэтому прак-

тическая ценность такого ускорения представляется весьма небольшой.

Однако даже кроме того, что пока этим алгоритмам не на чем работать, в данной области есть немало проблем. Во-первых, гипотоетическое применение КК пока ограничивается вышеописанными алгоритмами и моделированием квантовых систем, больше прорывов в этой области не было. Во-вторых, и самое главное, не очерчен круг задач, которые эффективно решаются КК, которые решаются вообще. Нет пока более или менее обозначенной теории квантовых алгоритмов, что, конечно, привлекает в данную область силы исследователей.

7 Заключение

В заключение хочется отметить, что создание «многокубитового» КК или доказательство невозможности этого существенно продвинет наши знания об устройстве мира. Исследование КВ, выделение классов задач, решаемых КК не только покажет вычислимость/невычислимость в новом свете, но и, возможно, даст ключ к решению проблем классической теории алгоритмов. Так что КВ — это один из передовых фронтов современной науки.

Список литературы

[1] Стин Э. 2000 *Квантовые вычисления* Ижевск: НИЦ «Регулярная и хаотическая динамика»

[2] Feynman R. 1982 *Simulating physics with computers* International Journal of Theoretical Physics 21: 467.

[3] Shor P. W. 1994 *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, in Proc. 35th Annual Symp. on Foundations of Computer Science, Santa Fe, IEEE Computer Society Press

[4] Сборник работ под ред. В. А. Садовничего *Квантовый компьютер и квантовые вычисления* Ижевск: Ижевская республиканская типография, 1999.