Эссе по курсу «Защита Информации» на тему:

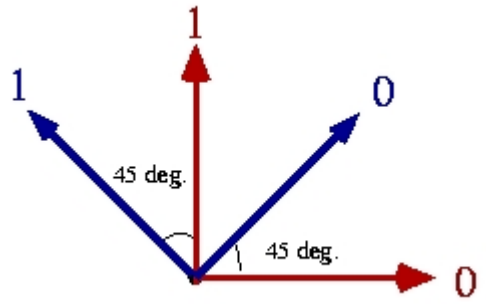
Квантовая рассылка ключей и обзор протокола BB84.

Выполнил студент 011 группы
Королев Александр

МФТИ
г. Долгопрудный
2004 г

Основой технологии квантовой криптографии является неосуществимость определения состояния квантовой системы без изменения её конфигурации, этот свойство известно, как принцип неопределенности Гайзенберга. Например, если мы хотим измерить поляризацию фотона, мы должны поставить поляризатор, пройдя через который фотон будет поляризован в той же плоскости, в которой находится поляризатор. Состояние квантовой системы, в данном случае это фотон, изменилось, это свойство можно использовать для передачи секретной информации. Пока отложим техническую сторону реализации протоколов, использующих принципы квантовой механики, скажем только, что сейчас уже такие системы существуют и работают.

Далее под квантовым битом будет пониматься фотон, который имеет одну поляризацию из четырех возможных.



Будем использовать два базиса для описания поляризации: базис Z определяется горизонтальным и вертикальным ортом, а орты базиса X повернуты относительно него на 45 градусов. Для передачи нулевого бита будем использовать поляризации 0 и 45 градусов, а для передачи единицы 90 и 135 градусов.

Допустим, Алиса и Боб хотят послать секретные сообщения друг другу, то единственный путь, который гарантирует совершенную секретность - использование метода “one time pad”. Конечно, современные алгоритмы кодирования достаточно хороши, и простой перебор не имеет смысла, но с появление квантовых компьютеров многие нынешние стандарты кодирования окажутся несостоятельными. Допустим, Алиса и Боб обладают общим закрытым ключом, который состоит из произвольной последовательности бит, известной им, но никому другому. Затем, чтобы послать сообщение, Алиса преобразует его в последовательность бит и складывает его по модулю два с ключом, результат операции посылается Бобу. То есть вместо каждого сообщения m Алиса посылает r=m+k, где k – секретный ключ. Она использует каждый ключ один раз, если бы ключ использовался дважды, то подслушивающий был бы способен получить некоторую информацию о сообщении.

Так как Боб тоже знает ключ, он может легко декодировать сообщение, выполнив операцию xor с ключом.

$$m=r+k$$

Напротив, подслушивающая Ева ничего не знает о ключе. Для неё k – произвольный набор бит, так что r – тоже произвольный набор бит. Таким образом, смотря на r, она не может получить информацию о переданном сообщении.

Проблема использования метода “one time pad” состоит в том, что на передачу каждого сообщения необходим новый ключ, т.е. необходима возможность оповещения собеседника об используемом ключе, причем это оповещение должно выполняться в

полной секретности. Метод квантового распределения ключей позволяет обменяться секретным ключом, используя открытый канал для его передачи.

Один из хорошо известных протоколов для квантового распределения ключей BB84, названный так, потому что он был предложен Беннет и Брассар в 1984 году. В этом протоколе Алиса посылает Бобу произвольную последовательность квантовых бит. Эти квантовые биты в равной степени могут быть в одном из четырёх состояний.

Состояние	**Базис**	**Значение**
|0>	Z	0
|1>	Z	1
|0> + |1>	X	0
|0> - |1>	X	1

Когда Боб получает квантовый бит, он произвольным образом выбирает базис для своих измерений Z или X, и записывает результаты измерений. Теперь Боб имеет произвольную последовательность бит. Затем, Алиса сообщает, какую последовательность базовых состояний она использовала при посылке каждого бита, но не говорит, какое конкретно было значение бита. Боб сообщает Алисе последовательность базисов, которые он использовал при измерении. Далее они находят корректные измерения, т.е. измерения, которые были сделаны при совпадении базиса использованного Алисой для посылки бита и базиса использованного Бобом для измерения. Остальные биты отбрасываются Бобом, как сделанные с неправильным использованием базиса. Таким образом, при условиях отсутствия ошибок в канале передачи и отсутствии прослушивания канала, Алиса и Боб имеют идентичные закрытые ключи.

Предположим, Ева видела, что Алиса и Боб применяют этот протокол. Она может даже перехватить некоторые квантовые биты, посланные Алисой Бобу. Однако, любые измерения произведенные над квантовым битом с целью определения его состояния неизбежно приведут к его изменению. Если случится так, что она выбрала такие же базовые состояния, как и Боб, то он не заметит этого и получи такой же результат как она, и такой же результат, если бы Ева не делала ничего. Однако Ева не знает, какие базисные состояния использует Боб. Если Ева использовала для измерений базис X, а Боб использовал Z, то Боб получит произвольные результаты, т.е. с вероятностью ½ он будет получать либо ноль, либо единицу. Это означает то, что когда Боб и Алиса будут сравнивать результаты, они обнаружат ошибку. Здесь «сравнивать результаты» подразумевается проверка на четность или проверка контрольных битов, но не прямое сравнение корректно измеренных битов.

В 1984 Беннет предложил следующий протокол передачи ключа, в котором усилен контроль ошибок.

1. Отправитель и получатель договариваются о произвольной перестановке битов в строках, чтобы сделать положения ошибок случайными.
2. Строки делятся на блоки размера k (k выбирается так, чтобы вероятность ошибки в блоке была мала).
3. Для каждого блока отправитель и получатель вычисляют и открыто оповещают друг друга о полученных результатах. Последний бит каждого блока удаляется.
4. Для каждого блока, где четность оказалась разной, получатель и отправитель производят итерационный поиск и исправление неверных битов.

5. Чтобы исключить кратные ошибки, которые могут быть не замечены, операции пунктов 1-4 повторяются для большего значения k.
6. Для того чтобы определить, остались или нет необнаруженные ошибки, получатель и отправитель повторяют псевдослучайные проверки:

- Получатель и отправитель открыто объявляют о случайном перемешивании позиций половины бит в их строках.
- Получатель и отправитель открыто сравнивают четности. Если строки отличаются, четности должны не совпадать с вероятностью 1/2.
- Если имеет место отличие, получатель и отправитель, использует двоичный поиск и удаление неверных битов.

Если отличий нет, после m итераций получатель и отправитель получают идентичные строки с вероятностью ошибки 2^{-m}.

Независимо от того, какие стратегии использует Ева для определения ключа, она вносит ошибки в измерения сделанные Бобом. Сравнивая некоторые произвольно выбранные подмножества ключа, Алиса и Боб могут понять, пытается ли Ева подслушивать их. Конечно, коммуникационный канал между Алисой и Бобом не идеальный, так что ошибки будут возникать даже в отсутствии Евы, но количество этих ошибок будет меньше. При увеличении их числа Алиса и Боб должны заподозрить наличие Евы.

Недостатком данного протокола является незащищенность от атаки называемой “man in the middle”. Если мы предположим, что Ева имеет полный доступ к коммуникационному каналу, и может вносить, заменять без задержки любые сообщения, то она способна свободно выдать себя как за Алису, так и за Боба. Например, она может прикинуться Бобом и получить секретный ключ от Алисы, а Бобу она передаст свой ключ. Получив ключ, Ева полностью управляет коммуникацией Алисы и Боба.

Квантовое распределение ключей вероятно наиболее известный пример использования квантовой механики в криптографии, но существует много других. Например, квантовое распределение ключей тесно связано с немного более строгим протоколом, называемым «uncloneable encryption», который использует квантовые состояния, для передачи сообщений, при этом они не могут быть прочитаны или скопированы Евой.

В 1989 г. Беннет и Брассар в Исследовательском центре IBM реализовали первую квантово-криптографическую систему. Квантовый канал представлял собой воздушную среду. Приемник и передатчик находились на одной скамье, и были накрыты светонепроницаемым кожухом. Таким образом, им удалось осуществить передачу фотонов на расстояние 30 см, основная проблема увеличения расстояния сохранение поляризации фотонов.

Квантовая криптография развивается не только в научно-исследовательском направлении, но и в направлении создания систем, которые могу реально использоваться во всех областях, где необходимо защищать информацию.

Наиболее известные компании, занимающиеся квантовой криптографией - IBM, GAP-Optique, Mitsubishi, Toshiba, MagiQ, QinetiQ, хотя в этой области пока нет абсолютных лидеров. IBM продолжает начатые ими исследования, которые проходят в лаборатории Almaden Research Center.

Исследователи из Лос-Аламоса передали квантовый ключ расстояние 48 км со скоростью в несколько десятков килобайтов в секунду. Такая скорость передачи является

приемлемой для соединения отделений банков. Специалистам фирмы GAP Optique удалось передать ключ на расстояние 67 км из Женевы в Лозанну, а корпорации Mitsubishi Electric удалось передать квантовый ключ на расстояние 87 км со скоростью один байт в секунду. Ученым исследовательского центра Toshiba Research Europe Limited (TREL) удалось передать квантовый ключ на расстояние 100 км, но это все равно достаточно только для коммуникации в пределах одного города.

Одной из основных проблем воплощения квантовой криптографии является проблема генерации единичных фотонов. Несколько лет доктор Эндрю Шилдс и его коллеги создали светодиод способный захватывать одну пару дырка электрон. Поэтому после рекомбинации электрона и дырки данный светодиод испускает один фотон. Учеными Фредериком Гроссаном из Института оптики в Орсэ (Франция) был разработан метод, позволяющий шифровать сообщения не с помощь единичных фотонов, а с помощью пучков фотонов или фотонных импульсов. Данный метод привлекателен простотой генерации световых импульсов, но более слабо защищен от атак злоумышленников. Также можно отметить, что в этом методе возможна потеря части фотонов.

Также в последнее время квантовой криптографией занялись такие компании как NEC, Verizon Communications. Продукты этих компаний являются коммерческими. Наибольшая на сегодняшний день скорость, достигнутая в квантовой передачи информации 250 Мбит/с, хотя уже в ближайшее время ожидается её рост.

Интерес к квантовой криптографии растет, уже появились коммерческие продукты в данной области, осталось только дождаться того момента, когда данная технология подешевеет, так что будущее, несомненно, за квантовой криптографией!

В эссе использованы материалы:

«Quantum Cryptography Tutorial» James Ford 1996
www.cs.dartmouth.edu/~jford/crypto.html

«Квантовая криптография» Александр Евангели.
Статья опубликована в PC Week/RE № 43 от 18.11.2003 г., стр. 31
www.computer-museum.ru/technlgy/quancryp.htm

«From Quantum Cheating to Quantum Security» Hoi-Kwong Lo Department of Elect. & Computer Engineering (ECE); & Department of Physics University of Toronto.
www.physicstoday.org/pt/vol-53/iss-11/p22.html