Введение в квантовую криптографию.

Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec
Выполнил Матвеев А.М 217 гр.
1 мая 2006 г.

Широко известно, что самыми надежными криптосистемами являются системы с секретным ключом, так как такие системы трудно или практически невозможно взломать, не зная ключ. Однако здесь возникает проблема: как же передать ключ при этом не рискуя отдать его в руки злоумышленника. Таким образом, основной задачей, которую нужно решать при создании высоко надежной криптографической системы, является проблема конфиденциального распространения ключа. Нужно не только по возможности исключить возможность перехвата и узнавания ключа злоумышленником (либо подмены по схеме Man-In-The-Middle), но также в случае попытки подделать либо перехватить часть информации узнавать об этом максимально быстро. Кроме того, нужно уметь определять подслушивание (для максимальной надежности).

Эту задачу помогают решить методы квантовой криптографии, в основе которых лежит «Принцип неопределенности Гейзенберга», сформулированный в 1927 г.
Дело в том, что нельзя измерить какой-либо параметр квантовой частицы, оставив при этом все остальные характеристики без изменения. Поэтому Ева не может каким-либо образом перехватить данные, посылаемые передающей стороной, оставаясь при этом не замеченной. Для передачи ключа между Алисой и Бобом используются различно поляризованные фотоны.

Упрощенный алгоритм (BB84 предложенный Чарлзом Беннетом и Брассаром в 1984 г. ,потом неоднократно модифицировавшийся и дополнявшийся) выглядит следующим образом:
Алиса и Боб обмениваются фотонами поляризованными по одному из четырех способов: ортогональная (вертикальная или горизонтальная) либо диагональная (под углом 45 или 135 градусов).

Условно обозначим их
\ - диагональная(135).
/ - диагональная(45).
| - ортогональная(вертикальная).
-- - ортогональная(горизонтальная).

Пусть в качестве передающей стороны выступает Боб. Он посылает 10 фотонов:
\ | / -- / \ -- / | \

На противоположной стороне Алиса принимает фотоны, используя один из двух типов приемников: ортогональный и такой же, но повернутый под углом 45 к предыдущему (кроме того, можно использовать, к примеру, вертикальную и циркулярную поляризацию тогда приемников также два: один умеет распознавать вертикальную, а другой право- или лево-циркулярные поляризации, но здесь для наглядности ограничимся предложенным вариантом).

Главной характеристикой каждый из приемников может правильно распознавать только один тип поляризации. Если правильно использовать нужный тип приемника, можно определить конкретную поляризацию: ортогональный распознает вертикальная поляризация или горизонтальная, «диагональный» - угол 45 или 135. (Диагональный – условное название для приемника, повернутого на 45 градусов, на самом деле он, конечно, ничем не отличается от первого). В остальных случаях – при неправильном выборе приемника - результат непредсказуем и абсолютно случаен..

После выполнения сеанса, получатель (в нашем случае Алиса) по открытому каналу уведомляет отправителя о том, какую последовательность приемников он использовал, а отправитель сообщает о том, какие из приемников были правильного типа. Те фотоны, для которых тип приемника был неправильный, отбрасываются. Оставшимся фотонам по взаимной договоренности присваивается значение 0 либо 1.
Например: вертикальная и диагональная(45) – 1, горизонтальная и диагональная(135) – 0.
Из этих битов получается ключ для последующего обмена данными. Если результаты Алисы и Боба будут заметно отличаться, то определяется вмешательство Евы в систему.

При этом Еве очень трудно при помощи перехвата (А-Е-Б) не выдать свое присутствие. Если бы она попыталась это сделать, то при приеме от Боба с 50% вероятностью выбирала бы неправильный анализатор, и, отправляя наугад Алисе вертикально или диагонально поляризованный фотон, не угадывала бы с поляризацией также в 50% случаев, что привело бы к расхождению в результатах в 25%, что легко обнаруживать при помощи ,например, сличения по открытому каналу договоренной части ключа.

Рассмотрим предложенный алгоритм на конкретном примере:
Д - «диагональный» фильтр, О - ортогональный.
0 или 45 – 1, 90 или 135 – 0.

Боб передает	\	|	/	--	/	\	--	/	|	\
Фильтр Боба	Д	О	Д	О	Д	Д	О	Д	О	Д
Фильтр Алисы	Д	О	О	Д	Д	О	О	О	Д	Д
Результаты А.	0	0	1	1	1	1	1	0	1	0
Правильных	+	+			+		+			+
Ключ	0	0			1		1			0

Получили ключ 00110. Результаты Алисы в тех случаях, когда она неправильно выбирает анализаторы, случайны, но они и не используются.

Однако на практике прием и передача фотонов осложняется присутствием шума, который может вызвать ошибки, причем при уровне оборудования скажем пятилетней давности, ошибки могут быть около 50%. Сейчас, конечно процент ошибок меньше.
Эти ошибки могут быть обнаружены и устранены с помощью, например, подсчета четности битов. Беннет в 1991 году предложил алгоритм, который позволяет это сделать:

1)Алиса и Боб договариваются о произвольной перестановке бит, это делает положения ошибок случайными.
2)Строки делятся на блоки размера N. N нужно выбрать так, чтобы вероятность ошибки в блоке была небольшой.
3) Для каждого блока Алиса и Боб вычисляют четность. После сообщения друг другу о результатах по открытому каналу отбрасывается последний бит.
4)Для блоков с разной четностью производится поиск и исправление неверных битов.

Однако в таком случае могут остаться кратные ошибки в блоке, которые не могут быть обнаружены контролем четности, поэтому следует произвести те же операции для больших N.
5)После этого для определения того, не осталось ли ошибок, Алиса и Боб проводят следующие псевдослучайные проверки:

а)Открыто объявляют о случайном перемешивании бит в строках.
б)Проверяют четности для строк(открыто). В случае если ошибка имеет место, она будет обнаружена с вероятностью 50%.
в)Если ошибка не обнаружена, операции повторяются, после m итераций ошибок нет с вероятностью 2 в степени –m.

Обнаружение и исправление ошибки может быть произведено следующим способом: хотя биты передаются сплошным потоком, можно представить их в виде блоков, для простоты блок возьмем небольшого размера 6x6.

1	0	1	0	1	1
0	1	1	0	1	1
0	1	*	1	1	1
1	1	0	1	0	0
1	0	1	0	0	1
1	1	0	1	1	1

Символ * означает место ошибки, которую нужно исправить.
Проверка четности битов Алисой и Бобом даст различный результат в третьей строке и третьем столбце, если сообщить открыто друг другу о результатах, можно определить какой бит должен стоять на этом месте. Однако такой метод неприемлем, в случае, если ошибок в блоке 2 или более например:

1	0	1	0	1	1
0	1	1	0	1	1
0	1	*	1	1	1
1	1	0	1	0	0
1	0	1	0	*	1
1	1	0	1	1	1

Это эквивалентно следующим ошибкам:

1	0	1	0	1	1
0	1	1	0	1	1
0	1	1	1	*	1
1	1	0	1	0	0
1	0	*	0	0	1
1	1	0	1	1	1

В таком случае исправить (а зачастую и обнаружить) ошибку нельзя.
Именно поэтому нужно выбирать блоки соответствующего небольшого размера, чтобы по возможности исключить вероятность кратной ошибки в одном блоке.

При практической реализации данного метода криптографии нужно решать также проблему интенсивности квантов света. Одиночный фотон тяжело получить и зарегистрировать. Поэтому можно использовать не единичные фотоны, а короткие импульсы. В качестве предающего устройства можно использовать, к примеру, импульсный лазер либо светоизлучающий диод. Однако при таком способе передачи данных есть вероятность того, что, скажем, из импульса длиной в 1000 фотонов при передаче злоумышленником будет перехвачено и отведено 100 из них. Тогда при длительном наблюдении за перепиской Алисы и Боба, Ева сможет при наличии достаточной вычислительной мощности расшифровать сообщения, что недопустимо. Для повышения надежности системы квантов должно быть порядка одного, это не даст Еве подслушивать незамеченной.

Но тогда для регистрации отдельных квантов света придется повысить чувствительность приемника, что неизбежно приведет к возникновению темнового шума, явления, при котором фотоны будут регистрироваться даже в отсутствие передачи. Тогда нужно использовать в качестве улей и единиц не единичные фотоны, а их определенные последовательности, используя при этом алгоритм, контролирующий и позволяющий исправлять ошибки. Кроме того, вступают в силу квантовые эффекты. Хотя фотон и регистрируется как частица, при передаче по оптическому волокну он ведет себя как волна. Это приводит к тому, что фотон регистрируется с какой-то вероятностью отличной от единицы. Также имеет место эффект поглощения в оптоволокне (порядка 0.3 – 3Дб/км).

Поэтому первые системы реализующие методы квантовой криптографии, которые были разработаны в 1989 г. Беннетом и Брастером были эффективны только на небольших расстояниях. Устройство представляло собой оптическую скамью, на концах которой были установлены передатчики Алисы и Боба, со светонепроницаемым кожухом размером 0,5х0,5м. оптическим каналом выступал просто воздух, длина канала составляла около 30см. Это был огромный шаг вперед в развитии квантовой криптографии.

В 2001 г. Эндрю Шилдс вместе с коллегами из Кембриджа и компании TREL разработали диод, способный излучать отдельные фотоны, диод построен на основе «квантовой точки» - микроскопическому кристаллу полупроводника, размером несколько нанометров. Он настолько мал, что при пропускании тока через него, создается только одна электронно-дырочная пара. Используя эту технологию, удалось в ходе эксперимента получить скорость передачи данных 75кБит/с. на достаточно большое расстояние.

Активными разработками в этой области в настоящее время занимается довольно много компаний из них крупнейшие: швейцарская ID Quantique, и американская Magiq Technologies из Нью-Йорка. К разработке квантового метода криптографии проявляют большие интересы военные и спецслужбы, а также крупные коммерческие организации. Защита информации при использовании данного метода практически абсолютна, что делает ее привлекательной, хоть она и дорога. Так конечный продукт компании Magiq Technologies стоит около 100 тысяч американских долларов. Что не останавливает тех, кто хочет получить действительно надежную систему защиты данных от несанкционированного доступа.

Система квантового распространения ключа (QKD – quantum key distribution) используемая MagiqTech названа Navajo по имени Североамериканского племени индейцев Навахо. Язык этого племени американцы использовали для передачи секретных сообщений во время Второй мировой войны. В те времена в Европе его никто не знал. MagiqTech реализовало технологию, позволяющую обмениваться данными на расстоянии до 120 км.. Для клиентов из телекоммуникационной области реализованы уровни VPN security.

Navajo состоит из 19-дюймовых устройств, называемых «черными ящиками» (так как это коммерческий продукт, то состав и назначение элементов держатся в секрете), передающих и принимающих фотоны с определенными характеристиками. Кроме того, что квантовый метод распространения ключа сам по себе достаточно надежен, в Navajo предусмотрено изменение ключа каждые 10 секунд, так что даже если злоумышленник каким-то образом сможет перехватить ключ он окажется абсолютно бесполезным.

Как сообщается одним из руководящих компанией лиц, мистером Геллардом, компания продолжает разработки в данной области, с целью создания новых надежных источников одиночных фотонов, механизмов квантовой памяти, а также квантовых повторителей. У Magiq Technologies есть далеко идущая цель по созданию квантовых компьютеров, с характеристиками приемлемыми для выпуска на рынок. Возможно это произойдет не в самом отдаленном будущем, и станет переворотом в развитие электронных и вычислительных технологий.

В настоящее время Magiq Technologies собирается экспортировать свой товар за пределы США, для чего нужно добиться разрешения на вывоз у правительства. В Швейцарии также разработана система подобная Навахо, но она находится пока в стадии разработки. Можно прогнозировать в ближайшее будущее вытеснения с рынков других систем в пользу квантовых.

Использованы материалы из нескольких источников:

1) http://www.citforum.ru/security/cryptography/quant_crypto/

2)http://ru.wikipedia.org

3) http://news.bbc.co.uk/1/hi/technology/3543495.stm

4) http://www.magiqtech.com/press/Magiq_Navajo_Launch.pdf

5) http://book.itep.ru/6/q_crypt.htm