МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ (ГУ)
Факультет радиотехники и кибернетики

Эссе по курсу «Защита информации»

Основы квантовой криптографии

Подготовил студент 316 группы
Ходаковский И.А.

Долгопрудный, 2006

1.Введение

Квантовая криптография — способ защиты линий связи, основанный на квантовых свойствах физических носителей информации.

На настоящий день квантовое шифрование рассматривается применительно к оптическим и электрическим линиям связи (витая пара и др.). В первом случае носителем информации является фотон или группа фотонов, во втором – электроны.

Квантовый канал — физический канал передачи данных, используемый для генерации секретного ключа.

Кубит — единица квантовой информации, аналог бита в квантовом компьютере.

Кубит допускает 2 состояния, $|0\rangle$ *и* $|1\rangle$. Состояния – стационарные, понимаются в квантово-механическом смысле, образуют полный набор (подробнее см. к примеру П.Дирак «Принципы квантовой механики», глава 2).

В силу принципа суперпозиции, состояние (не стационарное) системы, имеющей пару стационарных состояний $|0\rangle$ *и* $|1\rangle$, представляется суперпозицией

$$\psi = C_1|0\rangle + C_2|1\rangle, \quad {C_1}^2 + {C_2}^2 = 1$$

Вообще говоря, имеется более чем счётное множество состояний системы (коэффициенты комплексны). Однако при всяком взаимодействии с окружающим миром (при измерении параметров системы), мы случайным образом получаем одно из двух стационарных состояний. Вероятность получить каждое состояние определяется квадратом соответствующего коэффициента. Соответственно, повторное измерение состояния системы, вообще говоря не имеет отношения к тому состоянию, в котором пребывала система до первого измерения.

При передаче по оптическому каналу, кубитом является фотон (состояния – направление поляризации). При использовании металлических кабелей в качестве кубита выступает электрон (состояния – направление спина).

Основываясь на идее невозможности повторного измерения параметров изолированной квантовой системы, предлагается способ кодирования сигнала, позволяющий в идеале абсолютно точно установить факт перехвата и таким образом предотвратить потерю конфиденциальности.

2.Простейший алгоритм

Рассмотрим простейший вариант передачи, называемый BB84.

Для передачи информации в протоколе BB84 используются фотоны, поляризованные под углами 0, 45, 90, 135 градусов. С помощью измерения можно различить два ортогональных состояния: в случае если известно, что фотон поляризован либо вертикально, либо горизонтально, то путем измерения, можно установить — как именно; аналогично можно утверждать относительно поляризации под углами 45 и 135 градусов.

Состояния с диагональной поляризацией являются смешенными в базисе поляризаций 0 и 90 и наоборот, так что с достоверностью отличить вертикально поляризованный фотон от фотона, поляризованного под углом 45º, невозможно.

Эти особенности поведения квантовых объектов легли в основу протокола квантового распространения ключа. Отправитель кодирует отправляемые данные, задавая определенные квантовые состояния, получатель регистрирует эти состояния. Затем получатель и отправитель совместно обсуждают результаты наблюдений по открытому каналу связи. В итоге со сколь угодно высокой достоверностью можно гарантировать, что переданная и принятая кодовые последовательности тождественны. Обсуждение результатов касается ошибок, внесенных

шумами или злоумышленником, и ни в малейшей мере не раскрывает содержимого переданного сообщения.

Рассмотрим на примере процесс передачи ключа от Алисы к Бобу.

Обозначения приведены в таблицах:

Обозначения бит известны А. и Б. заранее.

Обозначение	Поляризация фотонов	Кодируемый бит
|	Вертикальная	0
—	Горизонтальная	1
/	Под угром 45,	0
\	Под углом 135	1

Обозначение анализатора	Поляризация фотонов
+	Прямоугольный
x	Диагональный

Итак, А. передаёт Б. 9 фотонов, Б. поставил поляризаторы наугад. По результатам измерений Б. проставляет значения бит.

Последовательность фотонов Алисы	|	/	/	—	\	|	|	—	—
Последовательность анализаторов Боба	+	x	+	+	x	x	x	+	x
Результаты измерений Боба	0	0	1	1	1	0	1	1	0
Анализаторы выбраны верно	да	да		да	да			да	
Ключ	0	0		1	1			1	

Первый бит – Б. наблюдает на выходе сигнал, фильтр вертикальный, смотрит таблицу (первая строка сверху) выше, пишет 0

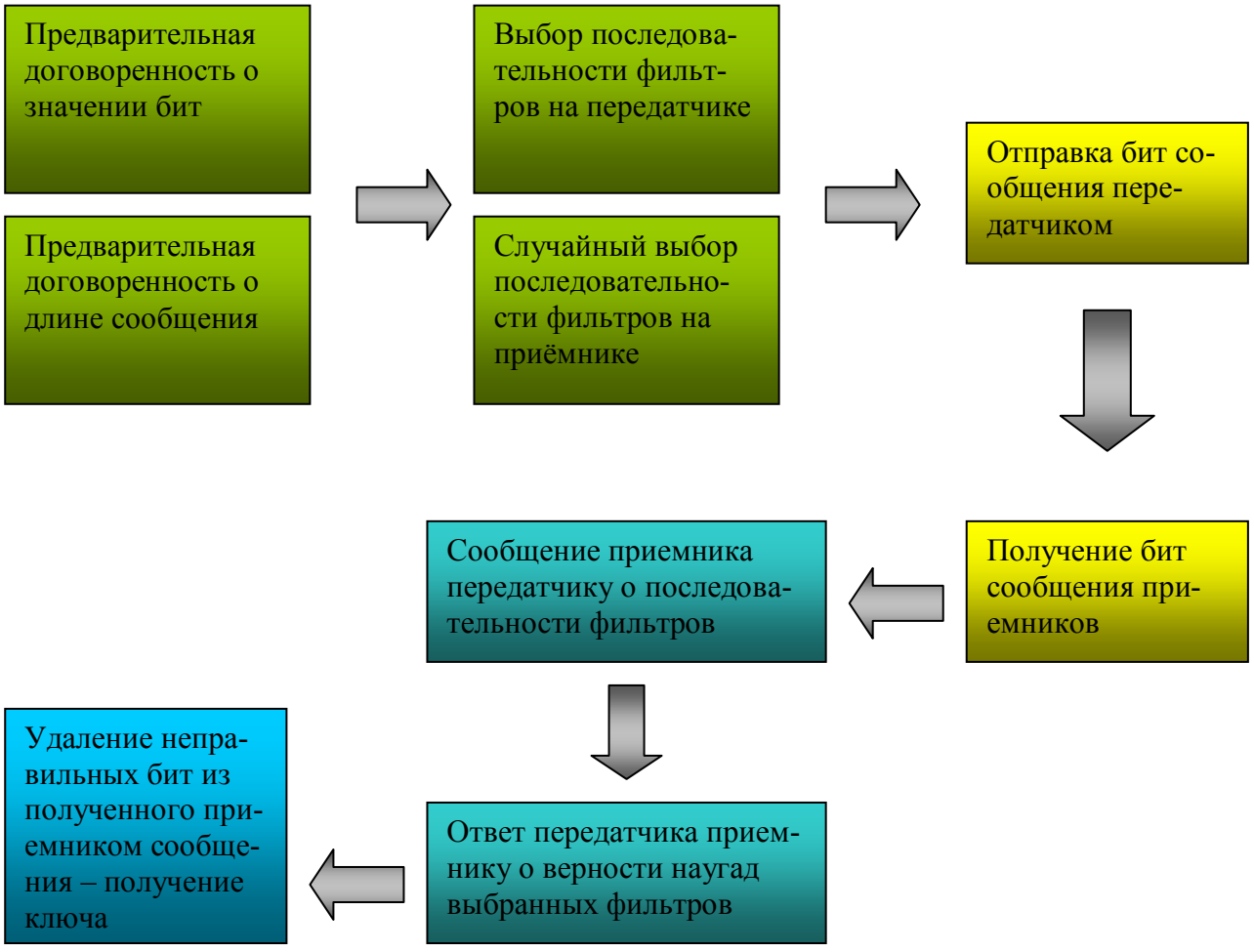
Второй бит – Б. наблюдает на выходе сигнал, фильтр диагональный, смотрит таблицу (третья строка сверху) выше, пишет 0

Третий бит – Б. не наблюдает на выходе сигнал, фильтр вертикальный, смотрит таблицу (вторая строка сверху) выше, пишет 1

И т.д. Кстати заметим, на самом деле Б. поставил фильтры | и /, а состояния, ортогональные приведённым, определяет по отсутствию сигнала (сигнал ниже порога).

После этого происходит сравнение фильтров. Отбрасывая ложные, Б. получает ключ 00111.

Изобразим алгоритм схематически.



3. Техническая реализация

Техническая схема передатчика приведена на рис.1, приёмника на рис.2

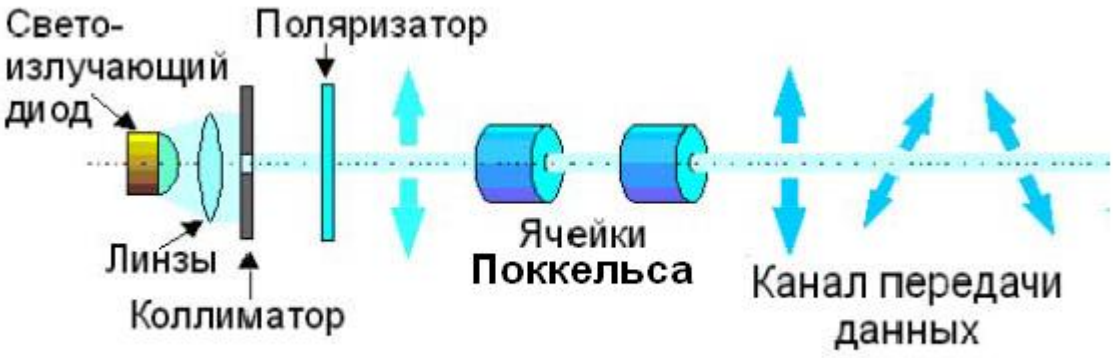


Рис.1. Схема передающей стороны

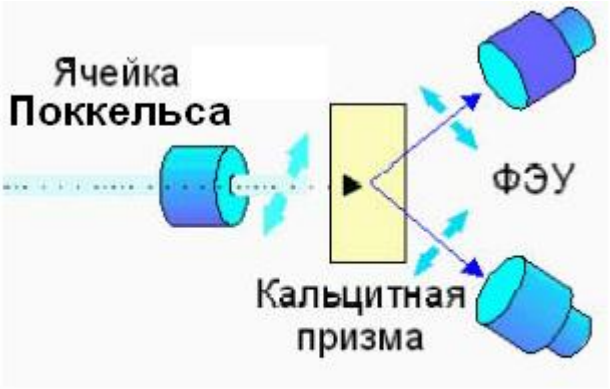


Рис.2. Схема принимающей стороны

Основные проблемы технического применения:

- малая скорость передачи
- низкая интенсивность излучения
- невозможность построения ретрансляторов (повторителей)

Первое и второе является следствием используемой однофотонной передачи (соответствующие светоизлучающие диоды были изготовлены в 2001г.) Увеличение числа фотонов (а следовательно и интенсивности), повышает вероятность необнаруженного подключения к каналу передачи. Последнее является фундаментальным ограничением.

Тем не менее, на настоящий момент сообщается о действующем прототипе системы квантового шифрования, работающим на скоростях 250 Мбит\с. О расстояниях передачи источник умалчивает.

4.Возможность взлома

Выполняя измерение поляризации фотона, считается, что вероятностью 0.5 мы получим неудовлетворительный результат. В том смысле, что ФЭУ не зафиксируют сигнала достаточного уровня, и единственное, что будет известно – исходная поляризация была ортогональна тому, что пытались измерить. А при правильном подборе соответствия бит и поляризации, это даёт вероятность 0.5 ошибки в одном бите.

Считается также, что в идеальном случае передачи одного фотона на бит, мы полностью исключаем возможность необнаруженного доступа к передаваемой информации. Так как измерение, проведённое над квантовым объектом, изменяет его свойства.

Давайте посмотрим на причины последнего утверждения.

Согласно формализму кв.мех., состояния даются векторами гильбертова пространства, для которых верен принцип суперпозиции. До измерения система находится в состоянии, являющимся суперпозицией базисных состояний этого пространства. Базисные состояния образуются стационарными волновыми функциями, соответствующими некоторым значениям наблюдаемых .

При измерении мы получаем признак того, что на момент этого измерения объект находился в определённом стационарном состоянии. А после измерения, согласно уравнению эволюции, объект снова оказывается в смешанном состоянии, и куда нас забросит повторное измерение – точно сказать нельзя.

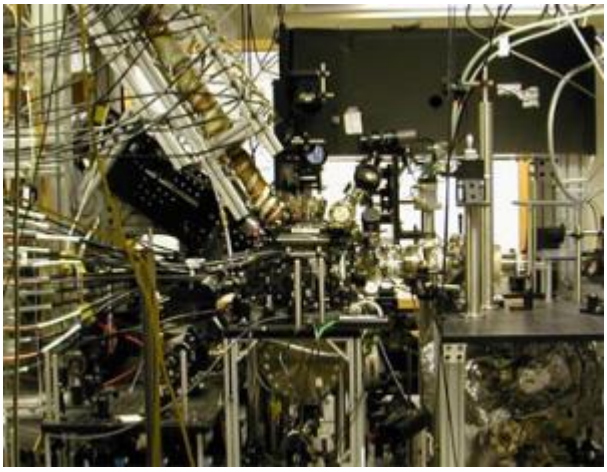
Для нас это означает следующее.

1. Передатчик отправляет фотон определённой поляризации – акт измерения, мы отправили систему в нужное стационарное состояние.
2. Приёмник недоброжелателя принимает фотон – проводит измерение, если попал, то хорошо, если нет, то узнать, в каком состоянии мы отправляли уже нельзя, поскольку акт измерения забросил систему в другое стационарное состояние, и эволюция её протекает уже из новой точки.

Возникает вопрос, а можно ли зафиксировать начальное состояние (точку), откуда начинается эволюция системы, с тем, чтобы спокойно проводить измерения до тех пор, пока не попадёт на нужный результат?

В теоретической физике известен квантовый эффект Зенона. Эффект был теоретически предсказан еще в 60-е годы советским физиком Халфиным Л.А. Впервые опубликованная в 1978г. (Е. Судершан, Б. Мизра) работа с аналогичным название описывала парадоксальную на первый взгляд ситуацию, когда достаточно частые измерения состояния системы, заставляли её пребывать в одном стационарном состоянии, в пределе на протяжении бесконечного

времени. В оригинальной работе рассматривается радиоактивный распад. Показано, что при достаточно частой проверке, распалось ядро или нет, ядро не распадается.



В экспериментах, проведенных в Массачусетском технологическом институте (фотография слева – установка), наблюдалось тридцатикратное замедление распада нестабильной системы за счет квантового эффекта Зенона и впервые было проведено сравнение импульсного и непрерывного наблюдения за квантовой системой, подтвердившие теоретические выводы.

Вкратце объяснение такого. Вероятность получить при измерении то или иное стационарное состояние зависит от значения коэффициентов в разложении состояния по базису гильбертова пространства. Некоторое время после измерения (в котором было получено состояние i), коэффициент при i-ой волновой функции близок к единицы. Т.е. если мы успеем провести повторное измерение до того, как его значение упадёт, то снова получим состояние i . И так далее.

Эффект имеет общий характер (присущ всем квантовым объектам) и можно предположить возможность технической реализации прибора для поддержания наперёд заданного стационарного состояния фотона. Использование подобного устройства сильно упростит процесс получения ключа при квантовом шифровании.

Но на настоящее время даже повторение оригинального эксперимента является тяжелой задачей, не говоря уже серийном выпуске «чёрных ящиков», с лёгкостью проводящий его подобие.

1. «Квантовая криптография» http://ru.wikipedia.org/
2. Введение в квантовую криптографию http://teormin.ifmo.ru/courses/intro/38.pdf
3. Алгоритм BB84 http://en.wikipedia.org/wiki/BB84
4. Квантовый эффект Зенона http://journal.issep.rssi.ru/articles/pdf/9709_071.pdf
5. *Misra B., Sudarshan E.C.G.* // J. Math. Phys. 1977. Vol. 18. P. 756–763.
6. Сообщение об экспериментальной проверке эффекта Зенона http://elementy.ru/news/430424