# Стойкость квантовых протоколов распределения ключей

*Янковская Ю. Ю., студентка 5-го курса, группы 188, Марина А. А., студентка 5-го курса, группы 1А8*
*Научные руководители – к.ф-м.н, доцент Литвинов Р.В., аспирант Чечулин С.О.*
*Проект ГПО РЗИ-0713 – Криптографические алгоритмы в системах защиты информации*

Квантовое распределение ключей – метод, с помощью которого между двумя абонентами (Алиса и Боб) может быть распределен секретный ключ, если они имеют доступ к квантовому каналу связи и открытому обычному каналу с возможностью аутентификации отправителя сообщения. Переданные по квантовому каналу биты используются для создания секретного ключа, которым затем шифруются сообщения, передаваемые по любому открытому каналу. Основным преимуществом квантового распределения ключей перед обычными классическими схемами является принципиальная возможность обнаружить подслушивающего агента, который, в силу законов квантовой физики, при подслушивании вынужден возмущать состояния передаваемых квантовых частиц. Таким образом, если уровень ошибок при передаче значительно превышает естественный уровень помех в канале, то это служит сигналом к прерыванию процедуры передачи ключа.

Однако, законы квантовой механики, благодаря которым существует возможность обнаружить злоумышленника - Еву, также допускают и различные виды атак на квантовый канал связи.

Стек КПРК включает специальную процедуру усиления секретности, при которой длина переданного ключа уменьшается на некоторое число бит, которое зависит от уровня ошибок при передаче. Тем самым уменьшается до приемлемого уровня количество информации о ключе, которое могла получить Ева.

Отметим также, что ошибки при передаче кубитов могут быть обусловлены не только активностью Евы, но и естественными помехами и затуханием в квантовом канале, а также ошибками при генерации и измерении состояний кубитов. В квантовой криптографии, вследствие невозможности отличить естественные помехи от создаваемых подслушиванием, все ошибки, возникающие при передаче кубитов, считаются созданными подслушивающим агентом. В настоящее время в экспериментах по передаче кубитов по оптоволоконным каналам, а также по воздуху, достигается уровень естественных помех не более нескольких процентов.

## Стратегии атак подслушивающего агента

Основные стратегии атак, которые может использовать Ева в случае, когда все сигналы содержат строго один фотон, подразделяют на два класса.

К первому классу относят некогерентные или индивидуальные атаки. При таких атаках Ева обрабатывает каждый фотон Алисы отдельно. Простейшим вариантом является атака перехвата – пересылки фотона. Ева перехватывает посылаемые Алисой фотоны, измеряет их состояния и отправляет затем новые фотоны Бобу в измеренных ею состояниях. Поскольку Ева не пропускает фотоны Алисы по каналу, а излучает новые, такую стратегию подслушивания называют также непрозрачной.

К некогерентным относят также атаку перепутывания квантовых проб Евы с пересылаемыми по каналу фотонами. При этом каждый фотон Алисы перепутывается с отдельной пробой независимо от других, а провзаимодействовавшие с пробами фотоны посылаются Бобу. Затем Ева хранит пробы в квантовой памяти и измеряет их состояния по отдельности после того, как закончится открытый обмен сообщениями между Алисой и Бобом на этапе просеивания ключа. Прослушивание открытых сообщений между Алисой и Бобом позволяет Еве узнать базисы, которые использовала Алиса, и тем самым выбрать

оптимальные измерительные процедуры для своих проб, чтобы получить больше информации о ключе. Разумеется, состояния фотонов Алисы, с которыми Ева перепутывает свои пробы, изменяются после перепутывания, однако уровень вносимых Евой ошибок может быть сделан меньше, чем при непрозрачной атаке. Такую атаку называют также полупрозрачной.

При любой некогерентной атаке Ева может уменьшить уровень вносимых ею ошибок за счет уменьшения получаемой ею информации – она должна перехватывать или перепутывать со своими пробами только некоторую часть фотонов Алисы.

Второй класс атак – так называемые когерентные атаки, при которых Ева может любым (унитарным) способом перепутать пробу любой размерности с целой группой передаваемых одиночных фотонов. Предельный вариант такой атаки, когда Ева перепутывает свою пробу со всей последовательностью переданных Алисой фотонов. Далее Ева хранит свою большую пробу до тех пор, пока не закончатся все открытые коммуникации между Алисой и Бобом, а затем производит наиболее общее измерение пробы по своему выбору.

Подклассом когерентных атак являются коллективные, при которых каждый фотон Алисы индивидуально перепутывается с отдельной пробой, как и при некогерентных атаках. Однако измерение производится не индивидуально для каждой пробы, а на всех пробах сразу, рассматриваемых как большая единая квантовая система.

## Атаки на протокол BB84 для случая однофотонных сигналов

BB84 - квантовый протокол использующий 4 квантовых состояния – два неортогональных состояния для кодирования 0 и два – для кодирования 1.

Измерим взаимную информацию Алисы и Боба $I_{AB}(D)$ по формуле:

$$I_{AB}(D) = \tfrac{1}{2}\varphi(1-2D)$$

Измерим взаимнуюинформацию Алисы и Евы $I_{AE}(D)$, в случае, когда Ева измеряет состояние пробы сразу после перепутывания с фотоном Алисы по формуле:

$$I_{AE}(D) = \tfrac{1}{2}\left\{1+\chi\left(\tfrac{1}{2}-\sqrt{2D-4D^2}\right)+\chi\left(\tfrac{1}{2}+\sqrt{2D-4D^2}\right)\right\}.$$

Для случая равновероятного использования двух базисов в протоколе BB84:

$$I_{AE}(D) = \tfrac{1}{2}\varphi\left(2\sqrt{D(1-D)}\right)$$

Зависимость взаимой информации от уровня ошибок D представлена на Рис.1.

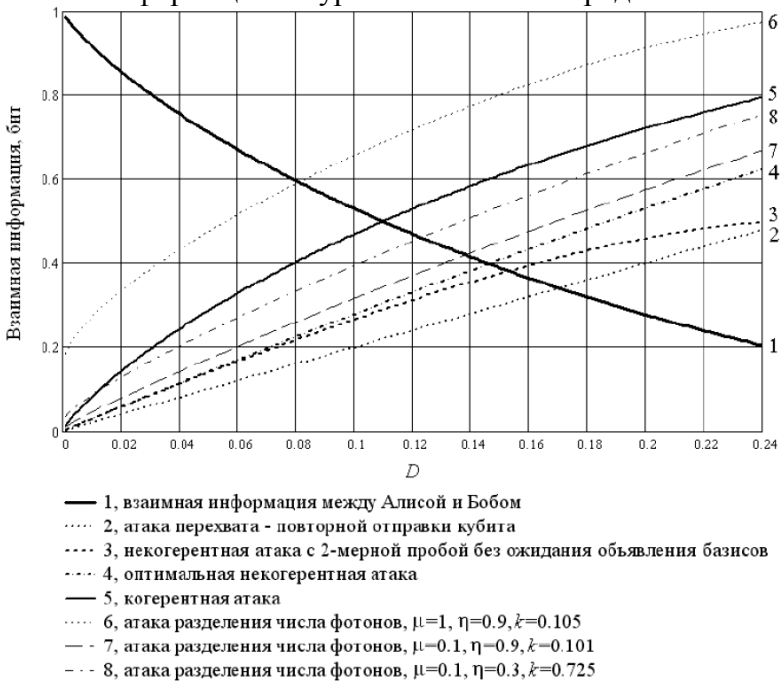


Рисунок 1. Взаимная информация $I_{AB}(D)$ (кривая 1) и $I_{AE}(D)$ для различных стратегий атак на протокол BB84 (кривые 2-8).

## Атака разделения числа фотонов на протокол BB84.

Однофотонные источники пока не созданы и на практике используют слабые когерентные импульсы, излучаемые лазерными светодиодами – многофотонные источники. Вероятность того, что импульс содержит n фотонов определяется распределением Пуассона, в случае канала с потерями формула примет вид:

$$p_{n,\,loss} = e^{-\eta\mu}\frac{(\eta\mu)^n}{n!}$$

где μ – среднее число фотонов в импульсе, η – коэффициент передачи канала.

Таким образом, становится возможной атака разделения числа фотонов. Если Ева обнаруживает в импульсе более одного фотона, она отводит один, позволяя остальным беспрепятственно пройти к Бобу. Затем Ева выполняет перепутывание перехваченного фотона со своей пробой и ожидает объявления базисов. Выполняя затем измерение состояния пробы, Ева получит точное значение переданного бита, не внося при этом никаких ошибок в просеянный ключ. Если же импульс несет один фотон, то стратегии Евы могут быть различны. Например, она может просто пропускать все однофотонные импульсы, что позволит ей остаться необнаруженной. Однако при малом μ число многофотонных импульсов будет невелико, и это не позволит Еве получить сколько-нибудь значительную информацию о ключе. Другая стратегия состоит в том, что Ева выполняет некогерентную атаку одного из рассмотренных выше типов на однофотонные импульсы.

Еще одна стратегия Евы состоит в блокировании части однофотонных импульсов (в результате Боб получает пустой импульс, т.е. его датчик не регистрирует фотон). Тем самым она увеличивает долю многофотонных импульсов, что позволяет ей увеличить информацию о ключе при том же уровне вносимых в просеянный ключ ошибок.

k – доля однофотонных импульсов, величина k выбирается так, чтобы число непустых импульсов, которое ожидает Боб для канала с потерями, равнялось числу непустых импульсов после того, как Ева заменяет канал на идеальный (η=1) и блокирует часть однофотонных импульсов:

$$1-e^{-\eta\mu} = (1-k)p_1 + p_{n>1},$$

Вероятность для Евы правильно измерить состояние пробы, перепутанной с фотоном Алисы, дается выражением:

$$P_{correct} = \frac{1-e^{-\mu}(1+\mu)+(1-k)\mu e^{-\mu}\left(1/2+\sqrt{D(1-D)}\right)}{1-e^{-\mu}(1+\mu k)},$$

$I_{AE}(D)$ для описанной атаки: $I_{AE}(D) = \frac{1}{2}\varphi\left[1-2(1-P_{correct})\right]$.

Рассматривается также возможность для Евы заменить квантовый канал с потерями, который используют Алиса и Боб, на канал без потерь (естественно, они не знают о замене). В этом случае Ева получает возможность блокировать некоторую часть однофотонных импульсов так, чтобы Боб в результате получил приблизительно ожидаемое им число пустых импульсов. Для исходного канала с очень большими потерями такая стратегия позволяет Еве получить почти полное знание ключа, не внося никаких ошибок.

Кроме того, существует некоторая область параметров η и μ , где атака разделения числа фотонов позволяет Еве сохранить не только ожидаемую Бобом долю пустых сигналов, но также и всю статистику числа фотонов в импульсе, т.е. Ева может остаться необнаруженной и получить при этом полную информацию о ключе, только, если потери в исходном канале очень велики. Отсюда в частности следует, что Алиса и Боб на практике должны использовать квантовый канал ограниченной длины так, чтобы его коэффициент передачи оставался достаточно высоким.

**Атаки на протокол с 6-ю состояниями для случая однофотонных сигналов.**

Этот протокол является расширением BB84 и использует три сопряженных базиса.

Тактика проведения некогерентных атак на протокол 6 состояний аналогична тактике для протокола BB84. Взаимная информация между Алисой и Евой для когерентной атаки на протокол с 6-ю состояниями вычисляется по той же схеме, что и для протокола BB84.

Взаимная информация между Алисой и Евой для оптимальной некогерентной атаки на протокол с 6-ю состояниями дается выражением:

$$I_{AE}(D) = 1 + (1-D)\left[f(D)\log_2 f(D) + (1-f(D))\log_2(1-f(D))\right],$$

где $f(D) = \frac{1}{2}\left(1 + \frac{\sqrt{D(2-3D)}}{1-D}\right)$.

Взаимная информация между Алисой и Евой для когерентной атаки на протокол с 6-ю состояниями вычисляется по той же схеме, что и для протокола BB84:

$$I_{AE}(D) = -\tfrac{1}{2}\left[(1-\tfrac{3}{2}D)\log_2(1-\tfrac{3}{2}D) + \tfrac{3}{2}D\log_2(\tfrac{1}{2}D)\right].$$

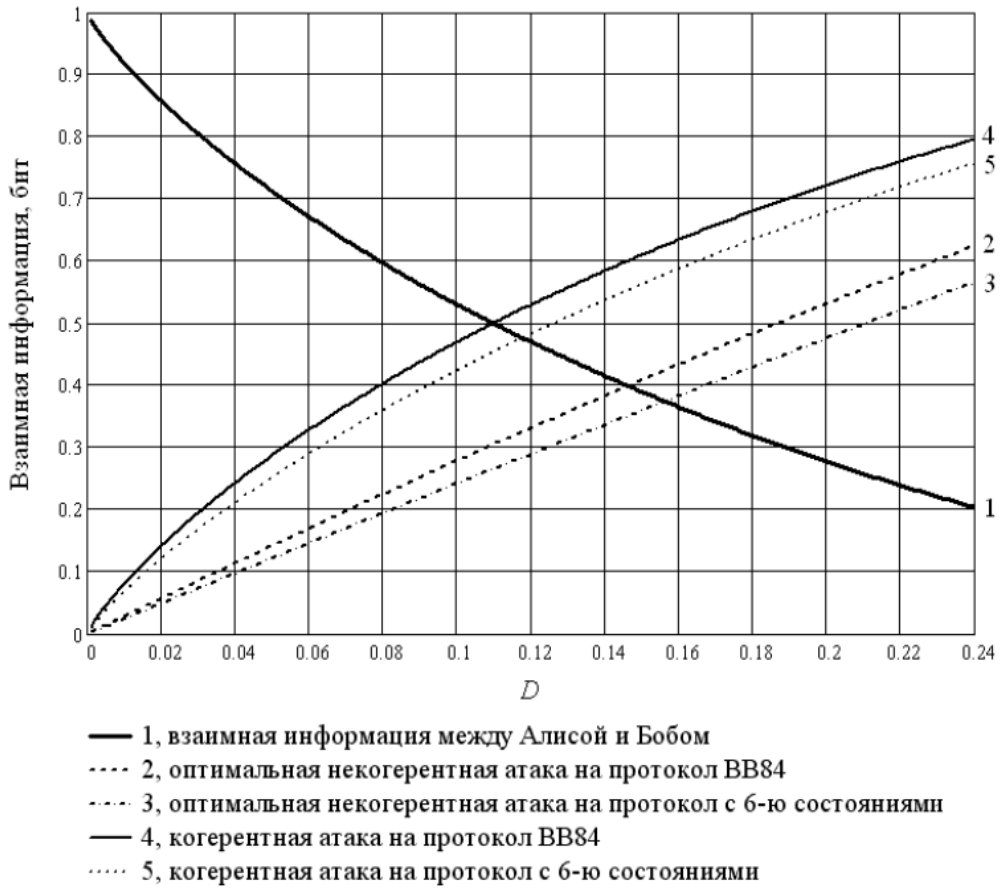


Рисунок 2 - Взаимная информация $I_{AB}(D)$ (кривая 1) и $I_{AE}(D)$ для различных стратегий атак на протокол BB84 (кривые 2-5)

Протокол с 6-ю состояниями является более стойким, чем протокол BB84, однако преимущество протокола с 6-ю состояниями невелико – при заданном D Ева получает меньше информации максимум на 5,8% при оптимальной некогерентной атаке и максимум на 4,7% при когерентной. С другой стороны, верхняя граница уровня ошибок, при которой протокол может быть реализован с использованием процедуры усиления секретности, для протокола с 6-ю состояниями также не намного выше, чем для BB84: 11,8% против 11%. Учитывая, что средняя эффективность протокола с 6-ю состояниями равна 1/3, в то время как для BB84 она равна 1/2, что приводит к значительно меньшей скорости передачи ключа в

протоколе с 6-ю состояниями, можно сделать вывод, что этот протокол практически не имеет никаких преимуществ по сравнению с протоколом BB84.

Атака разделения числа фотонов на протокол BB84 является достаточно мощной. Однако, при использовании в качестве источника сигналов слабых когерентных импульсов со средним числом фотонов в импульсе порядка 0,1, а также при использовании квантовых каналов с малыми потерями ($\eta$=0,9÷1), при такой атаке Алиса и Боб смогут установить секретный ключ, если уровень ошибок при передаче не превышает ~14%. Платой за секретность в данном случае является очень низкая эффективность протокола и, соответственно, низкая скорость передачи ключа.

## Список использованной литературы

1. Lutkenhaus N. Estimates for practical quantum cryptography // Physical Review A.- 1999.-V. 59, №5.- P. 3301-3319.

2. Hwang W., Ahn D., Hwang S. Eavesdropper's optimal information in variations of Bennett–Brassard 1984 quantum key distribution in the coherent attacks // Physics Letters A.- 2001.-V. 279, № 3-4.- P. 133-138.

3. Williamson M., Vedral V. Eavesdropping on practical quantum cryptography // Journal of Modern Optics.- 2003.- V. 50, № 13.- P. 1989-2011.

4. Niederberger A., Scarani V., Gisin N. Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography// Physical Review A.- 2005.- V. 71.- Art. 042316.

5. Bruss D. Optimal Eavesdropping in Quantum Cryptography with Six States // Physical Review Letters.- 1998.- V. 81, № 14.- P. 3018–3021.