УДК 003.26:621.39

Стойкость квантовых протоколов распределения ключей типа «приготовление-измерение»

Василиу Е.В.
Одесская национальная академия связи им. А.С. Попова, 65029, ул. Кузнечная 1, Одесса, Украина
vasiliu@te.net.ua

Аннотация

В работе проведен комплексный анализ стойкости двух протоколов типа «приготовление – измерение» к различным стратегиям атак подслушивающего агента. Показано, что протокол с 6-ю состояниями является незначительно более стойким, чем протокол BB84, как к некогерентной, так и к когерентной атаке. Детально проанализирована также атака разделения числа фотонов на протокол BB84.

***Ключевые слова**: квантовая криптография, протоколы BB84 и с 6-ю состояниями, некогерентная и когерентная атаки, атака разделения числа фотонов, взаимная информация.*

1. Введение

Квантовая криптография, способ применения законов квантовой физики для сведения на нет всех усилий подслушивающего агента, вырос за последнее десятилетие от уровня основополагающей идеи в целое мультидисциплинарное научное направление [1,2]. В настоящее время квантовая криптография включает несколько разделов: квантовые протоколы распределения ключей (КПРК), квантовые протоколы защищенной прямой связи, аутентификацию квантовых сообщения и квантовую цифровую подпись. Из перечисленных направлений в последние годы наибольшее внимание уделяется квантовому распределению ключей, фактически уже существуют опытные коммерческие образцы таких систем. Поэтому детальный анализ надежности различных КПРК является задачей первостепенной важности.

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, т.е. каналу для передачи отдельных квантовых частиц, например, фотонов, и открытому обычному каналу с возможностью аутентификации отправителя сообщения [2]. Переданные по квантовому каналу биты используются для создания секретного ключа, которым затем шифруются сообщения, передаваемые по любому открытому каналу, например, с использованием классической криптографической схемы одноразовых блокнотов. 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 [1,2]. Таким образом, подслушивающий агент, по традиции называемый Евой, вносит в передаваемую последовательность бит определенный процент ошибок. Если уровень ошибок при передаче значительно превышает естественный уровень помех в канале (который, разумеется, должен быть известен Алисе и Бобу), то это служит сигналом к прерыванию процедуры передачи ключа.

Однако, законы квантовой механики, благодаря которым существует возможность обнаружить Еву, также допускают и различные виды атак на квантовый канал связи. При этом Ева, как правило, не имеет возможности полностью узнать ключ, так как уровень вносимых ею помех будет при этом запредельным. Однако, используя определенные стратегии подслушивания, квантовую память для хранения состояний частиц и квантовые

вентили для вычислений, Ева может узнать некоторую часть ключа, внося при этом меньшее количество ошибок.

Стек КПРК включает специальную процедуру усиления секретности, при которой длина переданного ключа уменьшается на некоторое число бит, которое зависит от уровня ошибок при передаче [2,3]. Тем самым уменьшается до приемлемого уровня количество информации о ключе, которое могла получить Ева. Например, для протоколов с одиночными частицами длина окончательного ключа принимается равной [3]:

$$n_{fin} = n_{rec}(1-\tau) - n_S, \quad (1)$$

где n_{rec} – длина ключа после процедуры согласования, включающей исправление ошибок или отбрасывание несогласующихся битов Алисы и Боба; τ – доля битов, на которую должен быть уменьшен ключ вследствие возможного перехвата и n_S – дополнительный параметр безопасности. Укорочение окончательного ключа дополнительно на n_S бит уменьшает доступную Еве информацию о ключе экспоненциально в зависимости от значения n_S [3].

Величина τ определяется для каждого сеанса передачи ключа на этапе согласования в зависимости от оцененного Алисой и Бобом процента ошибок в данном сеансе. Уровень же ошибок показывает, сколько информации могла получить Ева о ключе. Это позволяет установить минимальное значение $\tau_{\min}$ для конкретного сеанса, при котором количество полученной Евой информации не будет превышать некоторой малой величины, приемлемой для конкретного криптографического приложения.

Таким образом, для практического определения $\tau_{\min}$ в конкретном сеансе передачи ключа, необходимо знать теоретические зависимости количества получаемой Евой информации от среднего уровня вносимых ею ошибок D для определенного КПРК и определенных стратегий атак на данный КПРК. Такие зависимости даются наибольшей из двух величин: взаимной информации Шеннона между Алисой и Евой $I_{AE}(D)$ или между Евой и Бобом $I_{EB}(D)$, где I измеряется в битах на 1 бит просеянного ключа. Для рассмотренных в настоящей работе атак Евы $I_{AE}(D) = I_{EB}(D)$, поэтому в дальнейшем будем использовать $I_{AE}(D)$. Эта величина сильно отличается для различных протоколов, а также для различных стратегий атак. Поэтому, сравнивая зависимости $I_{AE}(D)$, можно, с одной стороны, установить степень надежности конкретного протокола против различных стратегий атак, а с другой стороны, оценить надежность различных протоколов против одной и той же стратегии подслушивания.

Следует подчеркнуть, что от величины τ существенно зависит скорость генерации ключей в криптографической системе. Чем выше уровень стойкости протокола, т.е. чем меньше I_{AE} при заданном D, тем меньше будет $\tau_{\min}$ и тем выше скорость генерации секретных ключей.

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 [4].

Большинство из предложенных в настоящее время КПРК используют для передачи битов двухуровневые квантовые системы – кубиты. При этом существует два класса таких протоколов. Первый – это схемы с одиночными кубитами (например, фотонами, линейно поляризованными в двух взаимно-перпендикулярных направлениях), такие схемы называют

также «приготовление – измерение кубитов». Второй класс – это протоколы, основанные на квантовых корреляциях (перепутывании) двух кубитов.

Целью настоящей работы является анализ стойкости двух протоколов с передачей кубитов, относящихся к типу «приготовление – измерение», к различным стратегиям атак подслушивающего агента.

Следует отметить, что доказательство стойкости всего протокола квантового распределения ключа (при любых возможных стратегиях атак) является трудной теоретической задачей квантовой криптографии, которая в настоящее время не решена полностью ни для одного протокола. Однако некоторые аспекты безопасности различных КПРК уже анализировались в литературе. В частности для некоторых протоколов и для некоторых конкретных стратегий атак уже получены зависимости $I_{AE}(D)$. Однако авторы этих работ, как правило, рассматривают некоторый конкретный протокол и некоторый конкретный класс атак на этот протокол, не проводя при этом сравнительного анализа с другими классами атак и другими протоколами. Сказанным также обуславливается актуальность данной работы.

2. Стратегии атак подслушивающего агента

Простейшим видом съема информации в обычных оптических телекоммуникационных системах является разделение пучка фотонов. Однако в протоколах квантовой криптографии передача должна происходить посредством одиночных фотонов, и в таком случае Ева не может ответвить часть сигнала. Поэтому данный вид атак не применим в квантово-криптографических системах в идеальных условиях однофотонных сигналов. Однако такие источники сигналов пока не созданы. На практике в настоящее время используют слабые когерентные импульсы, излучаемые лазерными светодиодами [1]. Число фотонов в импульсе определяется распределением Пуассона, т.е. часть передаваемых импульсов содержит два и более фотонов. Поэтому атаки с разделением пучка фотонов в настоящее время возможны и в квантовой криптографии. Оценка количества попадающей к Еве информации о ключе при таких атаках дана ниже.

Основные стратегии атак, которые может использовать Ева в случае, когда все сигналы содержат строго один фотон, подразделяют на два класса [2].

К первому классу относят *некогерентные* или индивидуальные атаки. При таких атаках Ева обрабатывает каждый фотон Алисы отдельно. Простейшим вариантом является атака перехвата – повторной отправки 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*.

Отметим, что практическая реализация таких атак в настоящее время наталкивается на трудность физической реализации надежной квантовой памяти необходимого объема, а также на трудность физической реализации унитарных преобразований, перепутывающих пробы Евы с фотонами Алисы в необходимом базисе.

Следует подчеркнуть, что 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, иногда называют *объединенной* (*joint*) атакой [1], хотя некоторые авторы не выделяют отдельно этот предельный случай и называют когерентной любую атаку, при которой Ева обрабатывает несколько кубитов когерентно [2]. 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. Отметим, что такие атаки, кроме большой квантовой памяти, могут требовать наличия у Евы многокубитного квантового компьютера (пока не созданного), т.е. в настоящее время технически неосуществимы.

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.

3. Атаки на протокол BB84 для случая однофотонных сигналов

Первым в 1984 г. был предложен квантовый протокол распределения ключа, использующий 4 квантовых состояния – два неортогональных состояния для кодирования 0 и два – для кодирования 1. Например, Алиса использует либо $\oplus$-базис, соответствующий вертикальной (0) или горизонтальной (1) линейной поляризации фотонов, либо $\otimes$-базис, соответствующий двум диагональным линейным поляризациям, также кодирующим 0 и 1. Алиса случайным образом выбирает базис и поляризацию своих однофотонных импульсов и посылает их Бобу, а Боб также случайно выбирает один из двух базисов для измерения поляризации. Этот протокол носит название BB84 [1,2].

Отметим, что в данной работе рассматриваются только *несмещенные* протоколы. В этом случае Алиса (Боб) выбирает базисы для генерации (измерения) фотонов из двух возможных для BB84 (или трех для протокола с 6-ю состояниями) с равной вероятностью. Кроме того, рассматриваются только стандартные варианты протоколов «без задержки», т.е. Боб измеряет состояния кубитов Алисы сразу после их получения, а не хранит кубиты в квантовой памяти до тех пор, пока Алиса не объявит базисы.

Взаимная информация между Алисой и Бобом для всех КПРК, основанных на передаче кубитов, определяется выражением [5]:

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

где функция φ дается формулой:

$$\varphi(z) = (1-z)\log_2(1-z) + (1+z)\log_2(1+z)\,. \tag{3}$$

Рассмотрим сначала некогерентные атаки Евы. При атаке перехвата – повторной отправки фотонов Ева может использовать те же базисы, что Алиса и Боб (если эти базисы ей известны). В этом случае $I_{AE} = 2D$ [5]. Однако Ева может не знать базисов Алисы и Боба и использовать два базиса, повернутых относительно их базисов на некоторый угол. В этом случае вероятность правильно определить значение бита для Евы уменьшается, соответственно уменьшается и доступная ей информация.

Следующим видом некогерентных атак является использование Евой проб, индивидуально перепутываемых с кубитами Алисы, т.е. полупрозрачная некогерентная атака. В [6] был проведен анализ такой атаки для случая, когда в качестве проб Ева также использует кубиты. Когда Алиса посылает кубит Бобу в некотором состоянии $|\psi\rangle$, Ева перепутывает его со своей пробой. Первоначально проба Евы находится в некотором

известном состоянии $|0\rangle$ и совместное состояние неизвестного (для Евы) кубита и пробы – тензорное произведение $|\psi\rangle\otimes|0\rangle$. Это состояние подвергается некоторой унитарной эволюции, после чего неизвестный кубит отправляется Бобу, который производит стандартное измерение, безотносительно к стратегии Евы. Ева может либо измерить состояние своей пробы немедленно, либо хранить ее в квантовой памяти и ждать, пока Алиса и Боб объявят базис, который они использовали для кодирования данного бита, а затем провести измерение состояния пробы.

Используя результаты [6], для взаимной шенноновской информации между Алисой и Евой $I_{AE}(D)$ в случае, когда Ева измеряет состояние пробы сразу после перепутывания с фотоном Алисы, можно получить следующее выражение:

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

где $\chi(z)=(1-z)\log_2(1-z)$.

Однако эта атака не является оптимальной для Евы, так как она не ждет объявления использованных Алисой базисов. Кроме того, полученная Евой средняя информация I_{AE} для заданного среднего уровня ошибок D существенно зависит от выбора оператора измерения для ее пробы. Оптимизация некогерентной атаки Евы в смысле выбора оптимального оператора измерения из класса положительно определенных операторных мер (с учетом объявленного Алисой базиса) была выполнена в [7]. Мы воспользуемся результатом этой работы для случая равновероятного использования двух базисов в протоколе BB84:

$$I_{AE}(D)=\tfrac{1}{2}\varphi\left(2\sqrt{D(1-D)}\right), \quad (5)$$

где $\varphi(z)$ определено в (3).

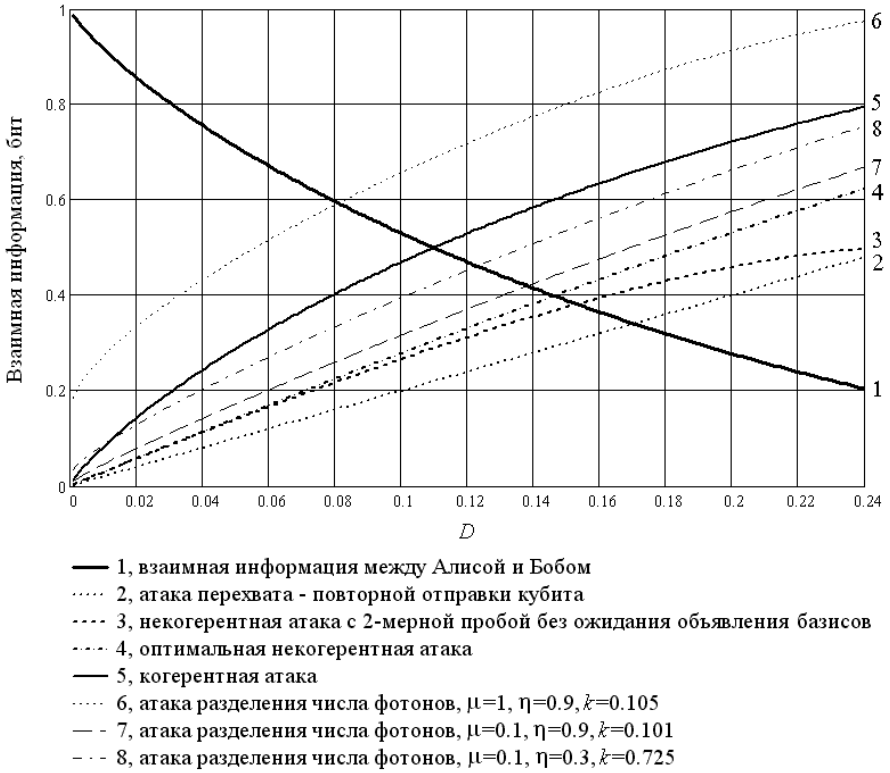

Рис. 1. Взаимная информация $I_{AB}(D)$ (кривая 1) и $I_{AE}(D)$ для различных стратегий атак на протокол BB84 (кривые 2–8)

На рис. 1 приведены зависимости $I_{AE}(D)$ для трех вышеописанных атак (кривые 2-4). Видно, что при атаке перехвата – повторной отправки кубитов Ева получает меньше информации о ключе, чем при полупрозрачных атаках, для любых D. Что касается выгоды Евы от оптимизации своей полупрозрачной атаки, то некоторый выигрыш в информации она

может получить лишь при достаточно больших *D*, когда Алиса и Боб наверняка прервут свой протокол передачи ключа (сравнить кривые 3 и 4). Отсюда следует вывод, что ожидание объявления базисов и оптимизация измерительной процедуры не приносит Евы большой выгоды при некогерентных атаках на протокол BB84.

Рассмотрим теперь когерентную атаку. В [8] была предложена общая схема вычисления $I_{AE}(D)$ при когерентной атаке на протоколы, основанные на передаче кубитов. В этой схеме $I_{AE}(D)$ вычисляется для КПРК с максимально перепутанными парами кубитов (состояния Белла), а затем схема, основанная на перепутывании, сводится к схеме, основанной на передаче одиночных кубитов. Таким образом, можно вычислить $I_{AE}(D)$ при когерентной атаке на протокол BB84 и на протокол с 6-ю состояниями.

Схема вычисления $I_{AE}(D)$ состоит в следующем [8]. Состояния базиса Белла $\left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle \pm |1\rangle|0\rangle\right)$ и $\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle \pm |1\rangle|1\rangle\right)$ кодируют два классических бита: $\left|\Phi^{+}\right\rangle = 00$, $\left|\Psi^{+}\right\rangle = 01$, $\left|\Phi^{-}\right\rangle = 10$, $\left|\Psi^{-}\right\rangle = 11$. Ева готовит состояние

$$|u\rangle = \sum_{i_1,i_2,\ldots,i_N} \sum_{j} \alpha_{i_1,i_2,\ldots,i_N,j} |i_1,i_2,\ldots,i_N\rangle \otimes |j\rangle, \qquad (6)$$

где i_k обозначает состояние *k*-ой пары, которое является одним из $\Psi^{\pm}$ или $\Phi^{\pm}$, $\alpha_{i_1,i_2,\ldots,i_N,j}$ – некоторые комплексные коэффициенты, значения $|j\rangle$ формируют ортонормированный базис пробы Евы, *N* – общее число переданных пар кубитов.

Ева посылает состояние (6) Алисе и Бобу, которые для каждого кубита независимо и случайно выполняют проективные измерения посредством операторов $\hat{S}_z = \left\{|0\rangle\langle 0|; |1\rangle\langle 1|\right\}$, $\hat{S}_x = \left\{|\overline{0}\rangle\langle\overline{0}|; |\overline{1}\rangle\langle\overline{1}|\right\}$ или $\hat{S}_y = \left\{|\overline{\overline{0}}\rangle\langle\overline{\overline{0}}|; |\overline{\overline{1}}\rangle\langle\overline{\overline{1}}|\right\}$, где $|\overline{0}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$, $|\overline{1}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$, $|\overline{\overline{0}}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right)$ и $|\overline{\overline{1}}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right)$.

Используя неравенство $I_{AE} \le S(\rho_{AB})$, где *S* – энтропия фон Неймана и приведенная матрица плотности ρ_{AB} вычисляется взятием частичного следа по подпространству состояний пробы Евы $\rho_{AB} = Tr_{Eve}|u\rangle\langle u|$, можно получить [8]:

$$I_{AE} \le -\sum_{i_1,i_2,\ldots,i_N} P_{i_1,i_2,\ldots,i_N} \log_2 P_{i_1,i_2,\ldots,i_N} = \log_2 \Omega, \qquad (7)$$

где Ω – число различных $|i_1,i_2,\ldots,i_N\rangle$, дающих вклад в средний уровень ошибок *D*, и $P_{i_1,i_2,\ldots,i_N} = \sum_j \left|\alpha_{i_1,i_2,\ldots,i_N,j}\right|^2$.

Величина Ω зависит от типа протокола и для BB84 имеет вид [8] $\Omega = \sum_{\frac{1}{2}(b+c)+d=D} \frac{N!}{a!b!c!d!}$, где *a*, *b*, *c* и *d* – количество элементов множеств $A = \{i_k \mid i_k = 11\}$, $B = \{i_k \mid i_k = 10\}$, $C = \{i_k \mid i_k = 01\}$ и $D = \{i_k \mid i_k = 00\}$ соответственно (здесь схема протокола с перепутанными кубитами сводится к схеме протокола с одиночными кубитами). Далее, предполагая, что в сумме доминирует лишь одно (максимальное) слагаемое и пренебрегая остальными, а также используя асимптотическую формулу Стирлинга $\log_2(n!) = n\log_2 n - n$ и равенства $\frac{1}{2}(b+c) + d = ND$, $b = c$ (первое равенство следует из схемы протокола BB84, второе – из условия максимума информации Евы при заданном *D*, см. [8]), можно получить:

$$\log_2 \Omega = \max\left\{(N - 2ND + d)\log_2 \frac{N - 2ND + d}{N} + 2(ND - d)\log_2 \frac{ND - d}{N} + d\log_2 \frac{d}{N}\right\}. \qquad (8)$$

Это выражения достигает максимума при $d = ND^2$, тогда после тождественных преобразований и деления на число кубитов $2N$, окончательно получим:

$$I_{AE}^{(\max)}(D) = 1 - \tfrac{1}{2}\varphi(1-2D), \tag{9}$$

где $\varphi(z)$ определено в (3).

На рис. 1 когерентной атаке соответствует кривая 5. Как видно, при такой атаке Ева может получить значительно больше информации о ключе, чем при некогерентных атаках. Это вполне ожидаемый результат – когерентная атака на КПРК является наиболее общей и позволяет получить тот максимум информации при подслушивании, который допускается законами квантовой механики. Однако, как отмечалось выше, практически такая атака неосуществима при сегодняшнем уровне технологий.

4. Атака разделения числа фотонов на протокол BB84

Рассмотренными в предыдущем разделе случаями исчерпываются основные стратегии атак на протокол BB84 при использовании Алисой однофотонных источников. Как отмечено выше, такие источники пока не созданы и на практике используют слабые когерентные импульсы, излучаемые лазерными светодиодами [1]. Вероятность того, что импульс содержит n фотонов определяется распределением Пуассона:

$$p_n = e^{-\mu}\frac{\mu^n}{n!}, \tag{10}$$

где μ – среднее число фотонов в импульсе.

В случае квантового канала с потерями, вероятность того, что Боб зарегистрирует в полученном импульсе n фотонов определяется формулой:

$$p_{n,\,loss} = e^{-\eta\mu}\frac{(\eta\mu)^n}{n!}, \tag{11}$$

где η – коэффициент передачи канала.

Вероятность зарегистрировать в импульсе более одного фотона дается формулой

$$p_{n>1,\,loss} = 1 - e^{-\eta\mu}(1+\eta\mu). \tag{12}$$

Таким образом, становится возможной атака разделения числа фотонов (photon number splitting attack) [9,10]. Для каждого импульса Ева должна выполнить квантовое неразрушающее измерение числа фотонов в импульсе, не влияя при этом на их поляризацию. Отметим, что такое измерение очень сложно выполнить, однако в настоящее время это технически возможно [9].

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. В этом случае, очевидно, она вносит ошибки в просеянный ключ, количество которых будет зависеть как от типа атаки, так и от доли однофотонных импульсов при передаче ключа.

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. При этом, однако, Ева может быть обнаружена другим способом, так как Боб, зная вероятность получить пустой

импульс $p_0 = e^{-\eta\mu}$, может обнаружить значительное превышение их количества над ожидаемым. Отметим, что Боб может также не только определять количество пустых импульсов, но и контролировать всю статистику получаемых им сигналов, выполняя неразрушающее измерение числа фотонов в импульсе. В этом случае Ева вынуждена будет отводить фотон только у небольшой части многофотонных импульсов, а остальные пропускать, не получая никакой информации.

В работах [9-11] 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 [11]. На рис. 2 эта область выделена серым цветом. Отметим, что на практике для передачи ключа по протоколу BB84 с помощью слабых когерентных импульсов используют источники с μ порядка 0,1. Этому на рис. 2 соответствует серая область $\eta < 0{,}176$, 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 (детали см., например, в [10]).

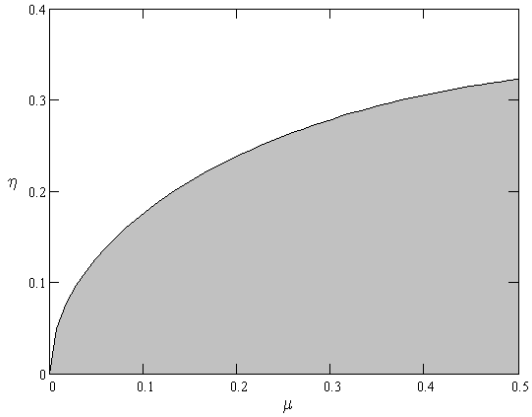

Рис. 2. Область параметров η и μ, где атака разделения числа фотонов будет успешна при замене исходного канала с потерями на идеальный [11]

Для вычисления $I_{AE}(D)$, следуя [9], рассмотрим следующую стратегию перехвата. Ева блокирует некоторую долю k однофотонных импульсов, а к остальным применяет некогерентную атаку. В свою очередь, от каждого многофотонного импульса Ева отводит один фотон и получает точное значение бита, измеряя состояние пробы после объявления базисов, как описано выше. Ошибки у Боба возникают только при атаке на неблокированные однофотонные импульсы, доля которых равна $1-k$.

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 ($\eta = 1$) и блокирует часть однофотонных импульсов:

$$1 - e^{-\eta\mu} = (1-k)p_1 + p_{n>1}, \tag{13}$$

откуда с использованием (10) получим

$$k = \frac{1}{\mu}\left(e^{\mu(1-\eta)} - 1\right). \tag{14}$$

Вероятность для Евы правильно измерить состояние пробы, перепутанной с фотоном Алисы, дается выражением [9]:

$$P_{correct} = \frac{1 - e^{-\mu}(1+\mu) + (1-k)\mu e^{-\mu}\left(1/2 + \sqrt{D(1-D)}\right)}{1 - e^{-\mu}(1+\mu k)}. \quad (15)$$

Так как вероятность для Евы неверно измерить состояние пробы равна $(1 - P_{correct})$, то $I_{AE}(D)$ для описанной атаки просто равна (см. выражение (2) для $I_{AB}(D)$):

$$I_{AE}(D) = \tfrac{1}{2}\varphi[1 - 2(1 - P_{correct})], \quad (16)$$

где $\varphi(z)$ определено в (3).

На рис. 1 приведены зависимости $I_{AE}(D)$ (16) для различных значений μ и η (кривые 6-8). Видно, что при любых параметрах η и μ Ева получает больше информации, чем при некогерентных атаках для строго однофотонных источников сигнала. При этом, разумеется, чем больше потери в канале, тем больше информации получит Ева (сравнить кривые 7 и 8), так как при увеличении потерь Ева может блокировать больше однофотонных импульсов, и, соответственно, использовать больше многофотонных. При $\mu = 1$ (кривая 6) количество информации у Евы будет значительно больше, чем при $\mu = 0{,}1$. Так при $\mu = 1$, даже для канала с небольшими потерями $(\eta = 0{,}9)$, внося всего 5% ошибок, Ева может узнать почти половину битов ключа. Очевидно, что в этом случае Алиса и Боб не могут использовать протокол BB84 для распределения секретного ключа. Поэтому для практической реализации протокола и рекомендуется использовать слабые когерентные импульсы с $\mu \le 0{,}1$. Обратной стороной этого является низкая скорость передачи, так как даже при полном отсутствии потерь в канале и при $\mu = 0{,}1$, в среднем только один из десяти импульсов содержит хотя бы один фотон.

Из нашего анализа следует также, что даже при использовании источника с $\mu = 0{,}1$ атака разделения числа фотонов достаточно эффективна – она, разумеется, будет эффективнее любой некогерентной атаки для однофотонных источников, а для каналов с большими потерями приближается по эффективности к когерентной атаке (см. рис. 1). Этим и обусловлена, в частности, необходимость создания однофотонных источников, что позволит значительно увеличить скорость передачи при использовании протокола BB84, а также повысить его надежность.

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

Этот протокол является расширением BB84 и использует максимально возможное число базисов для двухуровневых систем – три сопряженных базиса, в отличие от двух для BB84. Таким образом, Алиса использует для кодирования 0 и 1 один из трех базисов с равной вероятностью: $\{|0\rangle, |1\rangle\}$, $\left\{|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |\bar{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$ или $\left\{|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |\bar{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\right\}$ [12]. В остальном стадии этого протокола совпадают со стадиями BB84. Эффективность протокола с 6-ю состояниями меньше эффективности BB84, так как для генерации ключа здесь используется в среднем только $1/3$ переданных кубитов.

В работе [12] был проведен анализ и оптимизация полупрозрачной некогерентной атаки Евы на протокол с 6-ю состояниями, когда она использует двухкубитную пробу в начальном состоянии

$$|X\rangle = \alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \delta|11\rangle, \quad (17)$$

где комплексные коэффициенты α, β, γ и δ удовлетворяют условию

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1. \quad (18)$$

При этом предполагалось, что Ева обрабатывает все шесть возможных состояний одинаковым образом, то есть создает в среднем одинаковый процент ошибок в каждом

базисе. Иначе Алиса и Боб могли бы обнаружить подслушивание, сравнивая уровни ошибок по отдельности для каждого из базисов. Отметим, что подобное предположение делалось и для протокола BB84 в [7], что позволяет нам непосредственно сравнить эффективность оптимальной некогерентной атаки на эти протоколы.

Взаимная информация между Алисой и Евой для оптимальной некогерентной атаки на протокол с 6-ю состояниями дается выражением [12]:

$$I_{AE}(D) = 1 + (1-D)\left[f(D)\log_2 f(D) + (1-f(D))\log_2(1-f(D))\right], \qquad (19)$$

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 (см. п. 3). При этом вместо условий $\frac{1}{2}(b+c)+d = ND$, $b = c$ и $d = ND^2$ для протокола BB84 (первое следует из схемы протокола, остальные – из условия максимума информации Евы при заданном D) для протокола с 6-ю состояниями используются следующие: $\frac{1}{2}(b+c+d) = ND$, $b = c = d$ и $d = \frac{1}{2}ND$ [8]. Тогда выражение (7) можно окончательно привести к следующему виду:

$$I_{AE}(D) = -\tfrac{1}{2}\left[\left(1-\tfrac{3}{2}D\right)\log_2\left(1-\tfrac{3}{2}D\right) + \tfrac{3}{2}D\log_2\left(\tfrac{1}{2}D\right)\right]. \qquad (20)$$

На рис. 3 показаны зависимости $I_{AE}(D)$ для оптимальной некогерентной атаки на протоколы BB84 (5) и с 6-ю состояниями (19), а также для когерентной атаки на эти протоколы ((9) и (20) соответственно). Видно, что при всех D кривые для протокола с 6-ю состояниями лежат ниже соответствующих кривых для BB84. Это означает несколько большую стойкость протокола с 6-ю состояниями к указанным атакам.

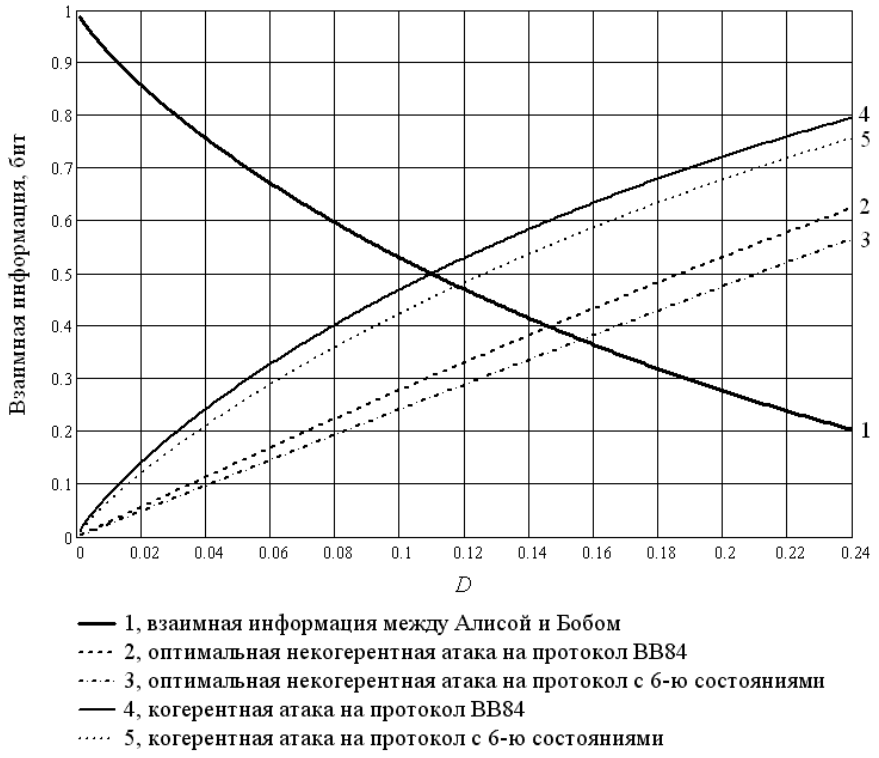

Рис. 3. Взаимная информация $I_{AB}(D)$ (кривая 1) и $I_{AE}(D)$ для различных стратегий атак на протокол с 6-ю состояниями (кривые 2–5)

На рис. 4 показана разность

$$\Delta(D) = I_{AE}^{(BB84)}(D) - I_{AE}^{(6-state)}(D) \qquad (21)$$

для оптимальной некогерентной атаки и когерентной атаки. Видно, что при некогерентной атаке на протокол с 6-ю состояниями, по сравнению с атакой на BB84, Ева получит меньше

информации максимум на 5,8 % при $D \approx 0{,}244$. Однако такой высокий уровень ошибок практически не приемлем для реализации протоколов, а для приемлемого уровня $D \sim 10\%$ преимущество протокола с 6-ю состояниями составляет менее 4%. Для когерентной атаки кривая $\Delta(D)$ имеет максимум, равный 4,7 %, при $D \approx 0{,}139$. Таким образом, и по отношению к когерентной атаке протокол с 6-ю состояниями обладает небольшим преимуществом над протоколом BB84.

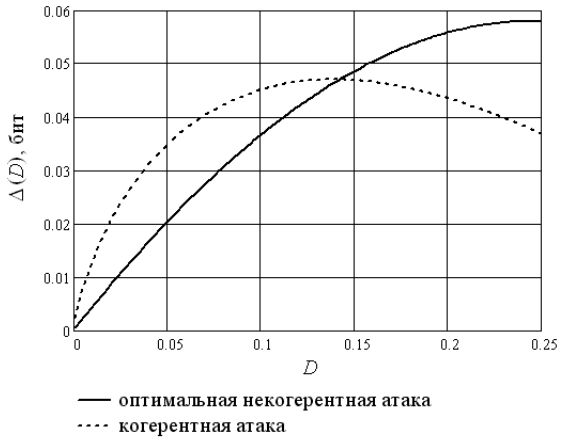

Рис. 4. $\Delta(D)$ (21) для некогерентной и когерентной атак

Согласно теореме Цизара и Кёрнера [13], Алиса и Боб могут установить секретный ключ, если взаимная информация между ними больше взаимной информации между Алисой и Евой, т.е. ключ может быть установлен только в том интервале ошибок D, где $I_{AB}(D) > I_{AE}(D)$. В этом случае, используя однонаправленный классический канал связи от Алисы к Бобу (с аутентификацией), они могут провести процедуру усиления секретности, после которой информация Евы о ключе станет пренебрежимо малой [1]. В случае если Алиса и Боб не ограничены однонаправленным каналом, то, применяя специальную процедуру преимущественной очистки (advantage distillation), они могут установить секретный ключ, даже если неравенство $I_{AB}(D) > I_{AE}(D)$ не выполняется [1]. Однако, такая процедура гораздо менее эффективна, чем стандартная процедура усиления секретности [1]. Поэтому в квантовой криптографии верхней границей допустимого уровня ошибок, как правило, считают значение D, получаемое из равенства $I_{AB}(D) = I_{AE}(D)$. На рис. 1 и 3 это значение D соответствует точкам пересечения соответствующих кривых.

Так, если Ева применяет лишь простую атаку перехвата – повторной отправки кубитов, протокол BB84 будет безопасным вплоть до $D \approx 17\%$. Для оптимальной некогерентной атаки Евы соответствующие границы $D \approx 14{,}6\%$ для BB84 и $D \approx 15{,}6\%$ для протокола с 6-ю состояниями. Для когерентной атаки $D \approx 11\%$ и $D \approx 11{,}8\%$ соответственно. Таким образом, протокол с 6-ю состояниями может быть успешно реализован при несколько более высоком уровне ошибок, чем протокол BB84, независимо от типа применяемой атаки.

Что касается атаки разделения числа фотонов на протокол BB84, то приведем соответствующую границу для $\mu = 0{,}1$ и $\eta = 0{,}9$, что приблизительно соответствует параметрам используемого на практике оборудования. Эта граница $D \approx 13{,}8\%$ и лежит между соответствующих границ для некогерентной и когерентной атак на однофотонные сигналы, ближе к границе для оптимальной некогерентной атаки. Такой результат вполне естественен, так как Ева блокирует долю k однофотонных импульсов ($k = 0{,}101$ для указанных μ и η), а к остальным применяет оптимальную некогерентную атаку. Так как в данном случае k мало, то стойкость протокола BB84 к атаке разделения числа фотонов не намного меньше, чем к оптимальной некогерентной атаке.

6. Обсуждение результатов

В работе проанализированы различные виды атак на два КПРК, использующих для передачи ключа кубиты, с целью сравнения стойкости этих протоколов к различным атакам. Протокол считается более стойким, если он допускает более высокий уровень ошибок, при котором Алиса и Боб могут установить секретный ключ с использованием процедур исправления ошибок и усиления секретности [14].

Исходя из вышеназванного критерия, следует сделать вывод, что 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 (см. рис. 1). 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 ($\eta = 0{,}9 \div 1$), 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.

Литература:

1. *Gisin N., Ribordy G., Tittel W., Zbinden H*. Quantum cryptography // Reviews of Modern Physics.- 2002.- V. 74, №1.- P. 145-195.
2. *Баумейстер Д., Экерт А., Цайлингер А*. Физика квантовой информации.- Москва: «Постмаркет», 2002.
3. *Lutkenhaus N.* Estimates for practical quantum cryptography // Physical Review A.- 1999.- V. 59, №5.- P. 3301-3319.
4. *Elliott C., Colvin A., Pearson D., Pikalo O., Schlafer J., Yeh H*. Current status of the DARPA Quantum Network.- Preprint: http://www.arxiv.org/abs/quant-ph/0503058.- 2005.- 12 p.
5. *Bechmann-Pasquinucci H*. Eavesdropping without quantum memory // Physical Review A.- 2006.- V. 73.- Art. 044305.
6. *Gisin N., Huttner B.* Quantum Cloning, Eavesdropping and Bell's inequality // Physical Letters A.- 1997.- V. 228.- P. 13-21.
7. *Fuchs C., Gisin N., Griffiths R., Niu C., Peres A.* Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy // Physical Review A.- 1997.- V. 56, № 2.- P. 1163–1172.
8. *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.
9. *Williamson M., Vedral V*. Eavesdropping on practical quantum cryptography // Journal of Modern Optics.- 2003.- V. 50, № 13.- P. 1989-2011.
10. *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.
11. *Lutkenhaus N., Jahma M.* Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack // New Journal of Physics.- 2002.- V. 4.- P. 44.1-44.9.
12. *Bruss D*. Optimal Eavesdropping in Quantum Cryptography with Six States // Physical Review Letters.- 1998.- V. 81, № 14.- P. 3018–3021.
13. *Csiszar I., Korner J*. Broadcast channels with confidential messages // IEEE Transactions on Information Theory.- 1978.- V. IT-24, № 3.- P. 339-348.
14. *Caruso F., Bechmann-Pasquinucci H., Macchiavello C*. Robustness of a quantum key distribution with two and three mutually unbiased bases // Physical Review A.- 2005.-V. 72.- Art. 032340.

В статье 4 рис., нет диаграмм и таблиц

Статья получена: 2007-01-30