УДК 003.26:621.39

Василиу Е.В., Горохов С.М.
Vasiliu E.V., Gorohov S.M.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТОЙКОСТИ ДВУХ КВАНТОВЫХ ПРОТОКОЛОВ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ПЕРЕДАЧЕЙ КУБИТОВ

COMPARATIVE ANALYSIS OF ROBUSTNESS OF TWO QUANTUM KEY DISTRIBUTION PROTOCOLS WITH QUBITS TRANSFER

Аннотация. На основе имеющихся в литературе результатов исследований стойкости квантовых протоколов распределения ключей к различным атакам подслушивающего агента проведен комплексный анализ надежности двух протоколов. Показано, что протокол с шестью состояниями является незначительно более стойким, чем протокол BB84, как к некогерентной, так и к когерентной атаке. Однако протокол с шестью состояниями имеет значительно меньшую эффективность чем BB84. Таким образом, для практического использования протокол BB84 является более предпочтительным. Детально проанализирована атака разделения числа фотонов на протокол BB84.

Summary. Based on the available results for the security of quantum key distribution protocols against various eavesdropping attacks the complex analysis of robustness of two these protocols is fulfilled. It is shown, that the 6-state protocol is slightly more robust, than the BB84-protocol, both against not coherent, and against coherent attack. However, the 6-state protocol has considerably smaller efficiency, than the BB84-protocol. Thus, for practical use the BB84-protocol is more preferable. The photon number splitting attack against BB84-protocol is analysed in details.

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 сообщений и квантовую цифровую подпись. Из перечисленных направлений квантовой криптографии в последние годы наибольшее внимание уделяется квантовому распределению ключей, фактически уже существуют опытные коммерческие образцы таких систем. Поэтому детальный анализ надежности КПРК в настоящее время является важной научной проблемой.

Большинство из предложенных КПРК используют для передачи битов двухуровневые (2-мерные) квантовые системы – кубиты. При этом каждый кубит кодирует один бит информации. Основными характеристиками таких протоколов являются стойкость к различным стратегиям атак подслушивающего агента, а также эффективность протокола, т.е. отношение количества бит, используемых для генерации ключа, к общему количеству бит, переданных по квантовому каналу связи.

Некоторые аспекты стойкости квантовых протоколов распределения ключей анализировались в литературе [3-11]. В частности, найдены оптимальные стратегии некогерентных атак на протоколы BB84 [6] и протокол с шестью состояниями [11]. Рассматривались также атаки, возможные только при использовании для передачи кубитов неоднофотонных источников сигналов [8-10], а также влияние на стойкость протокола технических параметров источника, детектора и квантового канала [1,8,9]. Однако авторы этих работ, как правило, рассматривают только некоторый конкретный КПРК и некоторую конкретную атаку на него, не проводя сравнительного анализа с другими атаками и другими протоколами. Таким образом, задачи сравнения стойкости данного протокола к различным стратегиям атак на него, и с другой стороны, сравнения стойкости нескольких протоколов к одной и той же стратегии атаки не решены полностью в настоящее время.

Целью настоящей работы является анализ стойкости двух протоколов с передачей кубитов: протокола BB84 и протокола с шестью состояниями к нескольким стратегиям атак подслушивающего агента. Для решения этой задачи необходимо выбрать некоторую величину, характеризующую стойкость протокола к атаке. В квантовой криптографии такой стандартной величиной (хотя и не единственно возможной) является взаимная информация Шеннона между одним из законных пользователей (Алиса и Боб) и подслушивающим агентом (Ева). При этом из двух величин: взаимной информации между Алисой и Евой $I_{\mathrm{AE}}(D)$ и взаимной информации между Евой и Бобом $I_{\mathrm{EB}}(D)$, где D – средний уровень ошибок, вносимых Евой в просеянный ключ, следует выбрать наибольшую. Для рассмотренных в настоящей работе атак $I_{\mathrm{AE}}(D) = I_{\mathrm{EB}}(D)$, поэтому в дальнейшем используется $I_{\mathrm{AE}}(D)$.

1. Атаки на протокол BB84 для случая однофотонных сигналов. Этот протокол использует 4 квантовых состояния – два неортогональных состояния для кодирования 0 и два – для кодирования 1. Например, Алиса использует либо ⊗-базис, соответствующий вертикальной (для кодирования 0) или горизонтальной (для кодирования 1) линейной поляризации фотонов, либо ⊗-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.

Отметим, что в данной работе рассматриваются только *несмещенные* протоколы с одиночными частицами. В этом случае Алиса (Боб) выбирает базисы для генерации (измерения) фотонов из двух возможных для протокола BB84 (или трех для протокола с шестью состояниями) с равной вероятностью, т.е. ни Алиса, ни Боб не отдают предпочтения какому-либо базису.

Взаимная информация между Алисой и Бобом для всех КПРК, основанных на передаче кубитов, дается выражением [4]:

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

где функция $\varphi(z)$ определяется формулой

$$.\varphi(z)=(1-z)\log_2(1-z)+(1+z)\log_2(1+z) \tag{2}$$

Проанализируем сначала некогерентные атаки Евы. При атаке перехвата – повторной отправки фотонов Ева может использовать те же базисы, что Алиса и Боб. В этом случае $I_{\mathrm{AE}}=2D$ [4]. 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. Мы не будем отдельно рассматривать этот случай, так как количество информации о ключе, попадающей к Еве при такой атаке $I_{\mathrm{AE}}<2D$, а эта величина, в свою очередь, меньше, чем доступная Еве информация при любых других видах атак.

Следующим видом некогерентных атак является использование Евой проб, индивидуально перепутываемых с кубитами Алисы, т.е. полупрозрачная некогерентная атака [2]. В работе [5] был проведен анализ такой атаки для случая, когда в качестве проб Ева использует двумерные квантовые системы. 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 пробы немедленно, либо хранить ее в квантовой памяти и ждать пока Алиса и Боб объявят базис, который они использовали для кодирования данного бита, и только затем провести измерение состояния пробы.

Используя результаты [5], для взаимной шенноновской информации между Алисой и Евой в случае, когда Ева измеряет состояние пробы сразу после перепутывания с фотоном Алисы, можно получить следующее выражение:

$$I_{AE}(D)=\frac{1}{2}\left(1+\chi\left[\frac{1}{2}-\sqrt{2D-4D^2}\right]+\chi\left[\frac{1}{2}+\sqrt{2D-4D^2}\right]\right), \tag{3}$$

где функция $\chi(z)=(1-z)\log_2(1-z)$.

Однако эта атака не является оптимальной для Евы, так как она не ждет объявления 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 была выполнена в [6]. Для $I_{\mathrm{AE}}(D)$ было получено следующее выражение [6]:

$$I_{\mathrm{AE}}(D)=\frac{1}{2}\varphi\left(2\sqrt{D(1-D)}\right), \tag{4}$$

где $\varphi(z)$ определено в (2).

На рис. 1 приведены зависимости $I_{\mathrm{AE}}(D)$ 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 должны прервать свой протокол передачи ключа (сравнить кривые 3 и 4). Отсюда можно сделать вывод, что ожидание объявления базисов и оптимизация измерительной процедуры не приносит Еве большой выгоды при некогерентных атаках на протокол BB84.

Рассмотрим теперь когерентную атаку [2] на протокол BB84. В работе [7] была предложена общая схема вычисления $I_{\mathrm{AE}}(D)$ при когерентной атаке на протоколы, основанные на передаче кубитов. В этой схеме $I_{\mathrm{AE}}(D)$ 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 $I_{\mathrm{AE}}(D)$ при когерентной атаке на протокол BB84 и на протокол с 6-ю состояниями.

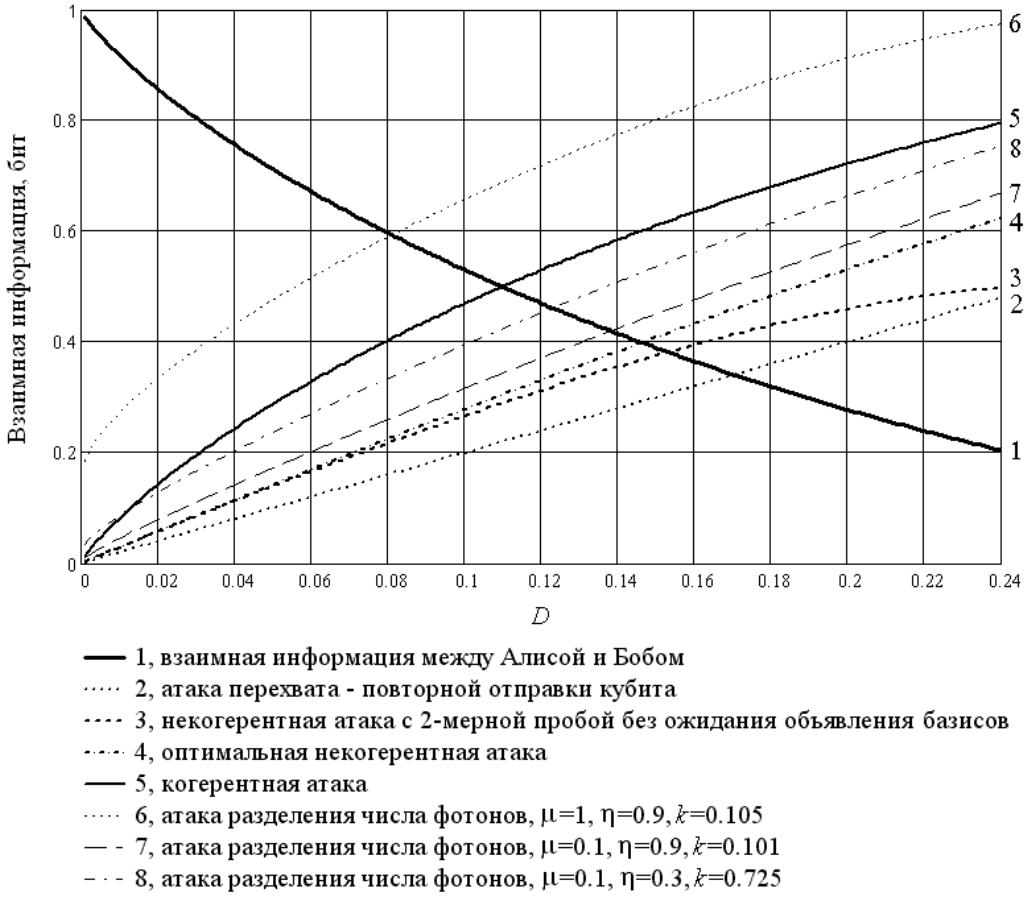

Рисунок 1 – Взаимная информация $I_{\mathrm{AB}}(D)$ (кривая 1) и $I_{\mathrm{AE}}(D)$ для различных стратегий атак на протокол BB84 (кривые 2–8)

Схема вычисления $I_{\mathrm{AE}}(D)$ состоит в следующем. 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

$$|u\rangle = \sum_{i_1,i_2,\ldots,i_N} \sum_{j} \alpha_{i_1,i_2,\ldots,i_N,j} |i_1, i_2, \ldots, i_N\rangle \otimes |j\rangle, \qquad (5)$$

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

Используя неравенство $I_{\mathrm{AE}} \le S(\rho_{\mathrm{AB}})$, где S – энтропия фон Неймана и приведенная матрица плотности ρ_{AB} вычисляется взятием частичного следа по подпространству состояний пробы Евы $\rho_{\mathrm{AB}} = Tr_{Eve}|u\rangle\langle u|$, можно получить [7]:

$$I_{\mathrm{AE}} \le -\sum_{i_1,i_2,\ldots,i_N} P_{i_1,i_2,\ldots,i_N} \log_2 P_{i_1,i_2,\ldots,i_N} = \log_2 \Omega, \qquad (6)$$

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

Величина Ω зависит от типа протокола и для BB84 имеет вид [7] $\Omega = \sum_{\frac{1}{2}(b+c)+d=D} \frac{N!}{a!\,b!\,c!\,d!}$, 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. [7]), можно получить:

$$\log_2 \Omega = \max\left\{(N - 2ND + d)\log_2 \frac{N - 2ND + d}{N} + 2(ND - d)\log_2 \frac{ND - d}{N} + d\log_2 \frac{d}{N}\right\}, \qquad (7)$$

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

$$I_{\mathrm{AE}}^{(\max)}(D) = 1 - \frac{1}{2}\varphi(1 - 2D), \qquad (8)$$

где $\varphi(z)$ определено в (2).

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 мощной и позволяет получить тот максимум информации при подслушивании, который допускается законами квантовой механики.

2. Атака разделения числа фотонов на протокол BB84. Рассмотренными в предыдущем разделе случаями исчерпываются основные стратегии перехвата информации в протоколе BB84 при использовании однофотонных источников. Однако 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 [8]:

$$p_n = e^{-\mu}\frac{\mu^n}{n!}, \qquad (9)$$

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 [8]:

$$p_{n,loss} = e^{-\eta\mu}\frac{(\eta\mu)^n}{n!}, \tag{10}$$

где η – коэффициент передачи канала.

Из (10) следует, что есть вероятность зарегистрировать более одного фотона в импульсе:

$$p_{n>1,loss} = 1 - e^{-\eta\mu}(1+\eta\mu). \tag{11}$$

Так, например, при $\mu = 1$ и $\eta = 0{,}9$ вероятность регистрации многофотонного импульса равна 0,228, т.е. в среднем почти 23% регистрируемых импульсов содержат более одного фотона.

В этом случае Ева может применить атаку разделения числа фотонов (photon number splitting attack) [8, 9]. Для каждого импульса Ева должна выполнить квантовое неразрушающее измерение числа фотонов в лазерном импульсе, не влияя при этом на их поляризацию. Отметим, что такое измерение очень сложно выполнить, однако в настоящее время это технически возможно [8].

Если Ева обнаруживает в импульсе более одного фотона, то 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 [1, 8-10]. Рассмотрим схему вычисления $I_{\mathrm{AE}}(D)$ только для самой сильной стратегии, когда Ева имеет возможность заменить квантовый канал с потерями, используемый законными пользователями, на канал без потерь [8]. В этом случае Ева может блокировать некоторую часть однофотонных импульсов так, чтобы Боб в результате получил приблизительно ожидаемое им число пустых импульсов. Отметим, что для исходного канала с очень большими потерями такая стратегия позволяет Еве получить почти полное знание ключа, не внося никаких ошибок [8].

Таким образом, Ева блокирует некоторую долю k однофотонных импульсов, а к остальным применяет некогерентную атаку. Ошибки в просеянный ключ вносятся 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 заменит канал на идеальный ($\eta = 1$) и блокирует часть однофотонных импульсов [8]:

$$1 - e^{-\eta\mu} = (1-k)p_1 + p_{n>1}, \tag{12}$$

откуда с использованием (9) получим

$$k = \frac{1}{\mu}\left(e^{\mu(1-\eta)} - 1\right). \tag{13}$$

Вероятность для Евы правильно измерить состояние пробы, перепутанной с фотоном Алисы, дается выражением [8]:

$$P_{correct} = \frac{1 - e^{-\mu}(1+\mu) + (1-k)\mu e^{-\mu}\left(1/2 + \sqrt{D(1-D)}\right)}{1 - e^{-\mu}(1+\mu k)}. \tag{14}$$

Так как вероятность для Евы неверно измерить состояние пробы равна $(1 - P_{correct})$, то взаимная информация между Алисой и Евой $I_{\mathrm{AE}}(D)$ для описанной атаки:

$$I_{\mathrm{AE}}(D) = \frac{1}{2}\varphi\left[1 - 2(1 - P_{correct})\right], \tag{15}$$

где $\varphi(z)$ определено в (2).

На рис. 1 приведены зависимости $I_{\mathrm{AE}}(D)$ (15) для различных значений μ и η (кривые 6-8). Видно, что при любых значениях этих параметров Ева получит больше информации, чем при некогерентных атаках для строго однофотонных источников сигнала. При этом, чем больше потери в канале, тем больше информации получит Ева (сравнить кривые 7 и 8), так как при увеличении потерь она может блокировать больше однофотонных импульсов, и, соответственно, использовать больше многофотонных.

Параметр μ источника фотонов также сильно влияет на мощность атаки. 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 протокол BB84 нельзя использовать для распределения секретного ключа. Поэтому для практической реализации протокола необходимо 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: $p_{n>0,\,loss} = 1 - e^{-\eta\mu} = 0{,}095$.

Из нашего анализа следует также, что даже при использовании источника с $\mu = 0{,}1$, атака разделения числа фотонов достаточно эффективна – она 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.

3. 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: $\{|0\rangle, |1\rangle\}$, $\left\{|\bar{0}\rangle = {}^{1}\!/_{\sqrt{2}}\left(|0\rangle + |1\rangle\right), |\bar{1}\rangle = {}^{1}\!/_{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right\}$ или $\left\{|\bar{0}\rangle = {}^{1}\!/_{\sqrt{2}}\left(|0\rangle + i|1\rangle\right), |\bar{1}\rangle = {}^{1}\!/_{\sqrt{2}}\left(|0\rangle - i|1\rangle\right)\right\}$, выбирая их с равной вероятностью [11]. В остальном стадии этого протокола совпадают со стадиями BB84.

В работе [11] был проведен анализ и оптимизация некогерентной атаки с двухкубитной пробой на протокол с 6-ю состояниями. Взаимная информация между Алисой и Евой дается выражением [11]:

$$I_{AE}(D) = 1 + (1-D)\left[f(D)\log_2 f(D) + (1-f(D))\log_2(1-f(D))\right], \qquad (16)$$

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

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. раздел 1 настоящей работы). 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: $\frac{2}{3}(b+c+d) = ND$, $b = c = d$ и $d = \frac{ND}{2}$ [7]. Тогда выражение (6) можно окончательно привести к следующему виду:

$$I_{AE}(D) = -\frac{1}{2}\left[\left(1 - \frac{3}{2}D\right)\log_2\left(1 - \frac{3}{2}D\right) + \frac{3}{2}D\log_2\left(\frac{D}{2}\right)\right]. \qquad (17)$$

На рис. 2 показаны зависимости $I_{\mathrm{AE}}(D)$ для оптимальной некогерентной атаки на протоколы BB84 (4) и с шестью состояниями (16), а также для когерентной атаки на эти протоколы (формулы (8) и (17) соответственно). Видно, что при всех D кривые для протокола с шестью состояниями лежат ниже соответствующих кривых для BB84. Это означает несколько большую стойкость протокола с шестью состояниями к указанным атакам.

На рис. 3 показана разность

$$\Delta(D) = I_{\mathrm{AE}}^{(BB84)}(D) - I_{\mathrm{AE}}^{(6-state)}(D) \qquad (18)$$

для оптимальной некогерентной атаки и когерентной атаки. Видно, что при некогерентной атаке на протокол с шестью 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 шестью 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 шестью состояниями обладает небольшим преимуществом над протоколом BB84.

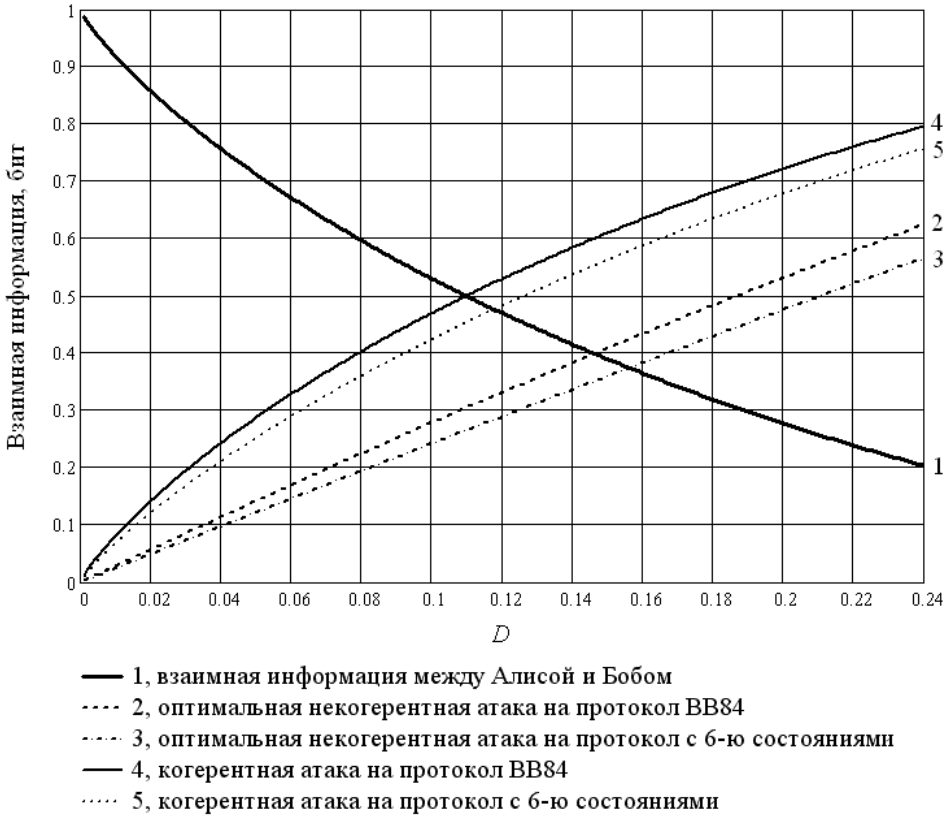

Рисунок 2 – Взаимная информация $I_{AB}(D)$ (кривая 1) и $I_{AE}(D)$ для различных стратегий атак на протокол с 6-ю состояниями (кривые 2–5)

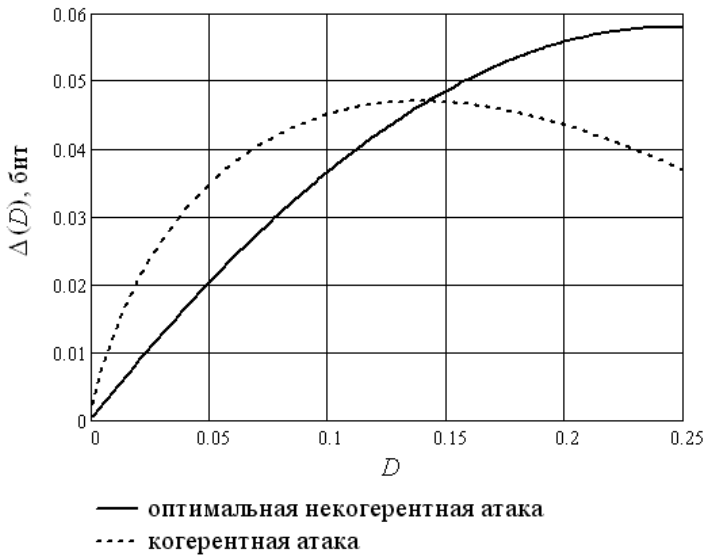

Рисунок 3 – $\Delta(D)$(18) для некогерентной и когерентной атак

Согласно теореме Цизара и Кёрнера [12] 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 только однонаправленный классический канал (с аутентификацией), они могут провести процедуру усиления секретности, после которой информация Евы о ключе станет пренебрежимо малой [1]. Поэтому в квантовой криптографии верхней границей допустимого уровня ошибок

считают значение $D_{\max}$, получаемое из равенства $I_{AB}(D_{\max}) = I_{AE}(D_{\max})$. На рис. 1, 2 значения $D_{\max}$ для различных стратегий атак соответствует точкам пересечения соответствующих кривых.

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

Для атаки разделения числа фотонов на протокол BB84 приведем границу допустимого уровня ошибок при $\mu = 0{,}1$ и $\eta = 0{,}9$, что приблизительно соответствует параметрам реально используемого в настоящее время оборудования. Эта граница $D_{\max} \approx 13{,}8\%$ и лежит между соответствующих границ для некогерентной и когерентной атак на однофотонные сигналы, ближе к границе для оптимальной некогерентной атаки. Следовательно, при таких параметрах источника сигналов и квантового канала стойкость протокола BB84 к атаке разделения числа фотонов не намного меньше, чем к оптимальной некогерентной атаке.

В заключение отметим следующее. Как показывает анализ, стойкость протокола BB84 ко всем видам атак *незначительно меньше* стойкости протокола с шестью состояниями. Однако скорость передачи ключа по протоколу BB84 *существенно выше*, так как его средняя эффективность равна $1/2$, а протокола с шестью состояниями – $1/3$. Таким образом, для передачи длинных ключей протокол BB84 следует предпочесть протоколу с шестью состояниями.

Если же подслушивающий агент имеет возможность применить атаку разделения числа фотонов на протокол BB84, то, используя источник со средним числом фотонов в импульсе не более 0,1, а также квантовый канал с малыми потерями ($\eta = 0{,}9 \div 1$), законные пользователи смогут установить секретный ключ, когда уровень ошибок при передаче не превышает ~ 14%. Однако платой за секретность в этом случае будет 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. – М.: «Постмаркет», 2002. – 376 с.
3. *Lutkenhaus N.* Estimates for practical quantum cryptography // Physical Review A. – 1999. – V. 59. – №5. – P. 3301-3319.
4. *Bechmann-Pasquinucci H*. Eavesdropping without quantum memory // Physical Review A. – 2006. – V. 73. – P. 044-305.
5. *Gisin N., Huttner B.* Quantum Cloning, Eavesdropping and Bell's inequality // Physical Letters A. – 1997. – V. 228. – P. 13-21.
6. *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.
7. *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.
8. *Williamson M., Vedral V*. Eavesdropping on practical quantum cryptography // Journal of Modern Optics. – 2003. – V. 50, № 13. – P. 1989-2011.
9. *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. – P. 042-316.
10. *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.
11. *Bruss D*. Optimal Eavesdropping in Quantum Cryptography with Six States // Physical Review Letters. – 1998. – V. 81. – № 14. – P. 3018–3021.
12. *Csiszar I., Korner J*. Broadcast channels with confidential messages // IEEE Transactions on Information Theory. – 1978. – V. IT-24. – № 3. – P. 339-348.