Письма в ЖЭТФ, том 100, вып. 4, с. 305 – 311

Двойственность квантовых каналов связи и коллективная атака прием–перепосыл на квантовое распределение ключей с дифференциально-фазовым кодированием

Д. А. Кронберг[+1)], *С. Н. Молотков*[+*×1)]

[+]*Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119991 Москва, Россия*

[*]*Институт физики твердого тела РАН, 142432 Черноголовка, Россия*

[×]*Академия криптографии Российской Федерации, 121552 Москва, Россия*

Поступила в редакцию 11 июля 2014 г.

Квантовое распределение ключей с дифференциально-фазовым кодированием (Differential Phase Shift, DPS) является наименее изученным. Рассмотрена атака коллективный прием–перепосыл. Даже для такой простейшей атаки анализ оказывается не самоочевидным. Показано, что использование коллективных измерений с применением запутанных состояний не увеличивает информации подслушивателя по сравнению с индивидуальными измерениями. Данный результат является следствием фундаментальных свойств квантовых каналов связи, связанных с двойственностью квантовых ансамблей и измерений.

DOI: 10.7868/S0370274X14160127

1. Введение. В квантовой криптографии основной задачей теории является вычисление длины секретного ключа в зависимости от наблюдаемой вероятности ошибки на приемной стороне [1–3]. Для реальных не однофотонных источников квантовых состояний (сильно ослабленного когерентного излучения лазера) она до конца не решена [3]. Все протоколы квантовой криптографии можно разделить на два класса. Первый класс (нерелятивистской квантовой криптографии) использует для обеспечения секретности ключей фундаментальные запреты квантовой механики на достоверную различимость неортогональных состояний [4]. Второй класс протоколов (релятивистской квантовой криптографии), кроме запретов квантовой механики, использует дополнительные фундаментальные ограничения, диктуемые специальной теорией относительности (фактически релятивистской причинностью), на достоверную различимость протяженных в пространстве-времени квантовых состояний [5, 6]. Данный класс протоколов разработан специально для передачи ключей на большие расстояния через открытое пространство. При этом секретность ключей гарантируется даже не при строго однофотонном источнике и при произвольных потерях в канале связи [5].

[1)]e-mail: dmitry.kronberg@gmail.ru; sergei.molotkov@gmail.ru

2. Типы протоколов квантовой криптографии. Протоколы нерелятивистской квантовой криптографии также можно разделить на две группы [3]. В протоколах первой группы информация о битах будущего секретного ключа кодируется в квантовые состояния независимо в каждой отдельной посылке. На приемной стороне каждый бит ключа извлекается посредством измерений $\mathcal{M}$ квантового состояния отдельно в каждой посылке:

$$x_1, x_2, x_3, \ldots, x_n \to \rho_{x_1} \otimes \rho_{x_2} \otimes \rho_{x_3} \otimes \cdots \otimes \rho_{x_n} \to \\ \to \mathcal{M}(\rho_{x_1}), \mathcal{M}(\rho_{x_2}), \mathcal{M}(\rho_{x_3}), \ldots, \mathcal{M}(\rho_{x_n}). \quad (1)$$

Во второй группе протоколов информация о битах ключа размазана по соседним независимым посылкам [7, 8]. Например, в протоколе с дифференциально-фазовым кодированием [7] биты ключа кодируются в относительную ("дифференциальную") фазу когерентных состояний в каждой посылке:

$$x_1, x_2, x_3, \ldots, x_n \to \\ \to |e^{i\varphi_1}\alpha\rangle \otimes |e^{i\varphi_2}\alpha\rangle \otimes |e^{i\varphi_3}\alpha\rangle \otimes \cdots \otimes |e^{i\varphi_{n+1}}\alpha\rangle \to \quad (2)$$

$$\to \mathcal{M}\begin{pmatrix} |\frac{1}{\sqrt{2}}(e^{i\varphi_1} + e^{i\varphi_2})\alpha\rangle \\ |\frac{1}{\sqrt{2}}(e^{i\varphi_1} - e^{i\varphi_2})\alpha\rangle \end{pmatrix} \otimes$$

$$\otimes \mathcal{M}\begin{pmatrix} |\frac{1}{\sqrt{2}}(e^{i\varphi_2} + e^{i\varphi_3})\alpha\rangle \\ |\frac{1}{\sqrt{2}}(e^{i\varphi_2} - e^{i\varphi_3})\alpha\rangle \end{pmatrix} \otimes \ldots \otimes$$

$$\otimes \mathcal{M} \left(\begin{array}{c} |\frac{1}{\sqrt{2}}(e^{i\varphi_n} + e^{i\varphi_{n+1}})\alpha\rangle \\ |\frac{1}{\sqrt{2}}(e^{i\varphi_n} - e^{i\varphi_{n+1}})\alpha\rangle \end{array} \right).$$

Отметим, что данный протокол не использует согласования базисов.

Для нерелятивистских протоколов первой группы существуют полные доказательства секретности распределяемых ключей. Для протоколов второй группы имеются частичные результаты в канале с потерями, но нет доказательств секретности даже для случая идеального (без потерь) квантового канала связи. Как показывает приводимый ниже анализ, даже для такой простой атаки ответ не является тривиальным и опирается на фундаментальные свойства квантовых каналов связи, такие, как супераддитивность и двойственность квантовых состояний и наблюдаемых (измерений).

3. Стойкость протоколов первого типа. Для протоколов первой группы доказано, по крайней мере в однофотонном случае, что наиболее общей атакой является коллективная [3]. Неформально в каждой посылке подслушиватель (Ева) использует вспомогательное квантовое состояние, которое приводится во взаимодействие (запутывается) с передаваемым состоянием, $\rho^E_{x_1} \otimes \rho^E_{x_2} \otimes \ldots \otimes \rho^E_{x_n}$. Свою искаженную квантовую систему Ева оставляет у себя в квантовой памяти, $\rho^E_{x_i} = \mathrm{Tr}_B\{|\Psi_{x_i}\rangle_{BEBE}\langle\Psi_{x_i}|\}$, а возмущенное состояние передатчика (Алисы) направляет на приемную сторону (к Бобу), $\rho^B_{x_i} = \mathrm{Tr}_E\{|\Psi_{x_i}\rangle_{BEBE}\langle\Psi_{x_i}|\}$. После измерений $(\mathcal{M}_y)$ искаженных информационных состояний Бобом и оценки вероятности ошибки через открытый канал Алиса назначает таблицу кодовых слов. На данный момент Алиса и Боб имеют битовые строки, причем строка Боба имеет ошибки. Алиса и Боб находятся в ситуации бинарного классического канала связи:

$$x_1, x_2, x_3, \ldots, x_n \to y_1, y_2, y_3, \ldots, y_n. \qquad (3)$$

Степень корреляции битовых последовательностей Алисы, $X = \{x_i\}_{i=1}^n$, и Боба, $Y = \{y_i\}_{i=1}^n$, дается взаимной информацией:

$$I(X:Y) = \sum_{x,y} p_{XY}(x,y) \log \frac{p_{X|Y}(x|y)}{\sum_{x'} p_X(x') p_{X|Y}(x'|y)}, \qquad (4)$$

$$p_{X|Y}(x|y) = \mathrm{Tr}\{\rho^B_x \mathcal{M}_y\},$$

$$p_{XY}(x,y) = p_X(x) p_{X|Y}(x|y), \quad \sum_y \mathcal{M}_y = \mathrm{id},$$

где id – единичный оператор. Для исправления ошибок Алиса назначает таблицу кодовых слов размером $2^{nI(X:Y)}$, включая в нее последовательность $x_1, x_2, x_3, \ldots, x_n$ которую она посылала:

$$\{X_{code}\} = \left\{ \begin{array}{c} \ldots\ldots\ldots\ldots \\ x_1, x_2, x_3, \ldots, x_n \\ \ldots\ldots\ldots\ldots \end{array} \right\} \quad \to \quad 2^{nI(X:Y)}. \qquad (5)$$

Боб, имея таблицу и свою последовательность $y_1, y_2, y_3, \ldots, y_n$ (фактически это последовательность $x_1, x_2, x_3, \ldots, x_n$, но с ошибками), может исправить ошибки с вероятностью единица. После этого Алиса и Боб имеют идентичные битовые строки – очищенный, но еще не секретный ключ.

Ева находится с Алисой в ситуации классически-квантового (c-q) канала связи:

$$x_1, x_2, x_3, \ldots, x_n \to \rho^E_{x_1} \otimes \rho^E_{x_2} \otimes \ldots \otimes \rho^E_{x_n}, \qquad (6)$$

Ева имеет в квантовой памяти последовательность квантовых состояний $\rho^E_{x_1} \otimes \rho^E_{x_2} \otimes \ldots \otimes \rho^E_{x_n}$, которая произошла из $|\Psi_{x_i}\rangle_{BE} = U_{BE}(|\varphi_{x_i}\rangle_B \otimes |E\rangle_E)$, $\rho^E_{x_i} = \mathrm{Tr}_B\{|\Psi_{x_i}\rangle_{BEBE}\langle\Psi_{x_i}|\}$. Цель Евы – восстановить битовую последовательность Алисы из последовательности квантовых состояний. Поскольку оператор U_{BE} задается самой Евой, она знает квантовые состояния $\rho^E_{x_i}$. Зная классическую кодовую таблицу (5), Ева может построить соответствующую кодовую таблицу из квантовых состояний $\{X^E_{q-code}\}$:

$$\{X^E_{q-code}\} = \left\{ \begin{array}{c} \ldots\ldots\ldots\ldots \\ \rho^E_{x_1}, \rho^E_{x_2}, \rho^E_{x_3}, \ldots, \rho^E_{x_n} \\ \ldots\ldots\ldots\ldots \end{array} \right\} \to 2^{n\chi(\rho^E)}. \qquad (7)$$

Сами состояния известны, но неизвестно, какое из этих состояний находится в каждой из ячеек. Цель Евы – извлечь классическую информацию, т.е., имея ρ^E_x, определить x из ансамбля квантовых состояний $\{p_X(x), \rho^E_x\}$ ($p_X(x)$ – вероятности появления состояний ρ^E_x). В соответствии с фундаментальной границей Холево для достижимой классической информации, информация, которую можно извлечь из квантового ансамбля, ограничена величиной Холево χ [9]:

$$\chi(\rho^E) = H(\overline{\rho^E}) - \sum_x p_X(x) H(\rho^E_x),$$
$$\overline{\rho^E} = \textstyle\sum_x p_X(x)\rho^E_x, \quad H(\rho) = -\mathrm{Tr}\{\rho \log \rho\}. \qquad (8)$$

Кроме того, теорема Холево гласит, что данная граница конструктивно достижима. Достигается она на кодовой таблице [9]. Неформально если передатчик выбирает кодовую таблицу (7) размером не более $2^{n\chi(\rho^E)}$, то используя коллективные измерения, которые фактически сводятся к проекции на запутанные (сцепленные) состояния, построенные исходя

из кодовой таблицы, приемник сможет безошибочно различить все кодовые слова. Поскольку кодовые слова привязаны к классическим битовым строкам $x_1, x_2, x_3, \ldots, x_n$, безошибочное различение квантовых кодовых слов означает безошибочное различение переданной битовой строки (6).

4. Коллективные и индивидуальные измерения, супераддитивность и аддитивность. Ева может измерять квантовые состояния индивидуально в каждой посылке, минимизируя ошибку измерения. В этом случае количество бит классической информации ограничено величиной $nC(\rho^E)$ – классической пропускной способностью квантового канала за один шаг (*one shot capacity*) [9]. Величина Холево равна классической пропускной способности квантового канала ($\overline{C}(\rho^E) = \chi(\rho^E)$). Она и достигается на коллективных измерениях, *которые строятся исходя из заранее известной кодовой таблицы* [9]. При этом имеет место неравенство $\overline{C}(\rho^E) > C_1(\rho^E)$, т.е. коллективные измерения позволяют извлечь больше классической информации из квантового ансамбля [9].

Достижимая информация при индивидуальных измерениях является *аддитивной* величиной [9]:

$$\max_{\mathcal{M}}\{I^{(n)}((\rho^E)^{\otimes n}, \mathcal{M}^{\otimes n})\} = \\ = \sum_{x,z} p_{XZ}(x,z)\log\frac{p_{X|Z}(x|z)}{\sum_{x'} p_X(x')p_{X|Z}(x'|z)} = \\ = nC_1(\rho^E), \qquad (9)$$

где измерения $\mathcal{M}$ реализуют разложение единицы. Соответствующие переходные вероятности

$$p_{X|Z}(x|z) = \mathrm{Tr}\{\rho_x^E \mathcal{M}_z\}, \\ p_{XZ}(x,z) = p_X(x)p_{X|Z}(x|z),\ (\sum_z \mathcal{M}_z)^{\otimes n} = \mathrm{id}^{\otimes n}. \qquad (10)$$

Достижимая информация при коллективных измерениях является *супераддитивной* величиной (детали см. в [9]):

$$\max_{\mathcal{M}^{(n)}}\{I^{(n)}((\rho^E)^{\otimes n}, \mathcal{M}^{(n)})\} = \\ = \sum_{X,Z} p_{XZ}^{(n)}(X,Z)\log\frac{p_{X|Z}^{(n)}(X|Z)}{\sum_{X'} p_X^{(n)}(X')p_{X|Z}^{(n)}(X'|Z)} = \\ = C^{(n)}(\rho^E). \qquad (11)$$

Существующие переходные вероятности имеют вид

$$p_{X|Z}^{(n)}(X|Z) = \mathrm{Tr}\{(\rho_{x_1}^E \otimes \rho_{x_2}^E \otimes \ldots \otimes \rho_{x_n}^E)\mathcal{M}_Z^{(n)}\}, \\ p_{XZ}^{(n)}(X,Z) = p_X^{(n)}(X)p_{X|Z}^{(n)}(X|Z), \qquad (12)$$

$$p_X^{(n)}(X) = \prod_{i=1}^n p_X(x_i), \quad \sum_Z \mathcal{M}_Z^{(n)} = \mathrm{id}^{\otimes n}, \\ Z = (z_1, z_2, \ldots, z_n), \quad X = (x_1, z_x, \ldots, x_n).$$

При этом имеет место свойство супераддитивности [9]:

$$\frac{C^{(n)}(\rho^E)}{n} + \frac{C^{(m)}(\rho^E)}{m} < \frac{C^{(n+m)}(\rho^E)}{n+m} < \chi(\rho^E), \qquad (13)$$

$$\overline{C}(\rho^E) = \lim_{n\to\infty}\frac{C^{(n)}(\rho^E)}{n}.$$

Отметим принципиальную разницу между двумя случаями.

Индивидуальные измерения. Никакой кодовой таблицы изначально нет. Источник посылает квантовые состояния независимо в каждой посылке в соответствии с распределением $p_X(x)$. Приемник в этом случае "видит" тензорное произведение квантовых состояний. Приемник осуществляет индивидуальные измерения в каждой посылке, которые минимизируют ошибку различения квантовых состояний. После измерений приемник имеет битовую строку Z, но с ошибками. Только после этого передатчик, зная ошибку на приемной стороне, оглашает классическую кодовую таблицу (5), поскольку ошибка приемника для оптимальных измерений известна. Приемник исправляет ошибки и получает информацию в $nC_1(\rho^E)$ бит (9).

Коллективные измерения. Передатчик сначала формирует кодовую таблицу квантовых состояний. Для приемника это означает, что в канал будет послана *только одна из кодовых последовательностей и никакая другая.* Приемник, исходя из кодовой таблицы, строит измерения, которые проецируют *всю квантовую последовательность* на некоторое сцепленное состояние. Если число кодовых квантовых последовательностей в кодовой таблице не превышает $2^{n\overline{C}(\rho^E)}$, то приемник безошибочно определит переданную последовательность. При этом количество бит информации будет равно $n\overline{C}(\rho^E)$ (13), что превышает информацию при индивидуальных измерениях.

Критическая ошибка при коллективных измерениях. Возвратимся к критической ошибке протоколов первой группы. Ошибка протокола определяется из уравнения (детали см. в [1–3])

$$R = \min_{\{U_{BE}|Q\}}\{I(X:Y) - \overline{C}(\rho^E)\}. \qquad (14)$$

Минимизацию в (14) надо понимать так. Ева выбирает унитарный оператор U_{BE} таким образом, чтобы максимизировать $\overline{C}(\rho^E)$ при заданной наблюдае-

мой вероятности ошибки Q (если протокол однопараметрический; случай двухпараметрических протоколов см. в [10]). Переходные вероятности, фигурирующие в $I(X:Y)$ и определяющие ошибку, зависят от структуры U_{BE}, контролируемого Евой.

Критическая ошибка при индивидуальных измерениях. Критическая ошибка при индивидуальных измерениях определяется из аналогичного (14) уравнения, куда вместо величины Холево $\overline{C}(\rho^E)$ входит классическая пропускная способность квантового канала связи за один шаг (*one shot*):

$$R = \min_{\{U_{BE}|Q\}} \{I(X:Y) - C_1(\rho^E)\}. \qquad (15)$$

Ева использует индивидуальные измерения "на ходу" над каждым состоянием, а затем по итогам измерения готовит состояние и перепосылает на приемную сторону.

5. Двойственность квантовых ансамблей и наблюдаемых. *Возникает вопрос: возможно ли, используя коллективные измерения "на ходу" (не дожидаясь оглашения кодовой таблицы), увеличить информацию Евы? При этом Ева собирает весь пакет из n состояний в квантовой памяти (напомним, что состояния посылаются индивидуально), а затем делает коллективные измерения над всей последовательностью.* Такую атаку можно назвать "коллективная атака прием–перепосыл". На первый взгляд по аналогии с вышеприведенными рассуждениями коллективные измерения должны увеличить извлекаемую из квантовых состояний информацию. Более формально данный вопрос можно переформулировать следующим образом. Является ли доступная классическая информация при такой атаке супераддитивной или аддитивной величиной? Как показано выше, информация Холево является супераддитивной величиной и достигается на коллективных измерениях. *Однако супераддитивность достигается при наличии кодовой таблицы.* В данном случае при атаке коллективный прием–перепосыл кодовой таблицы изначально нет и ансамбль передаваемых состояний распадается на тензорное произведение ансамблей, относящихся к отдельным посылкам:

$$\{p_X(x), \rho_x\} = \bigotimes_i \{p^i_X(x_i), \rho^i_x\} = \{\prod_i p^i_X(x_i), \bigotimes_i \rho^i_x\}.$$

Поэтому ответ на поставленный вопрос об аддитивности или супераддитивности информации заранее не очевиден.

Известно, что когда на входные последовательности не накладывается ограничений, но измерения индивидуальны, достижимая информация аддитивна [11, 12]. В нашей (противоположной) ситуации входные состояния посылаются индивидуально без использования кодовой таблицы, а измерения могут быть запутанными (коллективными сразу над всей последовательностью).

Оказывается, что две упомянутые ситуации связаны между собой нетривиальным свойством двойственности между ансамблем квантовых состояний и измерениями [13, 14]. Двойственность возникает следующим образом. Квантовое состояние $\{\rho\} = \{p_X(x), \rho_x\}$ и измерение $\{\mathcal{M}\} = \{\mathcal{M}_z\}$ (наблюдаемая) генерируют распределение вероятностей

$$p_{XZ}(x,z) = p_X(x)\mathrm{Tr}\{\rho_x \mathcal{M}_z\}. \qquad (16)$$

То же самое распределение вероятностей может быть получено из двойственного квантового ансамбля $\{\rho'\} = \{p'_Z(z), \rho'_z\}$ и двойственного измерения $\{\mathcal{M}'\} = \{\mathcal{M}'_x\}$:

$$p_{XZ}(x,z) = p'_Z(z)\mathrm{Tr}\{\rho'_z \mathcal{M}'_x\}. \qquad (17)$$

Соотношение двойственности выполняется, если

$$p'_Z(z)\rho'_Z = \sqrt{\overline{\rho_X}}\mathcal{M}_z\sqrt{\overline{\rho_X}}, \quad \overline{\rho_X} = \sum_x p_X(x)\rho_x,$$
$$p'_Z(z) = \mathrm{Tr}\{\overline{\rho_X}\mathcal{M}_z\}, \quad \mathcal{M}'_x = p_X(x)\frac{1}{\sqrt{\overline{\rho_X}}}\rho_x\frac{1}{\sqrt{\overline{\rho_X}}}. \qquad (18)$$

Из (4), (16)–(18) следует, что для взаимной информации

$$I(\rho, \mathcal{M}) = I(\rho', \mathcal{M}'). \qquad (19)$$

Пусть задан квантовый канал. Любой квантовый канал есть вполне положительное отображение Φ (Completely Positive Map, CPM) [9], которое преобразует входные состояния (матрицы плотности – положительные эрмитовы операторы со следом единица) в выходные матрицы плотности. По определению [9], пропускная способность квантового канала Φ за один шаг есть

$$C_1(\Phi) = \max_{\{\rho\}} \max_{\{\mathcal{M}\}} I(\Phi(\rho), \mathcal{M}). \qquad (20)$$

Само измерение может рассматриваться как канал связи (вполне положительное отображение). Действительно, пусть имеется измерение $\{\mathcal{M}\}$. Ему можно сопоставить разложение Крауса [15]. Для состояний ρ на входе канала и ρ_Φ на выходе имеем

$$\rho_\Phi = \Phi(\rho) = \textstyle\sum_z V_x(\rho)V_z^+, \quad V_z = \sqrt{\mathcal{M}_z},$$
$$\sum_z \mathcal{M}_z = \sum_z V_z^+ \cdot V_z = \mathrm{Id}. \qquad (21)$$

Если измерение $\mathcal{M}$ в (20) *фиксировано*, то пропускная способность за один шаг

$$C_1(\Phi) = \max_{\{\rho\}} I(\Phi(\rho)). \tag{22}$$

Канал Φ в (21) является каналом, разрушающим запутанность (*entanglement breaking*) [11, 12]. Фактически это происходит из-за того, что измерения являются индивидуальными (представимы в виде тензорного произведения). Поэтому после применения тензорной степени измерений $(\sum_z \mathcal{M}_z)^{\otimes n}$ над запутанным состоянием $\rho^{(n)}$ последнее переходит в незапутанное состояние, которое представимо в виде линейной оболочки тензорной степени состояний. Как было показано ранее, одношаговая пропускная способность (20) канала, разрушающего запутанность, является аддитивной величиной [11, 12] (наиболее короткое доказательство этого факта дано в [16], гл. 12). С учетом (21) и (22) имеем

$$\max_{\{\rho\}} I[(\Phi(\rho))^{\otimes n}] = nC_1(\Phi). \tag{23}$$

Неформально (23) означает, что если измерения являются индивидуальными, то использование запутанных входных состояний не увеличивает пропускную способность. В (23) происходит максимизация по входным состояниям ρ. Аддитивность означает, что достаточно максимизировать только по таким состояниям, которые представимы в виде тензорного произведения $\rho^{\otimes n}$.

Нас интересует ответ на двойственный по отношению к предыдущему вопрос: можно ли увеличить пропускную способность канала (увеличить количество извлекаемой из квантового ансамбля классической информации), если входной ансамбль состояний не запутан (представим в виде тензорного произведения ансамблей для отдельных посылок), а используемые измерения запутаны (являются коллективными, не представимы в виде тензорной степени)? В ответе на этот вопрос как раз и помогают соотношения двойственности (19) для квантовых каналов связи. Аддитивность пропускной способности в первом случае (входной ансамбль запутан, измерения не запутаны) из-за свойства двойственности автоматически приводит к аддитивности во втором случае (ансамбль состояний не запутан, измерения запутаны).

Связующим звеном являются соотношения двойственности (16)–(19) (детали см. в [13, 14]). Максимизация взаимной информации по входным состояниям при фиксированных измерениях для квантового канала связи эквивалентна максимизации по измерениям при фиксированных входных состояниях для двойственного канала. Из свойства двойственности (19) следует и обратное: если ансамбль входных состояний разделим (не запутан), а измерения являются запутанными (коллективными), то достижимая классическая информация является аддитивной величиной от длины последовательности и равна пропускной способности квантового канала за один шаг. Другими словами, максимальное количество классической информации может быть получено при помощи индивидуальных измерений, которые минимизируют вероятность ошибки при различении индивидуальных квантовых состояний.

6. Коллективная атака прием–перепосыл на протокол DPS. При коллективной атаке прием–перепосыл подслушиватель преобразует исходную последовательность (2), разделяя ее на две и сдвигая их на одну позицию друг относительно друга при помощи интерферометра Маха–Цандера. В результате преобразований в каждой позиции возникают состояния (см. также (2))

$$0 \to \begin{pmatrix} |\pm\alpha\rangle \\ |vac\rangle \end{pmatrix}, \quad 1 \to \begin{pmatrix} |vac\rangle \\ |\pm\alpha\rangle \end{pmatrix}. \tag{24}$$

Верхний и нижний элементы в вектор-столбце отвечают верхнему и нижнему выходу интерферометра. Подслушиватель собирает всю последовательность и производит измерения. Цель подслушивателя – различить с минимальной ошибкой всю последовательность, состоящую из ансамбля матриц плотности в каждой позиции $\{\rho\} = \{\frac{1}{2}, \rho_0; \frac{1}{2}, \rho_1\}$:

$$\begin{aligned} \rho_0 &= \begin{pmatrix} \frac{1}{2}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|\right) \\ |vac\rangle\langle vac| \end{pmatrix}, \\ \rho_1 &= \begin{pmatrix} |vac\rangle\langle vac| \\ \frac{1}{2}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|\right) \end{pmatrix}. \end{aligned} \tag{25}$$

Согласно теореме двойственности (см. п. 5) коллективные измерения не позволяют получить информации больше, чем оптимальные измерения над каждой посылкой отдельно. Минимальная ошибка различения матриц плотности есть $Q_c = \frac{1}{2}\left(1 - ||\frac{1}{2}\rho_0 - \frac{1}{2}\rho_1||_1\right)$, (где $||\rho||_1 = \mathrm{Tr}\{\sqrt{\rho^2}\}$. Результат интерпретируется как 0 или 1, но с ошибкой Q. Затем подслушиватель готовит и перепосылает последовательность квантовых состояний, аналогичную (2), в соответствии с результатами своих измерений, такую, чтобы после ее сдвига на приемной стороне возникла такая же последовательность 0 и 1, как и у подслушивателя. Алгоритм построения такой последовательности квантовых состояний очевиден. В результате подслушиватель

и принимающий имеют одинаковые битовые последовательности. Затем Алиса и Боб оценивают вероятность ошибки через открытый канал. Алиса посылает корректирующую информацию, которая доступна и подслушивателю. После исправления ошибок все участники протокола имеют одинаковые битовые строки. При этом длина ключа $R(Q_c)$ обращается в нуль. При такой атаке критическая ошибка протокола равна ошибке различения состояний подслушивателем. Приведенная оценка завышает критическую ошибку, поскольку подслушивателю приходится различать смешанные состояния $\frac{1}{2}(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|)$ и $|vac\rangle\langle vac|$, что сложнее (из-за большего эффективного перекрытия состояний), чем различить чистые состояния $|\alpha\rangle$ и $|-\alpha\rangle$ в исходной последовательности. В этом случае из-за теоремы двойственности коллективные измерения над всей последовательностью также не приводят к меньшей ошибке по сравнению с индивидуальными. Вместе с тем измерения над исходной последовательностью с ошибкой Q будут приводить к удвоенной ошибке (точнее, к ошибке $2Q(1-Q)$) на приемной стороне после сдвига исходной последовательности. Итоговая ошибка на стороне получателя оказывается меньше, несмотря на то что одна ошибка в исходной последовательности может вести к двум ошибкам сдвинутой последовательности. Этот недостаток перекрывается меньшей вероятностью ошибки при различении чистых состояний $|\alpha\rangle$ и $|-\alpha\rangle$.

Возможен третий вариант атаки с индивидуальными измерениями, когда подслушиватель различает лишь некоторую долю p состояний из всей исходной посылки. Каждое из этих состояний является смешанным и дается комбинацией двух состояний-кортежей, приводящих к одной и той же битовой строке. Например, для строки, состоящей из трех нулей, это

$$\rho_{000} = \frac{1}{2}(|\alpha\rangle|\alpha\rangle|\alpha\rangle|\alpha\rangle\langle\alpha|\langle\alpha|\langle\alpha|\langle\alpha| +$$

$$+ |-\alpha\rangle|-\alpha\rangle|-\alpha\rangle|-\alpha\rangle\langle-\alpha|\langle-\alpha|\langle-\alpha|\langle-\alpha|).$$

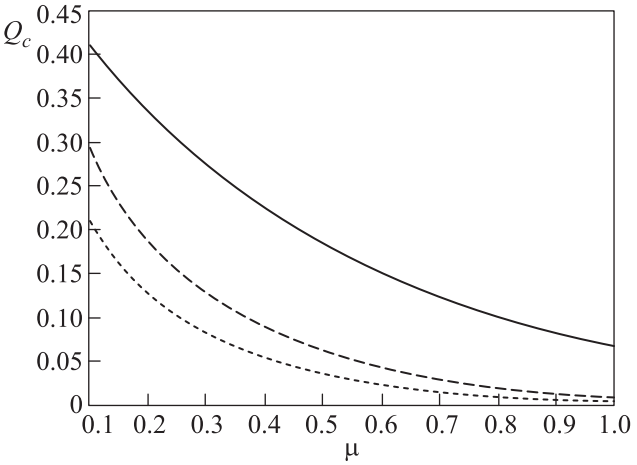
Оценка снизу для взаимной информации дает (см., например, [17])

$$I_{AE} \geq \frac{Np[1-h(Q)]-1}{N-1}. \qquad (26)$$

При больших длинах кортежей ($N \to \infty$) и измерении каждого состояния (параметр p равен единице) эта информация стремится к пропускной способности за один шаг c-q (classical-quantum) канала с состояниями $|\alpha\rangle$ и $|-\alpha\rangle$. Соответствующая критическая ошибка равна критической ошибке при приеме–перепосыле для протокола B92:

$$I_{AE} = I_{AB} = 1 - h(Q_c). \qquad (27)$$

Согласно (26) подслушиватель может получить информацию не меньше, чем (26). Однако при этом неизвестен явный алгоритм приготовления перепосылаемой последовательности, приводящей на приемной стороне к ошибке, которой соответствовала бы взаимная информация I_{AB} в (27) Алисы и Боба, т.е. неизвестно, достижима ли граница (27) конструктивно. На данный момент, насколько мы знаем, это открытый вопрос. Тем не менее в качестве



Зависимости критической ошибки от среднего числа фотонов ($\mu = |\alpha|^2$) для коллективной атаки прием–перепосыл. Пунктирная линия соответствует нижней оценке для всех подобных атак, штриховая – атаке с измерением состояний исходного кортежа, сплошная – атаке с измерением каждого состояния после сдвига кортежа

нижней оценки критической ошибки с точки зрения Алисы и Боба, т.е. величины, до которой гарантируется секретность ключей при атаке методом приема–перепосыла, такая величина подходит. График, соответствующий этой оценке, приведен на рисунке пунктирной линией.

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
2. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich, Dec. 2005.
3. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
4. C. B. Bennett, Phys. Rev. Lett. **68** 3121 (1992).

5. S. N. Molotkov, JETP Lett. **94**, 469 (2011); JETP Lett. **96**, 342 (2012).
6. I. V. Radchenko, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, arXiv:quant-ph/1403.3122; Las. Phys. Lett. **11**, 065203 (2014).
7. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002); K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003); K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).
8. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, arXiv:quant-ph/0506097.
9. A. S. Holevo, Russ. Math. Surveys. **53**, 1295 (1998).
10. С. Н. Молотков, ЖЭТФ **142**, 1 (2012).
11. I. Devetak and A. Winter, IEEE Trans. Inf. Theory **50**, 3183 (2004).
12. P. W. Shor, J. Math. Phys. **43**, 4334 (2002).
13. M. D'A. Giacomo, M. D'Ariano, and M. F. Sacchi, arXiv:quant-ph/11031972.
14. A. S. Holevo, arXiv:quant-ph/1103.2615.
15. K. Kraus, *States, Effects and Operations*, Springer-Verlag, Berlin (1983).
16. M. M. Wilde, arXiv:quant-ph/1106.1445.
17. Д. А. Кронберг, С. Н. Молотков, ЖЭТФ **145**(1), 5 (2014).