## *ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ І СИСТЕМИ*

*Воробиенко П.П., Василиу Е.В.*
*Одесская национальная академия связи им. А.С. Попова*

# ОПТИМАЛЬНАЯ НЕКОГЕРЕНТНАЯ АТАКА НА КВАНТОВЫЕ ПРОТОКОЛЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ПЕРЕДАЧЕЙ ТРЕХМЕРНЫХ КВАНТОВЫХ СИСТЕМ

Квантовое распределение ключей, основанное на фундаментальных законах квантовой механики, – это способ для двух удаленных сторон, обычно называемых Алисой и Бобом, генерировать общий секретный ключ для симметричного шифрования. Законы квантовой механики гарантируют безопасность квантового канала коммуникации в том смысле, что подслушивающий агент (Ева) может быть обнаружен легитимными пользователями [1, 2].

Существуют две основных схемы квантового распределения ключей: первая основана на передаче одиночных квантовых состояний, относящихся к неортогональным базисам (типа протоколов BB84 и с 6-ю состояниями [1, 2]), а вторая – на распределении перепутанных квантовых состояний между пользователями (типа схемы Экерта [1, 2]). Для передачи можно использовать двух-, трех- и т. д. мерные квантовые системы, соответственно каждая такая система несет один бит, один трит и т. д. информации.

Безопасность протоколов, основанных на передаче двумерных квантовых систем – кубитов, к настоящему времени исследована теоретически достаточно полно, а их потенциальная применимость для безопасного распределения ключа между двумя удаленными на большое расстояние пользователями продемонстрирована экспериментально [2]. Однако эффективность таких протоколов, определяемая как отношение использованного для создания ключа количества битов к общему количеству переданных битов, невелика. Использование для передачи многомерных квантовых систем является одним из путей увеличения эффективности протокола, а соответственно и скорости генерации ключа.

Недавно были предложены протоколы с передачей трехмерных квантовых систем (кутритов) обоих вышеназванных типов: протокол с передачей одиночных кутритов, относящихся к неортогональным базисам [3] (обобщение протокола с 6-ю состояниями на трехмерные системы), и протокол с передачей перепутанных пар кутритов, состояния которых восстанавливаются методом квантовой томографии – так называемый томографический протокол [4]. Была найдена также оптимальная некогерентная атака с использованием квантовых проб на эти протоколы. В [5] было предложено обобщение на кутриты оригинального протокола Экерта, а также рассмотрена симметричная некогерентная атака на предложенный протокол. Однако оптимизация атаки по параметрам проб не проводилась, поэтому вопрос о надежности протокола [5] остался открытым.

Цель настоящей работы – провести анализ и оптимизацию некогерентной атаки на протокол с перепутанными кутритами, предложенный в [5], а также сравнить стойкость этого протокола к некогерентной атаке со стойкостью других протоколов с кутритами [3, 4]. В качестве меры стойкости протокола используется шенноновская взаимная информация между Алисой и Евой $I_{AE}(D)$, являющаяся функцией среднего уровня ошибок *D*, вносимых Евой в просеянный ключ вследствие перехвата.

В [5] получены выражения для взаимной информации между Алисой и Бобом и Алисой и Евой, как функции от параметров $F$ и $\lambda$ квантовых проб Евы:

$$I_{AB}(F,\lambda) = 2\log_2 3 + \frac{1}{3}(1+F\lambda)\{\log_2(1+F\lambda) - \log_2 9\} + \frac{2}{3}(1-F\lambda)\{\log_2(1-F\lambda) - \log_2 9\}; \qquad (1)$$

$$\begin{aligned} I_{AE}(F,\lambda) &= \log_2 3 - 3\left\langle \tilde{E}_{00} \middle| \tilde{E}_{00} \right\rangle \log_2 \left\langle \tilde{E}_{00} \middle| \tilde{E}_{00} \right\rangle - 6\left\langle \tilde{E}_{11} \middle| \tilde{E}_{11} \right\rangle \log_2 \left\langle \tilde{E}_{11} \middle| \tilde{E}_{11} \right\rangle - \\ &- \Bigg[ -3\left\langle \tilde{E}_{00} \middle| \tilde{E}_{00} \right\rangle W_1 \log_2 \left( \left\langle \tilde{E}_{00} \middle| \tilde{E}_{00} \right\rangle W_1 \right) - 6\left\langle \tilde{E}_{00} \middle| \tilde{E}_{00} \right\rangle (1-W_1)^2 \log_2 \left( \left\langle \tilde{E}_{00} \middle| \tilde{E}_{00} \right\rangle (1-W_1)^2 \right) - \\ &- 6\left\langle \tilde{E}_{11} \middle| \tilde{E}_{11} \right\rangle W_2 \log_2 \left( \left\langle \tilde{E}_{11} \middle| \tilde{E}_{11} \right\rangle W_2 \right) - 12\left\langle \tilde{E}_{11} \middle| \tilde{E}_{11} \right\rangle (1-W_2)^2 \log_2 \left( \left\langle \tilde{E}_{11} \middle| \tilde{E}_{11} \right\rangle (1-W_2)^2 \right) \Bigg], \end{aligned} \qquad (2)$$

где $\left\{\left|\tilde{E}_{kl}\right\rangle\right\}$ – состояния проб Евы после измерения, а их скалярные произведения определяются выражениями

$$\left\langle \tilde{E}_{00} \middle| \tilde{E}_{00} \right\rangle = \frac{1+2F\lambda}{9}; \qquad \left\langle \tilde{E}_{11} \middle| \tilde{E}_{11} \right\rangle = \frac{1-F\lambda}{9}. \tag{3}$$

В (1), (2) и последующих формулах для взаимной информации единицей измерения является бит.

Величины $W_1$ и $W_2$ в (2) представлены формулами [5]

$$W_1 = \left(\frac{1}{3}\sqrt{1+2\tilde{\lambda}_1} + \frac{2}{3}\sqrt{1-\tilde{\lambda}_1}\right)^2; \qquad W_2 = \left(\frac{1}{3}\sqrt{1+2\tilde{\lambda}_2} + \frac{2}{3}\sqrt{1-\tilde{\lambda}_2}\right)^2, \tag{4}$$

где

$$\tilde{\lambda}_1 = \frac{1}{2}\frac{3F+4F\lambda-1}{1+2F\lambda}; \qquad \tilde{\lambda}_2 = \frac{1}{2}\frac{3F-2F\lambda-1}{1-F\lambda}. \tag{5}$$

Средний уровень ошибок между Алисой и Бобом зависит от параметров проб Евы следующим образом [5]

$$D = \frac{2}{3}\left(1-F\lambda\right). \tag{6}$$

Чтобы не быть выявленной легитимными пользователями при проверке нарушения неравенств Белла [1], Ева должна выбирать параметры $F$ и $\lambda$ так, чтобы выполнялось условие

$$F\lambda \geq \frac{6\sqrt{3}-9}{2} \approx 0{,}69615. \tag{7}$$

Для определения уровня стойкости этого протокола к некогерентной атаке необходимо найти зависимости $I_{\mathrm{AB}}(D)$ и $I_{\mathrm{AE}}(D)$, которые не были получены в [5]. Первое выражение легко получить подстановкой $F\lambda$ из (6) в (1):

$$I_{\mathrm{AB}}(D) = 2\log_2 3 + \left(\frac{2}{3} - \frac{D}{2}\right)\left\{\log_2\left(2-\frac{3}{2}D\right) - \log_2 9\right\} + D\left\{\log_2\left(\frac{3}{2}D\right) - \log_2 9\right\}. \tag{8}$$

Что касается $I_{\mathrm{AE}}$, то из (2)…(6) видно, что эта величина, кроме зависимости от *D*, будет зависеть также от одного из параметров проб. Это дает Еве возможность максимизировать информацию о ключе выбором одного из параметров своих проб. Для этого Ева должна сначала выбрать средний уровень ошибок *D*, который она будет создавать при перехвате, так, чтобы он не намного превышал естественный уровень шумов в канале, а затем выбрать один из параметров проб – *F* или $\lambda$ – так, чтобы величина $I_{\mathrm{AE}}$ была максимальной. Второй параметр при этом будет однозначно определяться из (6) для каждого фиксированного *D*, а Ева должна также следить за тем, чтобы параметры ее проб удовлетворяли условию (7).

Зависимость $I_{\mathrm{AE}}$ от параметра *F* представляет собой громоздкое выражение, которое здесь не приводится ввиду того, что, как следует из нашего анализа, $I_{\mathrm{AE}}$ зависит от *F* монотонно. При этом максимальную информацию Ева может получить, выбрав $F = 0{,}69615$, что соответствует $\lambda = 1$. Однако минимальный уровень ошибок, который возникает у легитимных пользователей при таком выборе параметров проб, равен 20,257 %. Очевидно, в этом случае атака будет легко обнаружена, либо прямой проверкой уровня ошибок, который будет значительно превышать естественный уровень помех в квантовом канале, либо проверкой нарушений неравенств Белла (из (6) и (7) следует, что неравенства Белла не нарушаются при $D > 0{,}20257$).

Получим теперь выражение для $I_{\mathrm{AE}}(D\,|\,\lambda)$. Для этого подставим *F* из (6) в (5), а затем полученные выражения для $\tilde{\lambda}_1$ и $\tilde{\lambda}_2$ подставим в (4). Тогда

$$W_1(D\,|\,\lambda) = \frac{1}{9(1-D)}\left[\frac{1{,}5D-1}{\lambda} - 3D + 4 + 2\sqrt{\left(\frac{2-3D}{\lambda} - 6D + 4\right)\left(1 - \frac{1-1{,}5D}{\lambda}\right)}\right]; \tag{9}$$

$$W_2(D\,|\,\lambda)=\frac{1}{9D}\left[\frac{3D-2}{\lambda}+3D+2+4\sqrt{\left(\frac{2-3D}{\lambda}+3D-2\right)\left(1-\frac{1-1{,}5D}{\lambda}\right)}\right]. \qquad (10)$$

Подставив теперь $F\lambda$ из (6) в (3), а затем полученные выражения – в (2), получим окончательно:

$$I_{\text{AE}}(D\,|\,\lambda)=\log_2 3-(1-D)\log_2\frac{1-D}{3}-D\log_2\frac{D}{6}+(1-D)\,W_1(D\,|\,\lambda)\log_2\frac{(1-D)\,W_1(D\,|\,\lambda)}{3}+$$
$$+2(1-D)\,(1-W_1(D\,|\,\lambda))^2\log_2\frac{(1-D)\,(1-W_1(D\,|\,\lambda))^2}{3}+DW_2(D\,|\,\lambda)\log_2\frac{DW_2(D\,|\,\lambda)}{6}+$$
$$+2D(1-W_2(D\,|\,\lambda))^2\log_2\frac{D(1-W_2(D\,|\,\lambda))^2}{6}, \qquad (11)$$

где $W_1(D\,|\,\lambda)$ и $W_2(D\,|\,\lambda)$ определены в (9) и (10) соответственно.

На рис. 1 приведены зависимости $I_{\text{AE}}(D\,|\,\lambda)$ для различных значений параметра $\lambda$. Видно, что эта величина зависит от $\lambda$ не монотонно. Вертикальная штриховая линия на рис. 1 соответствует $D=0{,}20257$.

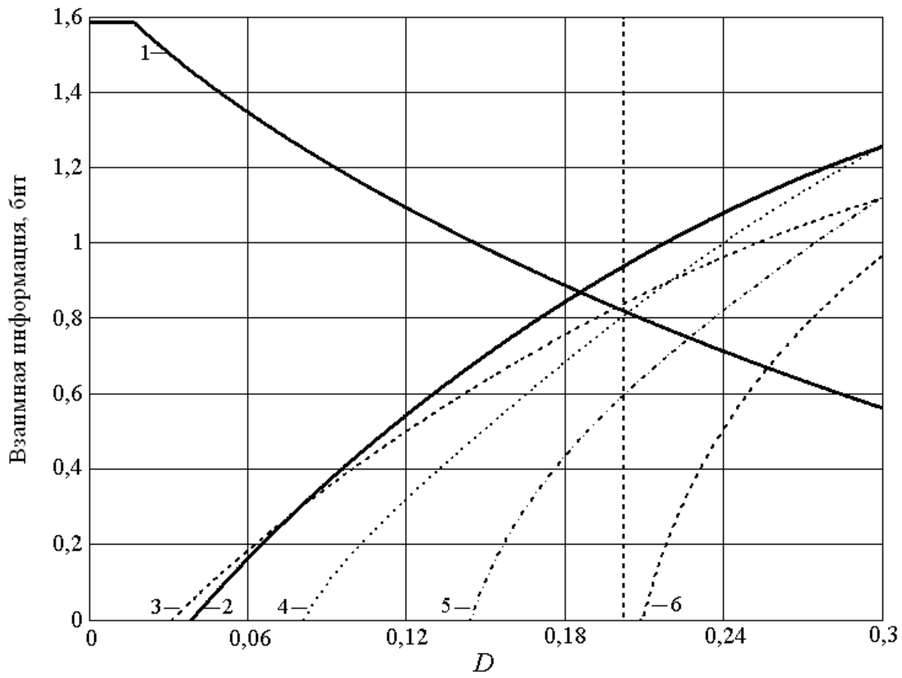


Рисунок 1 – Взаимная информация $I_{\text{AB}}(D)$ (кр. 1) и $I_{\text{AE}}(D\,|\,\lambda)$ для значений параметра $\lambda$: 0,9827 (кр. 2), 1 (кр. 3), 0,9 (кр. 4), 0,8 (кр. 5), 0,7 (кр. 6)

Чтобы найти значение параметра $\lambda$, которое было бы оптимальным для Евы, необходимо использовать теорему Цизара и Кернера, в соответствии с которой Алиса и Боб могут установить секретный ключ посредством процедуры усиления секретности, если взаимная информация между ними больше взаимной информации между Алисой и Евой [1]. Вследствие этого в квантовой криптографии верхней границей допустимого уровня ошибок считают значение $D_{\max}$, которое получают из уравнения $I_{\text{AB}}(D_{\max})=I_{\text{AE}}(D_{\max})$. Таким образом, для определения $D_{\max}$ как функции от $\lambda$ необходимо приравнять правые части (8) и (11). Уравнение, которое получается при этом, можно решить только численно. Решая это уравнение для различных значений $\lambda$, можно найти такое, которому соответствует минимальное значение $D_{\max}$. Именно это значение $\lambda$ и будет оптимальным для Евы.

Решая уравнение, полученное приравниванием (8) и (11), мы нашли, что минимальному $D_{\max}$, равному 0,186, соответствует $\lambda=0{,}9827$ (кривая 2 на рис. 1). Как видно, при таком значении

$\lambda$ Ева может получить больше информации, чем при любом другом $\lambda$, в широком интервале значений уровня ошибок $D$.

Выражения для $I_{\text{AB}}(D)$, а также для $I_{\text{AE}}(D)$ при оптимальной некогерентной атаке на протокол с передачей одиночных кутритов были получены в [3]:

$$I_{\text{AB}}(D) = \log_2 3 + (1-D)\log_2(1-D) + D\log_2\left(\frac{D}{2}\right); \tag{12}$$

$$I_{\text{AE}}(D) = \log_2 3 + (1-D)\left[ f(D)\log_2 f(D) + (1-f(D))\log_2\left(\frac{1-f(D)}{2}\right)\right], \tag{13}$$

где $f(D) = \dfrac{3-2D+\sqrt{(3-2D)^2 - 9(1-2D)^2}}{9(1-D)}$.

Соответствующие выражения для томографического протокола с кутритами имеют вид [4]

$$I_{\text{AB}}(D) = \log_2 3 + \beta_0 \log_2 \beta_0 + (1-\beta_0)\log_2 \beta_1; \tag{14}$$

$$I_{\text{AE}}(D) = \log_2 3 + \beta_0 [\eta_0 \log_2 \eta_0 + (1-\eta_0)\log_2 \eta_1], \tag{15}$$

где $\beta_0 = 1-D$; $\beta_1 = \dfrac{D}{2}$; $\eta_0 = 1-2\eta_1$; $\eta_1 = \dfrac{1}{3}\left(\sqrt{r_0} - \sqrt{r_1}\right)^2$; $r_0 = 1 - \dfrac{\beta_1}{\beta_0} + r_1$; $r_1 = \dfrac{\beta_1}{3\beta_0}$.

Путем несложных алгебраических преобразований можно доказать тождественность выражений (12) и (14), а также тождественность выражений (13) и (15). Таким образом, протокол с передачей одиночных кутритов [3] и томографический протокол с кутритами [4] имеют одинаковую стойкость к оптимальной некогерентной атаке.

На рис. 2 приведены зависимости $I_{\text{AB}}(D)$ и $I_{\text{AE}}(D)$ для протокола с перепутанными кутритами [5] (кривые 1, 3), а также для протоколов [3] и [4] (кривые 2, 4), где $I_{\text{AE}}(D\,|\,\lambda)$ для протокола [5] построено при $\lambda = 0{,}9827$, что соответствует найденному оптимальному значению этого параметра для Евы. Кривые 1 и 3 пересекаются в точке $D = 0{,}186$, а кривые 2 и 4 – в точке $D = 0{,}227$. Таким образом, из теоремы Цизара-Кернера следует, что протоколы, предложенные в [3] и [4], более стойки к оптимальной некогерентной атаке, чем протокол с перепутанными кутритами, предложенный в [5].

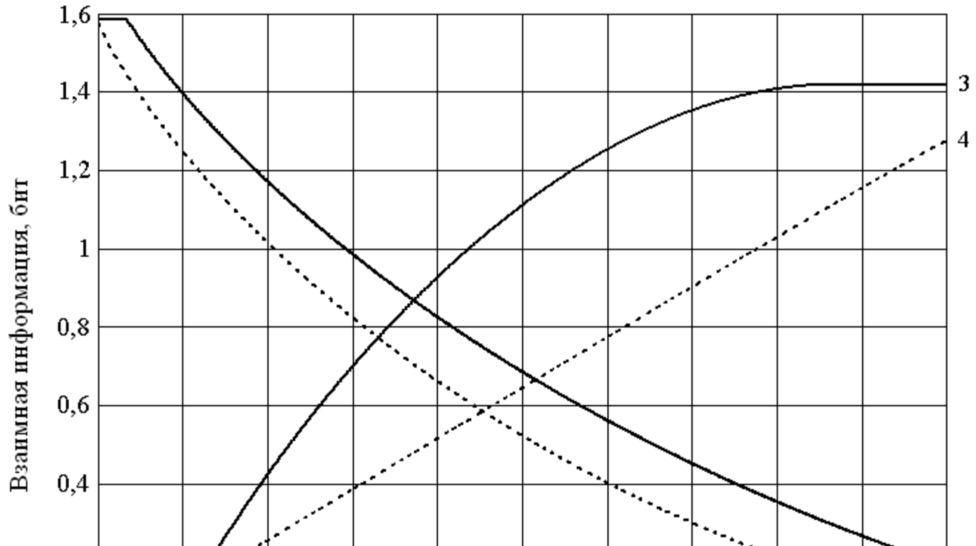


Рисунок 2 – Взаимная информация $I_{\text{AB}}(D)$ (кривые 1 и 2) и $I_{\text{AE}}(D)$ (кривые 3 и 4) для трех протоколов с кутритами (см. текст)

При использовании идеальных источника, приемника сигналов и измерительной аппаратуры, а также бесшумного квантового канала, эффективность протокола с одиночными кутритами [3], как и томографического протокола [4] равна $1/4$, а протокола с перепутанными кутритами [5] – $1/9$. Отсюда следует, что из трех рассмотренных протоколов наилучшими, как по критерию эффективности, так по критерию стойкости к некогерентной атаке, являются два протокола – протокол с одиночными кутритами и томографический протокол.

Таким образом, найдены оптимальные параметры квантовых проб для некогерентной атаки на протокол с перепутанными кутритами, предложенный в [5]. Показано, что стойкость к оптимальной некогерентной атаке протокола с одиночными кутритами и томографического протокола с кутритами, предложенных в [3] и [4] соответственно, одинакова. При этом стойкость этих двух протоколов выше стойкости протокола [5]. Учитывая также, что эти протоколы имеют бóльшую эффективность, чем протокол [5], оба их следует считать наиболее перспективными для практического использования. Если учесть также сложность технической реализации трех рассмотренных протоколов, то наиболее простым с этой точки зрения в настоящее время является протокол с передачей одиночных кутритов [3]. Следовательно, этот протокол следует признать наилучшим в смысле эффективности, простоты технической реализации и стойкости к оптимальной некогерентной атаке.

***Литература***

1. *Баумейстер Д., Экерт А., Цайлингер А.* Физика квантовой информации. – М.: Постмаркет, 2002. – 376 с.
2. *Dusek M., Lutkenhaus N., Hendrych M.* Quantum Cryptography // Progress in Optics. – V. 49. – Elsevier, 2006. – P. 381–454.
3. *Bruß D., Macchiavello C*. Optimal Eavesdropping in Cryptography with Three-Dimensional Quantum States // Physical Review Letters. – 2002. – V. 88, № 12. – Art. 127901.
4. *Liang Y.C., Kaszlikowski D., Englert B.-G., Kwek L.C., Oh C.H*. Tomographic quantum cryptography // Physical Review A. – 2003. – V. 68, № 2. – Art. 022324.
5. *Kaszlikowski D., Chang K., Oi D.K.L., Kwek L.C., Oh C.H*. Quantum Cryptography Based On Bell Inequalities for Three-Dimensional System // Physical Review A. – 2003. – V. 67, № 1. – Art. 012310.