УДК 003.26:621.39

Василиу Е.В.

Vasiliu E.V.

АНАЛИЗ БЕЗОПАСНОСТИ ПИНГ-ПОНГ ПРОТОКОЛА С КВАНТОВЫМ ПЛОТНЫМ КОДИРОВАНИЕМ

SECURITY ANALYSIS OF THE PING-PONG PROTOCOL WITH QUANTUM DENSE CODING

Аннотация. На основе методов квантовой теории информации проанализирована безопасность пинг-понг протокола с квантовым плотным кодированием. Показано, что этот протокол небезопасен как для передачи криптографического ключа, так и для прямой передачи секретных сообщений. Безопасное использование пинг-понг протокола с квантовым плотным кодированием возможно только для передачи битовых последовательностей специального вида.

Summary. Based on the methods of quantum information theory the security of ping-pong protocol with quantum dense coding is analysed. It is shown, that this protocol is not secure both for transfer of a cryptographic key, and for direct transfer of confidential messages. Safe use of the ping-pong protocol with quantum dense coding is possible only for transfer of bit sequences of a special kind.

Цель криптографии состоит в том, чтобы гарантировать, что секретное сообщение может быть прочитано только тем, для кого оно предназначено, и что сообщение не было изменено во время передачи. Квантовая криптография, бурно развивающееся в последние годы направление квантовой теории информации, предлагает новый подход к решению важной проблемы передачи секретных сообщений [1…3].

Одно из направлений квантовой криптографии – квантовые протоколы распределения ключей (КПРК), безопасность которых (*при определенных условиях*) гарантируется законами квантовой механики [1…3]. Другое направление – квантовые протоколы безопасной связи (КПБС), которые, в отличие от КПРК, предназначены для непосредственной передачи секретных сообщений, без первоначального распределения ключа для их шифрования [3…6]. При этом сообщение кодируется непосредственно квантовыми состояниями частиц. Таким образом, КПБС требуют большего уровня надежности, чем КПРК, так как подслушивающий агент в канале связи не только должен быть обнаружен легитимными пользователями, но и при этом не должен получить значительной части передаваемого сообщения [4]. Следует также отметить, что, поскольку сообщение, передаваемое через обычный классический канал, может быть полностью скопировано, невозможно передать секретное сообщение непосредственно через классический канал, в отличие от квантового канала связи [4].

В [5] предложен КПБС, названный пинг-понг протоколом, в котором используется пара фотонов, максимально перепутанных по их поляризационным степеням свободы. Для передачи бита используется только один из этих фотонов, поэтому подслушивающий агент (Ева), перехватив фотон и измерив его поляризацию, не может получить значение бита, не имея доступа ко второму фотону [5]. Тем не менее, используя квантовые пробы и выполняя соответствующие унитарные операции и последующие измерения над составными (фотоны-пробы) квантовыми системами, Ева имеет возможность перехватить некоторую часть сообщения [5]. Поэтому важной задачей квантовой криптографии является анализ условий выполнения пинг-понг протокола и его усовершенствований, при которых атака Евы будет гарантированно обнаружена и при этом она сможет перехватить лишь незначительную часть секретного сообщения.

В [5] проанализирована безопасность пинг-понг протокола и показано, что этот протокол полностью безопасен для передачи криптографического ключа. Для передачи секретных сообщений пинг-понг протокол квазибезопасен, т. е. любая эффективная атака Евы будет обнаружена, но прежде она может получить небольшую часть сообщения [5].

В пинг-понг протоколе [5] каждый передаваемый фотон (один из перепутанной пары) используется для кодирования одного классического бита. При этом используются два из четырех максимально перепутанных и взаимно ортогональных состояний в системе двух квантовых частиц – два из четырех состояния Белла. Используя все эти четыре состояния вместо двух, можно увеличить информационную емкость в два раза, т. е. передавать два бита информации с помощью одного фотона – так называемое квантовое плотное кодирование [1].

Эта идея усовершенствования пинг-понг протокола с помощью квантового плотного кодирования была предложена в [6]. Однако безопасность такого усовершенствованного протокола детально не анализировалась, было показано только, что вероятность обнаружения Евы отлична от нуля при некоторых условиях. Целью настоящей работы является детальный анализ безопасности пинг-понг протокола с квантовым плотным кодированием.

1. Пинг-понг протокол с квантовым плотным кодированием. Опишем кратко схему пинг-понг протокола с квантовым плотным кодированием [6].

Перепутанная пара фотонов может находиться в одном из четырех состояний Белла:

$$\begin{aligned}
\left|\varphi^{+}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|0\right\rangle + \left|1\right\rangle\left|1\right\rangle\right);\\
\left|\varphi^{-}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|0\right\rangle - \left|1\right\rangle\left|1\right\rangle\right);\\
\left|\psi^{+}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|1\right\rangle + \left|1\right\rangle\left|0\right\rangle\right);\\
\left|\psi^{-}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|1\right\rangle - \left|1\right\rangle\left|0\right\rangle\right),
\end{aligned} \qquad (1)$$

где $\left|0\right\rangle$ и $\left|1\right\rangle$ соответствуют горизонтальной и вертикальной поляризации фотонов.

Боб (принимающая сторона) приготавливает пару фотонов в состоянии $\left|\psi^{+}\right\rangle$. Он хранит один фотон (“домашний фотон”) в своей лаборатории и посылает Алисе (передающая сторона) другой фотон (“передаваемый фотон”) через квантовый канал (“пинг”). Алиса случайным образом переключается между режимом передачи сообщения и режимом контроля подслушивания.

В режиме передачи сообщения (рис. 1) Алиса выполняет унитарную операцию U_{ij} над передаваемым фотоном для кодирования информации и посылает его назад Бобу (“понг”). Кодирующие операции Алисы имеют вид [6]

$$U_{00} = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};\ U_{01} = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix};\ U_{10} = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};\ U_{11} = i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad (2)$$

и соответствуют следующим двухбитовым комбинациям: «00», «01», «10» и «11». σ_x, σ_y и σ_z в (2) – матрицы Паули.

Когда Боб получает передаваемый фотон обратно, он выполняет измерение над обоими фотонами в базисе Белла (1), чтобы декодировать посланную Алисой двухбитовую последовательность (см. рис. 1). Таким образом, одна пара перепутанных фотонов служит для передачи двух битов классической информации.

В режиме контроля подслушивания (рис. 2) Алиса случайным образом выбирает один из базисов – $B_z = \left\{\left|0\right\rangle, \left|1\right\rangle\right\}$ или $B_x = \left\{\left|+\right\rangle, \left|-\right\rangle\right\}$ – для измерения поляризации передаваемого фотона, где $\left|+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)$ и $\left|-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)$. Затем, используя публичный классический канал, Алиса посылает Бобу результат измерения и использованный ею базис. Боб также переключается в режим контроля и измеряет домашний фотон в том же базисе, который использовала Алиса. Затем он сравнивает оба результата измерения – свой и Алисы. Если результаты совпадают, то это означает, что Ева подслушивает, – и передача прерывается. В противном случае Боб посылает Алисе следующий фотон.

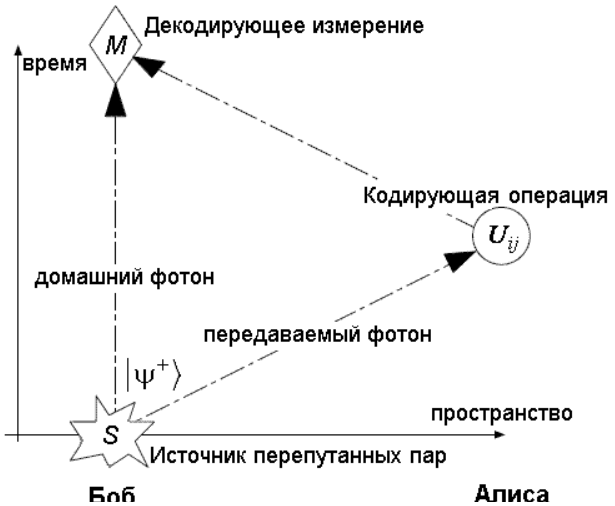

Рисунок 1 – Режим передачи сообщений

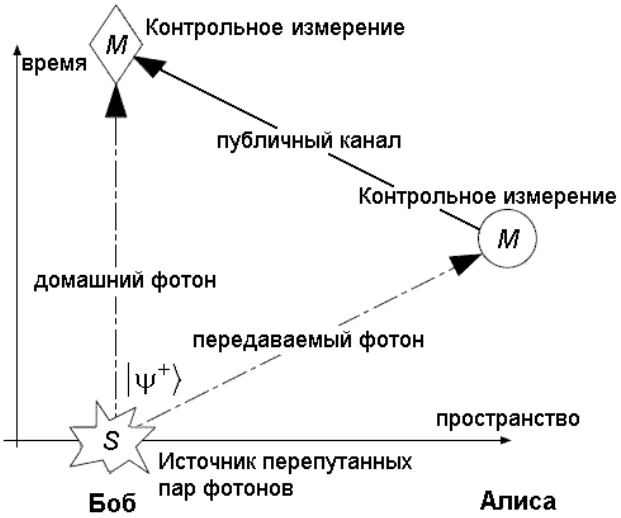

Рисунок 2 – Режим контроля подслушивания

2. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием. Цель подслушивающего агента Евы – определить, какую кодирующую операцию выполнила Алиса. Так как Ева не имеет доступа к "домашнему фотону" Боба, то она может производить манипуляции только с передаваемым фотоном, однако простой перехват фотона на пути от Алисы к Бобу и измерение его поляризации не дает Еве никакой информации вследствие перепутанности передаваемого фотона с "домашним" [5]. Поэтому Ева должна сначала выполнить "атакующую операцию" $\hat{A}$, перепутывая с передаваемым фотоном свою пробу (рис. 3), а после выполнения Алисой кодирующей операции выполнить измерение над составной системой "передаваемый фотон – проба" (см. рис. 3).

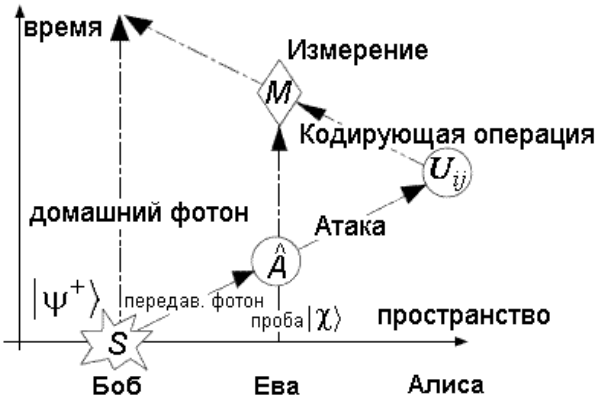

Рисунок 3 – Атака Евы

Кроме кодирующей операции, Алиса с определенной вероятностью должна выполнять и контрольное измерение, но, так как она выполняет это измерение до финального измерения Евы, последнее не влияет на вероятность обнаружения атаки. Таким образом, легитимные пользователи могут выявить только атакующую операцию $\hat{A}$.

Так как для Евы состояние передаваемого Бобом фотона неотличимо от полностью смешанного состояния, то это состояние можно записать в виде $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, что соответствовало бы ситуации, если бы Боб посылал передаваемый фотон в состояниях $|0\rangle$ либо $|1\rangle$ с одинаковой вероятностью $p = 1/2$ [5]. Тогда состояния составной системы "передаваемый фотон – проба Евы" после атаки записываются в виде

$$|\psi_1\rangle = \hat{A}|0,\chi\rangle = \alpha|0,\chi_{00}\rangle + \beta|1,\chi_{01}\rangle;$$
$$|\psi_2\rangle = \hat{A}|1,\chi\rangle = \alpha'|0,\chi_{10}\rangle + \beta'|1,\chi_{11}\rangle, \quad (3)$$

где $\{|\chi_{ik}\rangle\}$ – множество состояний пробы Евы; i, k – индексы однофотонных состояний у Боба и Алисы соответственно в каждой перепутанной паре фотонов.

Так как атакующая операция Евы $\hat{A}$ унитарна, то комплексные коэффициенты α, β, α', β' должны удовлетворять соотношениям $|\alpha|^2 + |\beta'|^2 = 1$; $|\alpha'|^2 + |\beta|^2 = 1$; $\alpha\beta^* + \alpha'^*\beta' = 0$, откуда следует: $|\beta'|^2 = |\beta|^2$ и $|\alpha'|^2 = |\alpha|^2$.

Вероятность обнаружить атакующую операцию Евы в режиме контроля подслушивания

$$d = |\beta|^2 = |\beta'|^2 = 1 - |\alpha|^2 = 1 - |\alpha'|^2. \tag{4}$$

Рассмотрим сначала случай, когда Боб посылает $|0\rangle$. Тогда после атакующей операции Евы состояние системы будет $|\psi_1\rangle = \hat{A}|0,\chi\rangle = \alpha|0,\chi_{00}\rangle + \beta|1,\chi_{01}\rangle$, а соответствующая матрица плотности

$$\rho_1 = |\psi_1\rangle\langle\psi_1| = |\alpha|^2|0,\chi_{00}\rangle\langle 0,\chi_{00}| + \alpha\beta^*|0,\chi_{00}\rangle\langle 1,\chi_{01}| + \alpha^*\beta|1,\chi_{01}\rangle\langle 0,\chi_{00}| + |\beta|^2|1,\chi_{01}\rangle\langle 1,\chi_{01}|. \tag{5}$$

Затем, после выполнения Алисой кодирования с помощью унитарных операций U_{00}, U_{01}, U_{10}, U_{11} (2) с вероятностями p_1, p_2, p_3, p_4 соответственно ($p_1 + p_2 + p_3 + p_4 = 1$), матрица плотности состояния системы будет иметь вид

$$\rho_1' = \begin{pmatrix} (p_3 + p_4)|\beta^2| & 0 & 0 & (p_3 - p_4)\alpha^*\beta \\ 0 & (p_1 + p_2)|\alpha^2| & (p_1 - p_2)\alpha\beta^* & 0 \\ 0 & (p_1 - p_2)\alpha^*\beta & (p_1 + p_2)|\beta^2| & 0 \\ (p_3 - p_4)\alpha\beta^* & 0 & 0 & (p_3 + p_4)|\alpha^2| \end{pmatrix}. \tag{6}$$

Максимальное количество классической информации $I_{\max}$, которое может быть извлечено из квантового состояния, определяется энтропией фон Неймана:

$$I_{\max} = S(\rho_1') \equiv -Tr\{\rho_1' \log_2 \rho_1'\} = \sum_{i=1}^{4} -\lambda_i \log_2 \lambda_i, \tag{7}$$

где λ_i – собственные значения матрицы плотности ρ_1' (6). $I_{\max}$ – это максимальное количество информации, которое может получить Ева после измерения состояния передаваемого фотона, который она перехватывает на пути от Алисы к Бобу (см. рис. 3).

Решив задачу на собственные значения для матрицы плотности ρ_1' (6), получим

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16p_1p_2|\alpha|^2|\beta|^2};$$

$$\lambda_{3,4} = \frac{1}{2}(p_3 + p_4) \pm \frac{1}{2}\sqrt{(p_3 + p_4)^2 - 16p_3p_4|\alpha|^2|\beta|^2}. \tag{8}$$

Используя (4), можно выразить $|\alpha|^2|\beta|^2$ через вероятность обнаружения атаки d: $|\alpha|^2|\beta|^2 = (1 - |\beta|^2)|\beta|^2 = d - d^2$. Тогда собственные значения (8) принимают вид

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16p_1p_2(d - d^2)};$$

$$\lambda_{3,4} = \frac{1}{2}(p_3 + p_4) \pm \frac{1}{2}\sqrt{(p_3 + p_4)^2 - 16p_3p_4(d - d^2)}. \tag{9}$$

Если теперь рассмотреть случай, когда Боб вместо $|0\rangle$ посылает $|1\rangle$, то представленные выше вычисления выполняются аналогично, приводя к тем же основным результатам (7) и (9).

Когда Алиса выполняет все четыре кодирующие операции (2) с одинаковой вероятностью, т. е. $p_1 = p_2 = p_3 = p_4 = \frac{1}{4}$, тогда $\lambda_{1,2} = \lambda_{3,4} = \frac{1}{4} \pm \frac{1}{2}\sqrt{d^2 - d + \frac{1}{4}}$. Отсюда при $d = 0$ получим: $\lambda_1 = \lambda_3 = \frac{1}{2}$, $\lambda_2 = \lambda_4 = 0$ и из (7) следует, что $I_{\max} = 1$. Таким образом, при кодировании Алисой строки битов с одинаковым количеством двухбитовых комбинаций, Ева, оставаясь необнаруженной,

может получить 1 бит классической информации, измерив состояние передаваемого фотона, который несет 2 бита. Это означает, в частности, что пинг-понг протокол с плотным кодированием небезопасен для передачи случайного криптографического ключа, так как в случае, если ключ содержит одинаковое число комбинаций «00», «01», «10» и «11», подслушивающий агент может узнать половину битов ключа, вообще не будучи обнаруженным. Отметим, что при генерации случайного ключа для симметричного шифрования с помощью генератора псевдослучайных чисел с равномерным распределением количество возможных ключей с приблизительно одинаковым числом вышеназванных двухбитовых комбинаций составляет значительную долю от всего множества возможных ключей.

На рис. 4 приведены зависимости максимального количества информации Евы $I_{\max}$ (7) от вероятности *d* того, что атака будет обнаружена в режиме контроля подслушивания. Кривые 1…7 на рис. 4 соответствуют следующим значениям вероятностей $p_1 \ldots p_4$:

1 – $p_1 = p_2 = p_3 = p_4 = 0{,}25$;

2 – $p_1 = 0{,}1$, $p_2 = 0{,}2$, $p_3 = 0{,}3$, $p_4 = 0{,}4$;

3 – $p_1 = \frac{1}{3}$, $p_2 = \frac{1}{3}$, $p_3 = \frac{1}{3}$, $p_4 = 0$;

4 – $p_1 = 0{,}5$, $p_2 = 0{,}5$, $p_3 = 0$, $p_4 = 0$;

5 – $p_1 = 0{,}8$, $p_2 = 0{,}1$, $p_3 = 0{,}1$, $p_4 = 0$;

6 – $p_1 = 0{,}3$, $p_2 = 0$, $p_3 = 0$, $p_4 = 0{,}7$;

7 – $p_1 = 0{,}8$, $p_2 = 0{,}2$, $p_3 = 0$, $p_4 = 0$.

Как видно из рис. 4, если Алиса использует четыре кодирующие операции (2) с равными или близкими вероятностями, то Ева может получить значительное количество информации при малой вероятности ее обнаружения (кривые 1…3 на рис. 4). Только в случае передачи специальных битовых строк, например «00010001…», что соответствует кривой 4 на рис. 4, или «00» с вероятностью 0,8 и «01» с вероятностью 0,2, что соответствует кривой 7, Ева получит небольшое количество информации и при этом вероятность ее обнаружения $d > 0$ при $I_{\max} > 0$.

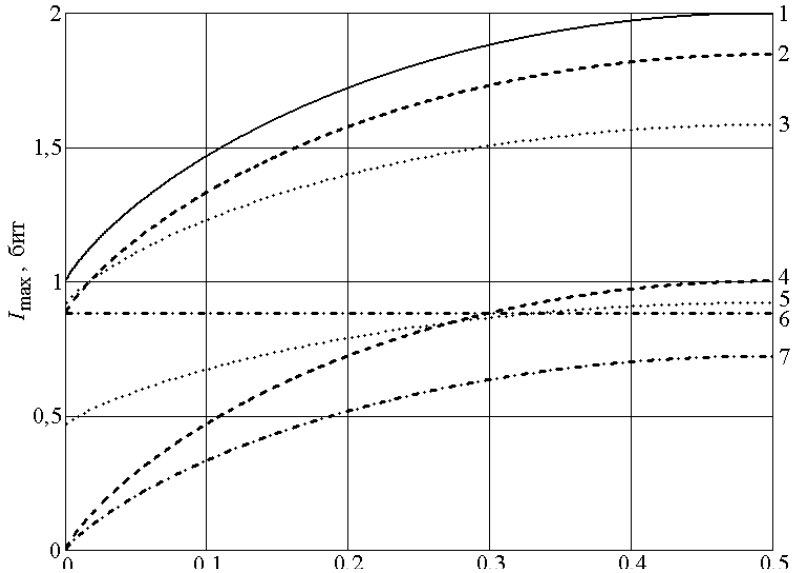

Рисунок 4 – Зависимость максимальной информации Евы $I_{\max}$ (7) от вероятности d обнаружения атаки

На рис. 5 показана максимальная информация Евы $I_{\max}$ при $d = 0$. В этом случае собственные значения матрицы плотности ρ'_1 (6): $\lambda_1 = p_1 + p_2$, $\lambda_2 = 0$, $\lambda_3 = p_3 + p_4 = 1 - p_1 - p_2$, $\lambda_4 = 0$. Подставив эти собственные значения в (7), получим

$$I_{\max}(p_1, p_2) = -(p_1 + p_2)\cdot \log_2(p_1 + p_2) - (1 - p_1 - p_2)\cdot \log_2(1 - p_1 - p_2). \qquad (10)$$

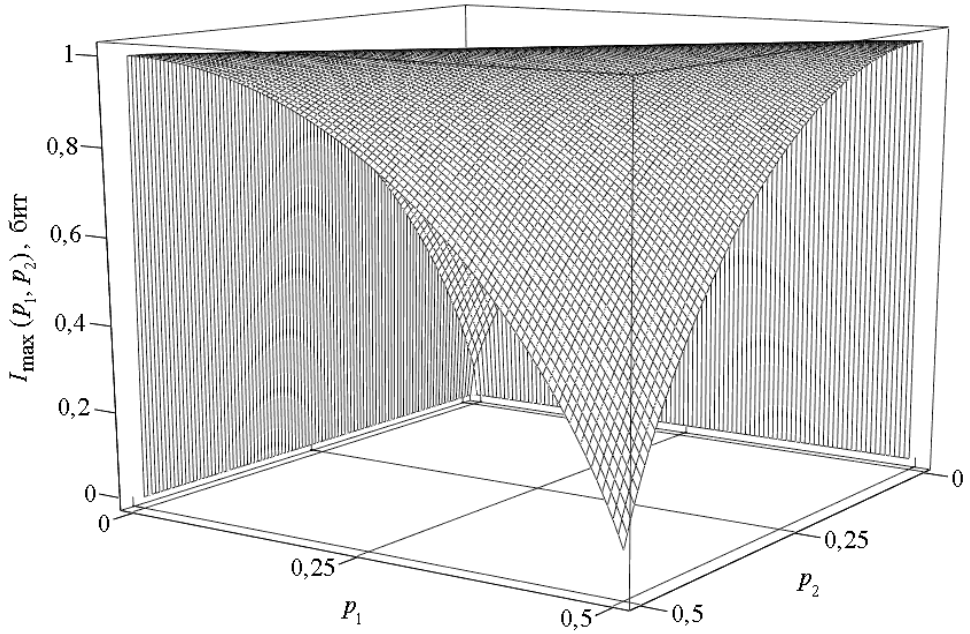

Рисунок 5 – Максимальная информация Евы $I_{\max}(p_1, p_2)$ (10) при $d = 0$

Как видно из рис. 5, Ева, оставаясь необнаруженной ($d = 0$), может получить 1 бит информации на передаваемый фотон при соотношениях между вероятностями кодирующих операций Алисы $p_1 + p_2 = 0{,}5$; $p_3 + p_4 = 0{,}5$. С другой стороны, при $p_1 = p_2 = 0$; $p_3 + p_4 = 1$ и при $p_1 = p_2 = 0{,}5$; $p_3 = p_4 = 0$ информация Евы равна нулю (при $d = 0$). Тем самым подтверждается сделанный выше вывод о безопасности пинг-понг протокола с квантовым плотным кодированием только для передачи битовых строк специального вида.

Отметим также еще одну специфическую особенность способа кодирования сообщений (2). Если Алиса всегда использует только одну из четырех кодирующих операций (2), то из (9) и (7) следует, что $I_{\max} \equiv 0$. Таким образом, при рассмотренной в настоящей работе атаке Евы она не в состоянии различить битовые строки вида «0000…», «0101…», «1010…» и «1111…». Очевидно, что если Алиса и Боб заранее договорятся о смысле таких строк, то пинг-понг протокол с квантовым плотным кодированием полностью безопасен для их передачи. Однако при необходимости передавать произвольные секретные сообщения или секретный криптографический ключ этот протокол не является безопасным, в отличие от оригинального пинг-понг протокола без плотного кодирования [5].

Таким образом, проанализирована безопасность пинг-понг протокола с квантовым плотным кодированием. Показано, что этот протокол небезопасен как для передачи криптографического ключа, так и для прямой передачи секретных сообщений. Безопасное использование пинг-понг протокола с квантовым плотным кодированием возможно только для передачи битовых строк специального вида, когда одна или две из возможных четырех комбинаций пар битов передаются с подавляющей вероятностью.

Литература

1. *Баумейстер Д., Экерт А., Цайлингер А*. Физика квантовой информации. – М.: Постмаркет, 2002. – 376 с.
2. *Dusek M., Lütkenhaus N., Hendrych M.* Quantum Cryptography // Progress in Optics. – Elsevier. – 2006. – V. 49. – P. 381–454.
3. *Василиу Е.В., Воробиенко П.П.* Проблемы развития и перспективы использования квантово-криптографических систем // Наукові праці ОНАЗ ім. О.С. Попова. – 2006. – № 1. – С. 3–17.

4. *Deng F.-G., Long G.L., Liu X.-S.* Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block // Physical Review A. – 2003. – V. 68. – № 4. – Art. 042317.
5. *Boström K., Felbinger T*. Deterministic Secure Direct Communication Using Entanglement // Physical Review Letters. – 2002. – V. 89. – № 18. – Art. 187902.
6. *Cai Q*.-Y., Li B.-W. Improving the capacity of the Boström-Felbinger protocol // Physical Review A. – 2004. – V. 69. – № 5. – Art. 054301.