УДК 003.26:621.39+530.145

Василиу Е.В.
Vasiliu E.V.

АНАЛИЗ АТАКИ НА ПИНГ-ПОНГ ПРОТОКОЛ С ТРИПЛЕТАМИ ГРИНБЕРГЕРА – ХОРНА – ЦАЙЛИНГЕРА

ANALYSIS OF ATTACK ON THE PING-PONG PROTOCOL WITH GREENBERGER – HORNE – ZEILINGER'S TRIPLETS

Аннотация. На основе методов квантовой теории информации проанализирована атака с использованием квантовых проб на пинг-понг протокол с триплетами Гринбергера – Хорна - Цайлингера. Показано, что при использовании легитимными пользователями в режиме контроля подслушивания двух измерительных базисов протокол является квазибезопасным, аналогично пинг-понг протоколу с белловскими парами. Показано также, что увеличение числа перепутанных кубитов, используемых для реализации пинг-понг протокола, позволяет увеличить не только эффективность протокола, но и повысить уровень его безопасности.

Summary. The attack with use of quantum probes on the ping-pong protocol with Greenberger – Horne – Zeilinger's triplets is analysed using the methods of quantum information theory. It is shown, that the protocol is quasisecure using two measuring bases by legitimate users in a control mode similarly to the ping-pong protocol with the Bell states. It is also shown, that the increase of entangled qubits number, used for realisation of the ping-pong protocol, allows to increase not only protocol efficiency, but also to increase its level of security.

В настоящее время квантовая криптография – быстро развивающееся приложение квантовой теории информации, которое предлагает новый подход к построению защищенных систем конфиденциальной связи. Квантовые протоколы безопасной связи – новая концепция в квантовой криптографии – предназначены для непосредственной передачи секретных сообщений через квантовый канал без предварительного шифрования сообщений [1…3]. Разработка таких протоколов, анализ их стойкости ко всем стратегиям атак, допускаемым законами квантовой механики, является важной научно-технической проблемой.

Одним из протоколов квантовой безопасной связи является пинг-понг протокол, в котором используется пара максимально перепутанных кубитов – состояния Белла, а для передачи используется только один кубит из перепутанной пары [1]. При этом за один цикл протокола передается один бит информации. Пинг-понг протокол с квантовым плотным кодированием [2, 3] позволяет, пересылая один кубит, передать два бита информации за один цикл протокола. Возможно дальнейшее увеличение информационной емкости квантового канала путем использования полностью перепутанных триплетов, четверок и т.д. кубитов, например, состояний Гринбергера – Хорна – Цайлингера (ГХЦ). Так, при использовании ГХЦ-триплетов, пересылая два кубита между легитимными пользователями канала, Алисой и Бобом, за один цикл протокола можно передать три бита информации.

Пинг-понг протокол с использованием ГХЦ-триплетов предложен в [4]. Разработана схема измерений для процедуры контроля подслушивания, которая необходима для обеспечения асимптотической безопасности протокола. Однако атака подслушивающего агента, Евы, с использованием квантовых проб, унитарных операций и последующих измерений над составными (фотоны–пробы) квантовыми системами не анализировалась. Целью настоящей работы является детальный анализ атаки с использованием квантовых проб на пинг-понг протокол с ГХЦ-триплетами, а также комплексная оценка безопасности этого протокола.

1. Пинг-понг протокол с ГХЦ-триплетами. Опишем кратко схему пинг-понг протокола с ГЦХ-состояниями триплета кубитов [4].

Имеется восемь полностью перепутанных ортогональных трехкубитных ГХЦ-состояний:

$$\left|\Psi_{1,2}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|000\right\rangle \pm \left|111\right\rangle\right); \quad \left|\Psi_{3,4}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|100\right\rangle \pm \left|011\right\rangle\right);$$

$$\left|\Psi_{5,6}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|010\right\rangle \pm \left|101\right\rangle\right); \quad \left|\Psi_{7,8}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|110\right\rangle \pm \left|001\right\rangle\right), \tag{1}$$

где $|0\rangle$ и $|1\rangle$ – базисные состояния одного кубита. Так как в квантовых коммуникациях в качестве кубитов используют фотоны, то в этом случае $|0\rangle$ и $|1\rangle$ соответствуют вертикальной и горизонтальной поляризациям фотона.

Поскольку восемь состояний ГХЦ нормированы и взаимно ортогональны, то они образуют базис в гильбертовом пространстве трех кубитов.

Боб (принимающая сторона) подготавливает три фотона в состоянии $|\Psi_1\rangle$. Он хранит третий фотон (“домашний фотон”) в своей лаборатории и посылает Алисе (передающая сторона) первые два (“передаваемые фотоны”) через квантовый канал. Алиса случайным образом переключается между режимом передачи сообщения и режимом контроля подслушивания.

В режиме передачи сообщения (рис. 1) Алиса выполняет кодирующую унитарную операцию U_{ijk} над двумя передаваемыми фотонами и посылает их назад Бобу.

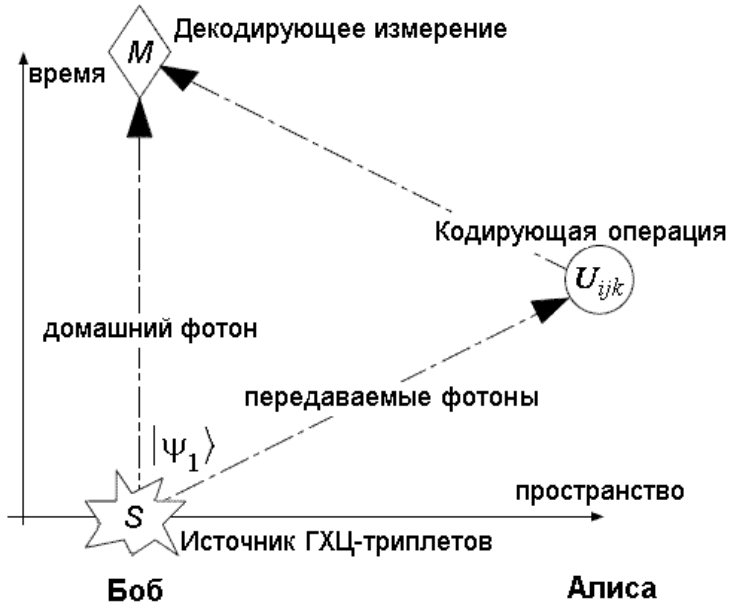

Рисунок 1 – Режим передачи сообщений

Кодирующие операции Алисы, построенные таким образом, чтобы они содержали минимально возможное количество нетождественных операций, имеют вид [4]:

$$U_{000} = I \otimes I;\ U_{001} = I \otimes \sigma_z;\ U_{010} = \sigma_x \otimes I;\ U_{011} = i\sigma_y \otimes I;$$
$$U_{100} = I \otimes \sigma_x;\ U_{101} = I \otimes i\sigma_y;\ U_{110} = \sigma_x \otimes \sigma_x;\ U_{111} = i\sigma_y \otimes \sigma_x \quad (2)$$

и соответствуют следующим трехбитовым комбинациям: «000», «001», «010», «011», «100», «101», «110» и «111». В (2) использованы следующие обозначения: $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ – тождественный оператор; $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$ и $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ – операторы Паули.

Получив два кубита обратно от Алисы, Боб выполняет измерение над всеми тремя кубитами в ГХЦ-базисе ($GHZ = \{|\Psi_k\rangle\langle\Psi_k|\}$, где $k = 1\ldots8$) и тем самым достоверно определяет трехбитовую строку, которую она послала (см. рис. 1).

В режиме контроля подслушивания (рис. 2) Алиса сначала сообщает Бобу по обычному незащищенному каналу о переключении в этот режим. Тогда Боб случайным образом выбирает один из двух измерительных базисов: $B_z = \{|0\rangle\langle 0|; |1\rangle\langle 1|\}$ или $B_x = \{|+\rangle\langle +|; |-\rangle\langle -|\}$, где $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ и $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, а затем выполняет измерение состояния своего “домашнего” фотона в выбранном базисе.

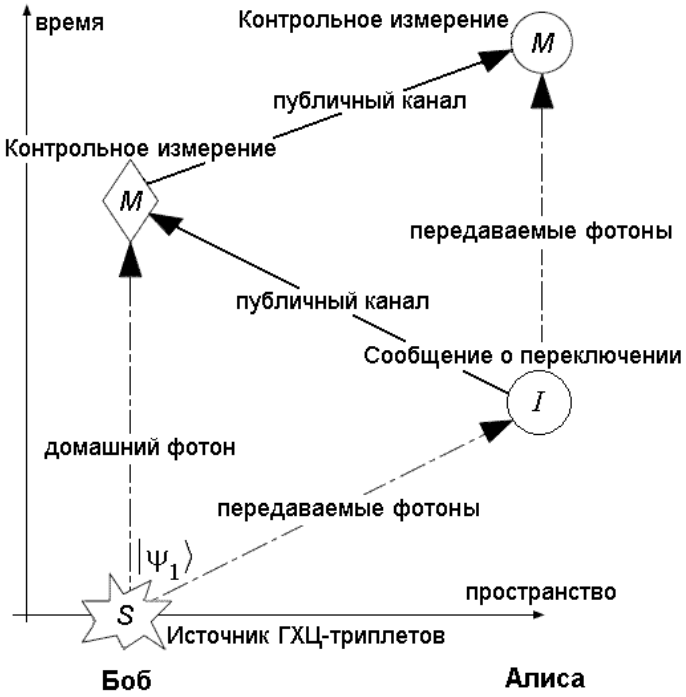

Рисунок 2 – Режим контроля подслушивания

В результате измерения в базисе B_z Боб получит $|0\rangle$ с вероятностью $1/2$, а состояние триплета после измерения будет $|000\rangle$. Тогда Боб сообщает Алисе по обычному каналу, что он выбрал базис B_z, а также сообщает результат своего измерения. Алиса выполняет измерения состояний своих двух кубитов также в базисе B_z, при этом ее результат должен быть $|0\rangle$, $|0\rangle$. С вероятностью $1/2$ Боб получит $|1\rangle$ и состояние триплета будет $|111\rangle$. Тогда Алиса, выполнив измерения в том же базисе, должна получить $|1\rangle$, $|1\rangle$. Если же результаты Алисы отличаются от приведенных, то это означает, что Ева подслушивает (мы пренебрегаем здесь возможными ошибками при излучении, детектировании и передаче фотонов и считаем, что используется идеальное оборудование). Тогда Алиса и Боб прерывают передачу. В противном случае Боб подготавливает следующий ГХЦ-триплет и выполняется следующий цикл протокола.

Аналогично, если в режиме контроля подслушивания Боб выберет базис B_x, то он с вероятностью $1/2$ получит $|+\rangle$ и состояние триплета будет $|\Psi^+\rangle \otimes |+\rangle$, или Боб получит $|-\rangle$ и состояние триплета будет $|\Psi^-\rangle \otimes |-\rangle$, где $|\Psi^+\rangle = \left(|00\rangle + |11\rangle\right)/\sqrt{2}$ и $|\Psi^-\rangle = \left(|00\rangle - |11\rangle\right)/\sqrt{2}$ – два из состояний Белла. Тогда после получения сообщения от Боба о выбранном базисе и результате измерения, Алиса измеряет два своих кубита в базисе Белла и в первом случае должна получить $|\Psi^+\rangle$, а во втором $|\Psi^-\rangle$. Если это не так, то протокол прерывается, иначе выполняется следующий цикл протокола.

2. Атака с использованием квантовых проб на пинг-понг протокол с ГХЦ-триплетами. Аналогично стратегии атаки на пинг-понг протокол с белловскими состояниями [1, 3] Ева должна сначала выполнить атакующую операцию $\hat{E}$, перепутывая свою пробу с передаваемыми фотонами на пути Боб $\rightarrow$ Алиса, а после выполнения Алисой одной из кодирующих операций (2) выполнить измерение над составной системой “передаваемые фотоны – проба” (рис. 3).

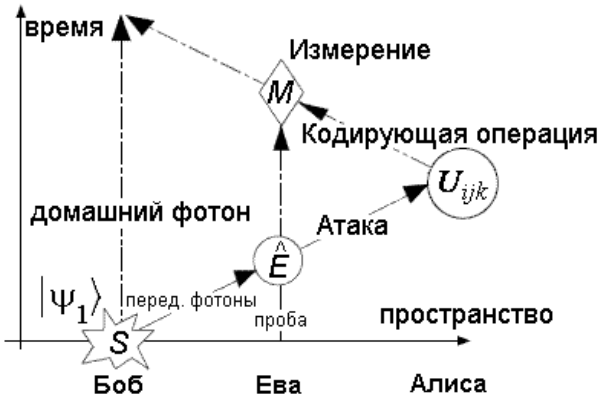

Рисунок 3 – Атака Евы

Кроме режима передачи сообщения, легитимные пользователи с определенной вероятностью q переключаются также в режим контроля подслушивания в квантовом канале. Однако Ева, прослушивая открытый обычный канал связи между ними, узнает о переключении в режим контроля подслушивания после выполнения атакующей операции $\hat{E}$, но до своего финального измерения, которое она в этом случае выполнять не будет. Таким образом, легитимные пользователи могут выявить только атакующую операцию $\hat{E}$.

Согласно теореме расширения [1], атакующая операция Евы $\hat{E}$ на линии Боб → Алиса может быть реализована унитарным оператором в гильбертовом пространстве проб H_E, размерность которого удовлетворяет условию $\dim H_E \le (\dim H_B)^2$, где H_B – размерность гильбертова пространства двух кубитов, пересылаемых от Боба к Алисе ($\dim H_B = 4$).

Состояние пересылаемой Бобом пары кубитов является полностью смешанным, его редуцированная матрица плотности $\rho_B = Tr_3(|\Psi_1\rangle\langle\Psi_1|) = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$, где индекс «3» у символа операции “частичный след” обозначает номер кубита, по которому берется след. Состояния первого и второго кубитов в пересылаемой паре также полностью смешаны. Так, для первого кубита $\rho_1 = Tr_2(\rho_B) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ и аналогично для второго $\rho_2 = Tr_1(\rho_B) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. Это соответствует ситуации, как если бы Боб посылал пару кубитов в одном из состояний $|00\rangle$, $|01\rangle$, $|10\rangle$ или $|11\rangle$.

Таким образом, состояния составной системы “передаваемые кубиты – проба Евы” после атаки могут быть записаны в виде:

$$
\begin{aligned}
|\psi^{(1)}\rangle &= \hat{E}|00,\varphi\rangle = \alpha_1|00,\varphi_{0000}\rangle + \beta_1|01,\varphi_{0001}\rangle + \gamma_1|10,\varphi_{0010}\rangle + \delta_1|11,\varphi_{0011}\rangle;\\
|\psi^{(2)}\rangle &= \hat{E}|01,\varphi\rangle = \alpha_2|00,\varphi_{0100}\rangle + \beta_2|01,\varphi_{0101}\rangle + \gamma_2|10,\varphi_{0110}\rangle + \delta_2|11,\varphi_{0111}\rangle;\\
|\psi^{(3)}\rangle &= \hat{E}|10,\varphi\rangle = \alpha_3|00,\varphi_{1000}\rangle + \beta_3|01,\varphi_{1001}\rangle + \gamma_3|10,\varphi_{1010}\rangle + \delta_3|11,\varphi_{1011}\rangle;\\
|\psi^{(4)}\rangle &= \hat{E}|11,\varphi\rangle = \alpha_4|00,\varphi_{1100}\rangle + \beta_4|01,\varphi_{1101}\rangle + \gamma_4|10,\varphi_{1110}\rangle + \delta_4|11,\varphi_{1111}\rangle,
\end{aligned}
\qquad (3)
$$

где $\{|\varphi_{ijkl}\rangle\}$ – множество состояний пробы Евы.

Матричное представление атакующей операции Евы имеет вид:

$$\hat{E} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \delta_1 & \delta_2 & \delta_3 & \delta_4 \end{pmatrix} \tag{4}$$

Из условия унитарности операции $\hat{E}$ следуют такие соотношения между параметрами пробы Евы:

$$\alpha_i^* \alpha_j + \beta_i^* \beta_j + \gamma_i^* \gamma_j + \delta_i^* \delta_j = \varepsilon_{ij}, \tag{5}$$

где ε_{ij} – символ Кронекера, $i = 1...4$, $j = 1...4$.

Также соблюдаются следующие соотношения:

$$\begin{aligned} &|\alpha_1|^2 = |\beta_2|^2 = |\gamma_3|^2 = |\delta_4|^2; \qquad |\alpha_2|^2 = |\beta_3|^2 = |\gamma_4|^2 = |\delta_1|^2; \\ &|\alpha_3|^2 = |\beta_4|^2 = |\gamma_1|^2 = |\delta_2|^2; \qquad |\alpha_4|^2 = |\beta_1|^2 = |\gamma_2|^2 = |\delta_3|^2. \end{aligned} \tag{6}$$

Рассмотрим случай, когда Боб посылает $|00\rangle$, т. е. состояние квантовой системы "передаваемые кубиты – проба Евы" после атаки $\hat{E}$ становится $|\psi^{(1)}\rangle$ (см. (3)). Остальные случаи в формуле (3) рассматриваются аналогично.

После выполнения Алисой кодирующих операций U_{000}, U_{001}, U_{010}, U_{011}, U_{100}, U_{101}, U_{110}, U_{111} (2) с частотами p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8 соответственно, оператор плотности системы "передаваемые кубиты – проба Евы" будет иметь вид:

$$\rho^{(1)} = \sum_{i=1}^{8} p_i |\psi_i^{(1)}\rangle\langle\psi_i^{(1)}|, \tag{7}$$

где

$$\begin{aligned}
|\psi_1^{(1)}\rangle &= U_{000}|\psi^{(1)}\rangle = \alpha_1|00,\varphi_{0000}\rangle + \beta_1|01,\varphi_{0001}\rangle + \gamma_1|10,\varphi_{0010}\rangle + \delta_1|11,\varphi_{0011}\rangle, \\
|\psi_2^{(1)}\rangle &= U_{001}|\psi^{(1)}\rangle = \alpha_1|00,\varphi_{0000}\rangle - \beta_1|01,\varphi_{0001}\rangle + \gamma_1|10,\varphi_{0010}\rangle - \delta_1|11,\varphi_{0011}\rangle, \\
|\psi_3^{(1)}\rangle &= U_{010}|\psi^{(1)}\rangle = \alpha_1|10,\varphi_{0000}\rangle + \beta_1|11,\varphi_{0001}\rangle + \gamma_1|00,\varphi_{0010}\rangle + \delta_1|01,\varphi_{0011}\rangle, \\
|\psi_4^{(1)}\rangle &= U_{011}|\psi^{(1)}\rangle = -\alpha_1|10,\varphi_{0000}\rangle - \beta_1|11,\varphi_{0001}\rangle + \gamma_1|00,\varphi_{0010}\rangle + \delta_1|01,\varphi_{0011}\rangle, \\
|\psi_5^{(1)}\rangle &= U_{100}|\psi^{(1)}\rangle = \alpha_1|01,\varphi_{0000}\rangle + \beta_1|00,\varphi_{0001}\rangle + \gamma_1|11,\varphi_{0010}\rangle + \delta_1|10,\varphi_{0011}\rangle, \\
|\psi_6^{(1)}\rangle &= U_{101}|\psi^{(1)}\rangle = -\alpha_1|01,\varphi_{0000}\rangle + \beta_1|00,\varphi_{0001}\rangle - \gamma_1|11,\varphi_{0010}\rangle + \delta_1|10,\varphi_{0011}\rangle, \\
|\psi_7^{(1)}\rangle &= U_{110}|\psi^{(1)}\rangle = \alpha_1|11,\varphi_{0000}\rangle + \beta_1|10,\varphi_{0001}\rangle + \gamma_1|01,\varphi_{0010}\rangle + \delta_1|00,\varphi_{0011}\rangle, \\
|\psi_8^{(1)}\rangle &= U_{111}|\psi^{(1)}\rangle = -\alpha_1|11,\varphi_{0000}\rangle - \beta_1|10,\varphi_{0001}\rangle + \gamma_1|01,\varphi_{0010}\rangle + \delta_1|00,\varphi_{0011}\rangle.
\end{aligned} \tag{8}$$

Подстановка формул (8) в (7) приводит к очень громоздкому выражению для оператора плотности и по этой причине полученное выражение для этого оператора здесь не приводится.

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

$$I_{\max} = S\left(\rho^{(1)}\right) \equiv -Tr\left\{\rho^{(1)}\log_2\rho^{(1)}\right\} = -\sum_{i=1}^{16}\lambda_i\log_2\lambda_i, \tag{9}$$

где λ_i – собственные значения оператора плотности $\rho^{(1)}$ (7). Величина $I_{\max}$ показывает, сколько информации может получить Ева после финального измерения над составной системой "передаваемые кубиты – проба".

Для нахождения собственных значений λ_i оператора плотности $\rho^{(1)}$ (7), этот оператор был записан в матричном виде в следующем ортогональном базисе:

$$\left\{\left|00,\varphi_{0000}\right\rangle, \left|01,\varphi_{0000}\right\rangle, \left|10,\varphi_{0000}\right\rangle, \left|11,\varphi_{0000}\right\rangle, \left|00,\varphi_{0001}\right\rangle, \left|01,\varphi_{0001}\right\rangle, \left|10,\varphi_{0001}\right\rangle, \left|11,\varphi_{0001}\right\rangle,\right.$$
$$\left.\left|00,\varphi_{0010}\right\rangle, \left|01,\varphi_{0010}\right\rangle, \left|10,\varphi_{0010}\right\rangle, \left|11,\varphi_{0010}\right\rangle, \left|00,\varphi_{0011}\right\rangle, \left|01,\varphi_{0011}\right\rangle, \left|10,\varphi_{0011}\right\rangle, \left|11,\varphi_{0011}\right\rangle\right\}. \tag{10}$$

Полученная матрица имеет размер 16×16 и здесь не приводится ввиду ее громоздкости. Собственные значения матрицы плотности $\rho^{(1)}$ были найдены с использованием инструментария символьных вычислений программы Mathematica 6:

$$\lambda_{1,2} = \frac{1}{2}(p_1+p_2) \pm \frac{1}{2}\sqrt{(p_1+p_2)^2 - 16p_1p_2\left(|\alpha_1|^2+|\gamma_1|^2\right)\left(|\beta_1|^2+|\delta_1|^2\right)};$$

$$\lambda_{3,4} = \frac{1}{2}(p_3+p_4) \pm \frac{1}{2}\sqrt{(p_3+p_4)^2 - 16p_3p_4\left(|\alpha_1|^2+|\beta_1|^2\right)\left(|\gamma_1|^2+|\delta_1|^2\right)};$$

$$\lambda_{5,6} = \frac{1}{2}(p_5+p_6) \pm \frac{1}{2}\sqrt{(p_5+p_6)^2 - 16p_5p_6\left(|\alpha_1|^2+|\gamma_1|^2\right)\left(|\beta_1|^2+|\delta_1|^2\right)}; \tag{11}$$

$$\lambda_{7,8} = \frac{1}{2}(p_7+p_8) \pm \frac{1}{2}\sqrt{(p_7+p_8)^2 - 16p_7p_8\left(|\alpha_1|^2+|\beta_1|^2\right)\left(|\gamma_1|^2+|\delta_1|^2\right)}.$$

Остальные восемь собственных значений матрицы плотности $\rho^{(1)}$ равны нулю.

Таким образом, максимальная информация Евы

$$I_{\max} = -\sum_{i=1}^{8}\lambda_i\log_2\lambda_i, \tag{12}$$

где λ_i определены в (11).

Аналогичным образом рассматриваются остальные случаи в (3), т. е. когда Боб вместо $\left|00\right\rangle$ посылает $\left|01\right\rangle$, $\left|10\right\rangle$ или $\left|11\right\rangle$. Для $\left|10\right\rangle$ собственные значения матрицы плотности совпадают с формулами (11), а для $\left|01\right\rangle$ и $\left|11\right\rangle$ имеют вид (с учетом соотношений (6)):

$$\lambda_{1,2} = \frac{1}{2}(p_1+p_2) \pm \frac{1}{2}\sqrt{(p_1+p_2)^2 - 16p_1p_2\left(|\alpha_1|^2+|\gamma_1|^2\right)\left(|\beta_1|^2+|\delta_1|^2\right)};$$

$$\lambda_{3,4} = \frac{1}{2}(p_3+p_4) \pm \frac{1}{2}\sqrt{(p_3+p_4)^2 - 16p_3p_4\left(|\alpha_1|^2+|\delta_1|^2\right)\left(|\beta_1|^2+|\gamma_1|^2\right)};$$

$$\lambda_{5,6} = \frac{1}{2}(p_5+p_6) \pm \frac{1}{2}\sqrt{(p_5+p_6)^2 - 16p_5p_6\left(|\alpha_1|^2+|\gamma_1|^2\right)\left(|\beta_1|^2+|\delta_1|^2\right)}; \tag{13}$$

$$\lambda_{7,8} = \frac{1}{2}(p_7+p_8) \pm \frac{1}{2}\sqrt{(p_7+p_8)^2 - 16p_7p_8\left(|\alpha_1|^2+|\delta_1|^2\right)\left(|\gamma_1|^2+|\beta_1|^2\right)}.$$

3. Анализ стратегии атаки Евы, оценка безопасности протокола. При использовании в режиме контроля подслушивания двух измерительных базисов – B_z и B_x, вероятность обнаружить атакующую операцию $\hat{E}$ Евы

$$d = q_z d_z + q_x d_x, \tag{14}$$

где q_z и q_x – вероятности использования Алисой и Бобом базисов B_z и B_x соответственно ($q_z + q_x = 1$); d_z и d_x – вероятности обнаружения атаки Евы при измерениях в базисах B_z и B_x соответственно.

Оптимальная стратегия для Евы, т. е. выбор оптимальных параметров атакующей операции α_1, β_1, γ_1 и δ_1 в (4) (остальные параметры получаются из (6)), зависит от стратегии контроля подслушивания, которую выбирает Алиса, т. е. от ее выбора q_z и q_x. Ева не знает заранее, какие значения q_z и q_x выбрала Алиса, но Ева может оценить эти величины в процессе реализации протокола, прослушивая незащищенный обычный канал между Алисой и Бобом, когда они обмениваются информацией в режиме контроля подслушивания. Тогда Ева может изменить стратегию своей атаки соответствующим образом. Однако, чтобы оценить q_z и q_x, Еве необходимо получить информацию хотя бы о нескольких сеансах контроля подслушивания. Поэтому оптимальной стратегией для Алисы будет изменение q_z и q_x через каждые несколько сеансов так, чтобы Ева не успевала приспособить свою атаку к их новым значениям.

В качестве примера выбора Евой параметров α_1, β_1, γ_1 и δ_1 рассмотрим случай, когда Алисы выбрала $q_z = q_x = 1/2$. Тогда для Евы, задача которой состоит в минимизации величины d (14), оптимальным выбором будет $d_x = d_z$. Далее Ева должна выбрать желаемую величину d_z (при этом чем меньше будет d_z, тем меньше будет информация $I_{\max}$ Евы согласно (11)… (13)) и, наконец, значения α_1, β_1, γ_1 и δ_1 так, чтобы они удовлетворяли выражениям (5) и одновременно выполнялось соотношение $d_x = d_z$.

Как следует из первого выражения в (3), в случае, когда Боб посылает $|00\rangle$

$$d_z = |\beta_1|^2 + |\gamma_1|^2 + |\delta_1|^2 = 1 - |\alpha_1|^2. \tag{15}$$

Аналогично, если Боб посылает $|01\rangle$, то

$$d_z = |\alpha_2|^2 + |\gamma_2|^2 + |\delta_2|^2 = 1 - |\beta_2|^2 = |\beta_1|^2 + |\gamma_1|^2 + |\delta_1|^2 = 1 - |\alpha_1|^2, \tag{16}$$

где для получения последних двух равенств использованы выражения (6). То же самое выражение для d_z получается и когда Боб шлет $|10\rangle$ и $|11\rangle$, как следует из (3) и (6). Таким образом, общее выражение для вероятности обнаружения атаки при использовании в режиме контроля подслушивания измерительного базиса B_z имеет вид (15).

Выражение для d_x может быть получено аналогично тому, как выше получено выражение для d_z. В силу того, что состояние пересылаемой Бобом пары кубитов полностью смешанное, теперь можно считать, что Боб посылает пару кубитов в одном из состояний $|++\rangle$, $|+-\rangle$, $|-+\rangle$, или $|--\rangle$. Тогда формулы (3) заменяются на следующие:

$$\begin{aligned}
|\psi^{(1)}\rangle &= \hat{E}|++,\varphi\rangle = a_1|++,\varphi_{++++}\rangle + b_1|+-,\varphi_{+++-}\rangle + c_1|-+,\varphi_{++-+}\rangle + d_1|--,\varphi_{++--}\rangle;\\
|\psi^{(2)}\rangle &= \hat{E}|+-,\varphi\rangle = a_2|++,\varphi_{+-++}\rangle + b_2|+-,\varphi_{+-+-}\rangle + c_2|-+,\varphi_{+--+}\rangle + d_2|--,\varphi_{+---}\rangle;\\
|\psi^{(3)}\rangle &= \hat{E}|-+,\varphi\rangle = a_3|++,\varphi_{-+++}\rangle + b_3|+-,\varphi_{-++-}\rangle + c_3|-+,\varphi_{-+-+}\rangle + d_3|--,\varphi_{-+--}\rangle;
\end{aligned} \tag{17}$$

$$\left|\psi^{(4)}\right\rangle = \hat{E}\left|--,\varphi\right\rangle = a_4\left|++,\varphi_{--++}\right\rangle + b_4\left|+-,\varphi_{--+-}\right\rangle + c_4\left|-+,\varphi_{---+}\right\rangle + d_4\left|--,\varphi_{----}\right\rangle .$$

Далее, все формулы (4)…(13) остаются справедливыми при замене $\alpha_1 \to a_1$, $\beta_1 \to b_1$, $\gamma_1 \to c_1$, $\delta_1 \to d_1$ и т. д. Таким образом, выражение (15) переходит в выражение

$$d_x = |b_1|^2 + |c_1|^2 + |d_1|^2 = 1 - |a_1|^2 . \qquad (18)$$

Используя (3) и (17), можно получить следующие выражения, связывающие параметры α_1, β_1, γ_1 и δ_1 с параметрами a_1, b_1, c_1 и d_1:

$$\alpha_1 = (a_1 + b_1 + c_1 + d_1)/2, \quad \beta_1 = (a_1 - b_1 + c_1 - d_1)/2,$$
$$\gamma_1 = (a_1 + b_1 - c_1 - d_1)/2, \quad \delta_1 = (a_1 - b_1 - c_1 + d_1)/2. \qquad (19)$$

Используя теперь условие оптимальности атаки Евы $d_x = d_z$ (при выборе Алисы $q_z = q_x = 1/2$) и учитывая все вышеприведенные соотношения для α_1, β_1, γ_1, δ_1, a_1, b_1, c_1, d_1, можно получить различные допустимые наборы параметров атакующей операции Евы.

Приведем, как пример, два таких набора:

1) $d_x = d_z = 1/4$; $\alpha_1 = \sqrt{3}/2$; $\beta_1 = \gamma_1 = \delta_1 = 1/(2\sqrt{3})$; $I_{\max} = 2{,}65$;

2) $d_x = d_z = 3/4$; $\alpha_1 = 1/2$; $\beta_1 = \gamma_1 = 1/2$; $\delta_1 = -1/2$; $I_{\max} = 3$,

где $I_{\max}$ получено по формулам (11), (12) при $p_1 = p_2 = ... = p_8 = 1/8$.

На рис. 4 приведены зависимости от d_z максимального количества информации $I_{\max}$ Евы при $|\alpha_1|^2 = 1 - d_z$, $|\beta_1|^2 = |\gamma_1|^2 = |\delta_1|^2 = d_z/3$ и различных значениях частот $p_1 \dots p_8$ кодирующих операций Алисы (2). В этом случае выражения для собственных значений (11) матрицы плотности (7) принимают вид:

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16p_1p_2 \cdot \frac{2}{3}d_z\left(1 - \frac{2}{3}d_z\right)};$$

$$\lambda_{3,4} = \frac{1}{2}(p_3 + p_4) \pm \frac{1}{2}\sqrt{(p_3 + p_4)^2 - 16p_3p_4 \cdot \frac{2}{3}d_z\left(1 - \frac{2}{3}d_z\right)};$$

$$\lambda_{5,6} = \frac{1}{2}(p_5 + p_6) \pm \frac{1}{2}\sqrt{(p_5 + p_6)^2 - 16p_5p_6 \cdot \frac{2}{3}d_z\left(1 - \frac{2}{3}d_z\right)}; \qquad (20)$$

$$\lambda_{7,8} = \frac{1}{2}(p_7 + p_8) \pm \frac{1}{2}\sqrt{(p_7 + p_8)^2 - 16p_7p_8 \cdot \frac{2}{3}d_z\left(1 - \frac{2}{3}d_z\right)}.$$

Значения частот $p_1 ... p_8$ кодирующих операций Алисы, а также энтропия $H = -\sum_{i=1}^{8} p_i \log_2 p_i$ двоичного кода для кривых 1…5 на рис. 4 приведены в табл. 1.

Таблица 1 – Частоты триграмм $p_1 \dots p_8$ и энтропия H (бит/триграмма) двоичного кода

№ кривой на рис. 4	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	H
1	0,125	0,125	0,125	0,125	0,125	0,125	0,125	0,125	3,00
2	0,25	0,25	0,25	0,25	0	0	0	0	2,00
3	0,4	0,1	0	0	0,4	0,1	0	0	1,72
4	0,5	0	0	0	0	0	0	0,5	1,00
5	0,9	0,1	0	0	0	0	0	0	0,47

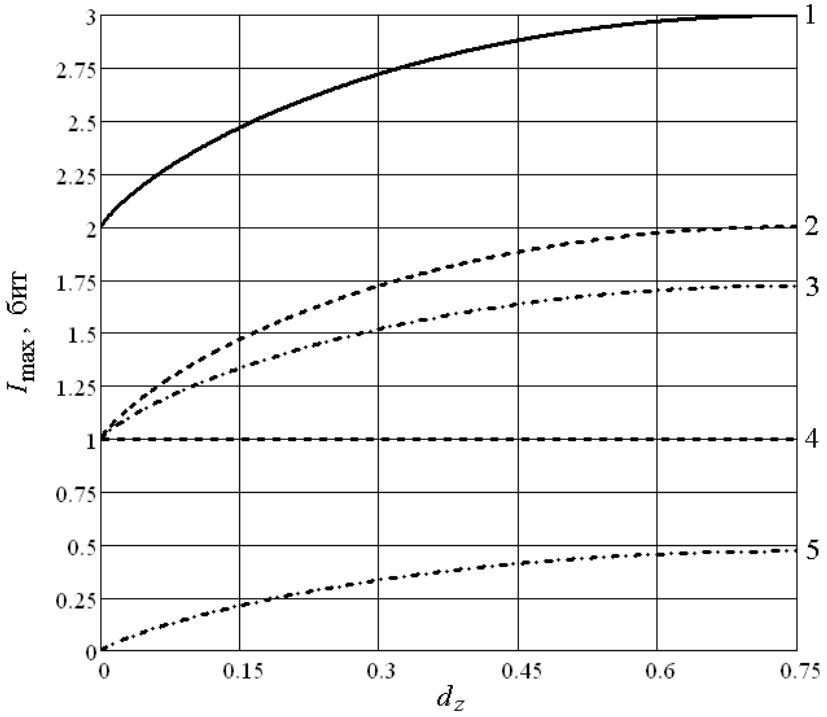

Рисунок 4 – Зависимость максимальной информации Евы $I_{\max}$ (12) от вероятности d_z обнаружения атаки при измерениях в базисе B_z

Как видно из рис. 4, количество информации, которую может получить Ева, ограничено энтропией источника, т. е. энтропией передаваемого Алисой двоичного кода, как и должно быть. Значения $I_{\max}$ при d_z = 0,75 равны соответствующей энтропии источника (см. рис. 4), так как при таком значении d_z Ева может получить полную информацию, выполняя свое измерение над системой "передаваемые фотоны – проба". При этом, так как более низкая энтропия источника означает наличие определенной априорной информации об источнике (о распределении частот $p_1 \ldots p_8$ кодирующих операций Алисы), которой у Евы может и не быть (например, Ева не знает, какую кодировку текста использует Алиса), то понижение энтропии источника могло бы быть способом повышения безопасности протокола. Так, чтобы определить кодировку Алисы, Еве необходимо перехватить, по крайней мере, десяток бит, а полная вероятность ее обнаружения растет экспоненциально с ростом перехваченной ею информации [1, 5]. Подчеркнем, что здесь имеется принципиальное отличие от шифртекста, передаваемого по обычному каналу связи, который подслушивающий агент может полностью перехватить, оставшись незамеченным, и затем анализировать. В таком случае, чем ниже будет энтропия шифртекста, тем, конечно, задача его криптоанализа будет легче. В случае же пинг-понг протокола полная вероятность обнаружения подслушивания растет экспоненциально с увеличением количества переданных по квантовому каналу бит [1, 5], поэтому введение в сообщение дополнительных, не несущих информации бит может ускорить обнаружение подслушивания без увеличения информации Евы. Однако Ева может и обладать некоторой априорной информацией, т. е. информацией о распределении частот $p_1 \ldots p_8$. Например, Ева точно знает, что текстовое сообщение передается в 16-битной кодировке Unicode и что это сообщение на английском языке, тогда первые 8 бит каждого символа являются нулями и Ева может просто пропускать передачу этих бит, не выполняя атаки. В таком случае как полезная информация Евы, извлекаемая при измерении, так и полная вероятность ее обнаружения уже никак не будут зависеть от энтропии источника. Таким образом, понижение энтропии источника может повысить безопасность пинг-понг протокола с ГХЦ-триплетами только при отсутствии у Евы какой-либо априорной информации об источнике, а так как легитимные пользователи не могут гарантировать этого в общем случае, то такой способ повышения безопасности протокола нельзя считать удовлетворительным. Отметим, что для пинг-понг протокола с белловскими парами и квантовым плотным кодированием зависимость информации Евы от энтропии источника такая же

[3, 6], но искусственное понижение энтропии источника также не может быть способом повышения безопасности этого варианта протокола по тем же причинам, что и для протокола с ГХЦ-триплетами.

Для протокола с ГХЦ-триплетами, как и для протокола с белловскими парами, существует невидимый режим подслушивания ($d_z = 0$), когда легитимные пользователи используют в режиме контроля подслушивания только один измерительный базис B_z. При этом для случая равномерного распределения частот кодирующих операций Алисы в протоколе с белловскими парами Ева может получить 1 бит информации на двоичную биграмму, т. е. 50% информации [3, 6]. Для протокола с ГХЦ-триплетами Ева получит 2 бита на триграмму, т. е. ≈ 66,7% информации (см. кривую 1 на рис. 4 при $d_z = 0$). Следовательно, легитимные пользователи должны либо обязательно использовать два измерительных базиса в режиме контроля подслушивания (для протокола с ГХЦ-триплетами $d_x = 0{,}75$ при $d_z = 0$ и наоборот), либо использовать определенные классические криптографические методы для повышения безопасности протокола, например метод, предложенный в [6].

В заключение отметим следующее. В работе проанализирована атака с использованием квантовых проб на пинг-понг протокол с ГХЦ-триплетами. Показано, что при использовании легитимными пользователями в режиме контроля подслушивания двух измерительных базисов (B_z и B_x) протокол является квазибезопасным, аналогично пинг-понг протоколу с белловскими парами. При этом, если подслушивающий агент хочет получить полную информацию, то вероятность его обнаружения при измерениях в одном из базисов равна 75% (для протокола с белловскими парами – 50% [3]). Таким образом, увеличение числа перепутанных кубитов, используемых для реализации протокола, позволяет увеличить не только эффективность протокола, но и повысить уровень его безопасности.

В работе показано также, что при использовании в режиме контроля подслушивания только одного измерительного базиса существует невидимый режим подслушивания, при котором подслушивающий агент может получить до 66,7% информации, вообще не будучи обнаруженным. Следовательно, легитимные пользователи должны либо использовать два измерительных базиса, либо определенные методы классической криптографии для повышения безопасности протокола.

Литература

1. *Boström K., Felbinger T.* Deterministic secure direct communication using entanglement // Physical Review Letters. – 2002. – Vol. 89. – № 18. – Art. 187902.
2. *Cai Q.-Y., Li B.-W.* Improving the capacity of the Boström-Felbinger protocol // Physical Review A. – 2004. – V. 69. – № 5. – Art. 054301.
3. *Василиу Е.В*. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32 – 38.
4. *Василиу Е.В.* Пинг-понг протокол квантовой безопасной связи с триплетами Гринбергера – Хорна – Цайлингера // Materialy IV miedzynarodowej naukowi-praktycznej konferencji «Strategiczne pytania swiatowej nauki – 2008», 15 – 28 lutego 2008 roku. – Przemysl, «Nauka i studia». – Т. 10. – С. 40 – 44.
5. *Василиу Е.В., Василиу Л.Н.* Оценка количества информации, попадающей к злоумышленнику, для трех вариантов пинг-понг протокола квантовой безопасной связи // Материали за IV международна научна практична конференция «Научно пространство на Европа – 2008», 15 – 30 април 2008 г. – София, «Бял ГРАД-БГ» ООД. – Т. 29. – С. 34 – 40.
6. *Василиу Е.В*. Безопасность пинг-понг протокола квантовой связи для передачи текстовых сообщений // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 2. – С. 36 – 44.