УДК 003.26:621.39+530.145

Асимптотическая безопасность пинг – понг протокола квантовой прямой связи с трех-кубитными состояниями Гринбергера – Хорна – Цайлингера

Василиу Е.В.
Одесская национальная академия связи им. А.С. Попова,
65029, ул. Кузнечная 1, Одесса, Украина
vasiliu@te.net.ua

Аннотация

На основе методов квантовой теории информации проанализирована атака с использованием вспомогательных квантовых систем на пинг – понг протокол с триплетами Гринбергера – Хорна – Цайлингера и квантовым сверхплотным кодированием. Показано, что при использовании легитимными пользователями в режиме контроля подслушивания двух измерительных базисов протокол является асимптотически безопасным, аналогично пинг – понг протоколу с белловскими парами. Проведен сравнительный анализ асимптотической безопасности трех вариантов пинг – понг протокола. Показано, что при выборе стратегии атаки, которая дает подслушивающему агенту полную информацию, протокол с белловскими парами и сверхплотным кодированием и протокол с ГХЦ – триплетами имеют практически одинаковую стойкость к такой атаке. Предложен способ усиления безопасности пинг – понг протокола, состоящий в обратимом хешировании блоков сообщения.

Ключевые слова*: квантовая криптография, пинг – понг протокол, ГХЦ – состояния, квантовое сверхплотное кодирование, атака на протокол, асимптотическая безопасность, усиление безопасности.*

1. Введение

Квантовая теория информации – новое междисциплинарное направление, возникшее на стыке квантовой механики, теории информации и теории вычислений, интенсивно развивается в последние два десятилетия [1]. Одним из прикладных направлений этой новой теории является квантовая криптография – методы защиты информации, в которых используются протоколы, основанные на фундаментальных законах квантовой механики. Так, квантовые протоколы распределения ключей обеспечивают безопасный способ создания секретного ключа, используя который две авторизованные стороны, Алиса и Боб, могут затем обмениваться секретными сообщениями с использованием известных алгоритмов классической криптографии [1]. Недавно была предложена новая концепция квантовой криптографии, получившая название квантовой безопасной прямой связи (КБПС) [2]. В протоколах КБПС секретный ключ вообще не используется, а его роль играет статический квантовомеханический ресурс – совместно используемые авторизованными пользователями группы перепутанных квантовых частиц, например, пары Эйнштейна – Подольского – Розена или триплеты Гринбергера – Хорна – Цайлингера (ГХЦ). Секретное сообщение, закодированное с помощью квантовых состояний таких групп кубитов, передается непосредственно через квантовый канал связи. При этом законы квантовой механики гарантируют обнаружение подслушивание в канале, для чего легитимные стороны должны выполнить определенную последовательность квантовых измерений над некоторой частью переданных кубитов. Обнаружив подслушивающего агента, Еву, Алиса и Боб прекращают передачу сообщения.

Одним из протоколов КБПС является пинг – понг протокол, в котором в качестве кубитов используется пара фотонов, максимально перепутанных по их поляризационным степеням свободы – состояния Белла [2]. Информация кодируется фазой перепутанных кубитов. Так как только один кубит передается от Боба к Алисе (пинг), а затем назад от Алисы к Бобу (понг), закодированная информация не может быть извлечена измерением состояния этого одного кубита. Декодирование становится возможным только при выполнении измерения в базисе Белла над обоими кубитами, что позволяет определить корреляцию кубитов друг с другом.

Однако, используя вспомогательные квантовые системы (пробы) и выполняя соответствующие унитарные операции и последующие измерения над составными (фотоны – пробы) квантовыми системами, Ева имеет возможность перехватить некоторую часть сообщения [2]. Поэтому в пинг – понг протоколе предусмотрен специальный режим контроля подслушивания, используя который Алиса и Боб обнаруживают операции Евы [2 – 4].

Отметим, что недавно этот первоначальный вариант пинг – понг протокола был реализован на экспериментальном оборудовании [5]. При этом демонстрация работы протокола была выполнена не путем непосредственной передачи сообщения по квантовому каналу, а путем передачи по такому каналу случайного двоичного ключа длиной 10000 бит (разумеется, пинг – понг протокол можно использовать и в качестве квантового протокола распределения ключей). Скорость передачи достигала 4250 бит/с, а уровень ошибок составил 3,8%, что можно считать вполне приемлемыми значениями для практического использования протоколов квантовой криптографии.

В первоначальном варианте пинг – понг протокола каждый передаваемый кубит (один из перепутанной пары) используется для кодирования одного классического бита. Возможно увеличить информационную емкость канала путем использования квантового сверхплотного кодирования, в этом случае с помощью одного кубита можно передать два бита информации [3, 4]. Дальнейшее увеличение информационной емкости предполагает использование вместо перепутанных пар кубитов их троек, четверок и т.д. Один из протоколов с передачей пакетов полностью перепутанных триплетов кубитов, так называемый многошаговый протокол КБПС, предложен в [6]. Другой протокол с использованием ГХЦ – триплетов, позволяющий секретно передать сообщение от Алисы к Бобу под контролем третьей доверенной стороны, предложен в [7]. Достоинством этих протоколов является высокий уровень стойкости к атакам, а недостатком – необходимость наличия квантовой памяти большого объема для хранения состояний пакетов кубитов до завершения всего протокола. В отличие от таких протоколов, для пинг – понг протокола требуется хранить лишь состояние одного кубита (у Боба) в течение одного цикла протокола. Поэтому с точки зрения практической реализации пинг – понг протокол обладает несомненным преимуществом перед протоколами с пересылкой больших пакетов кубитов. Однако пинг – понг протокол является асимптотически безопасным, т.е. любая эффективная атака Евы будет обнаружена, но прежде она сможет получить некоторую небольшую часть сообщения [2 – 4]. Тем не менее безопасность пинг – понг протокола может быть усилена с использованием методов классической криптографии [8]. Поэтому значительный интерес представляет разработка вариантов пинг – понг протокола с использованием перепутанных состояний трех и большего числа кубитов, которые, с одной стороны, обладают значительной информационной емкостью, а, с другой стороны, легче реализуемы технически, чем протоколы, предложенные в [6, 7].

Схема пинг – понг протокола с использованием ГЦХ – триплетов и квантового сверхплотного кодирования, разработанная на основе оригинальной версии протокола [2] и многошагового протокола [6], предложена в [9]. Эта схема кратко изложена в следующем разделе статьи. Целью настоящей работы является разработка метода усиления секретности пинг – понг протокола с ГХЦ – триплетами, для чего необходимо сначала проанализировать атаку подслушивающего агента на этот протокол.

2. Пинг – понг протокол с ГХЦ – триплетами

Имеется восемь полностью перепутанных ортогональных трехкубитных ГХЦ – состояний:

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

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

где $\left|0\right\rangle$ и $\left|1\right\rangle$ – базисные состояния одного кубита.

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

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

Кодирующие операции Алисы, построенные таким образом, чтобы они содержали минимально возможное количество нетождественных операций, имеют вид [7]:

$$U_{000} = I \otimes I;\ U_{001} = I \otimes \sigma_z;\ U_{010} = \sigma_x \otimes I;\ U_{011} = i\sigma_y \otimes I;$$

$$U_{100} = I \otimes \sigma_x;\ U_{101} = I \otimes i\sigma_y;\ U_{110} = \sigma_x \otimes \sigma_x;\ U_{111} = i\sigma_y \otimes \sigma_x \qquad (2)$$

и соответствуют следующим трехбитовым комбинациям: «000», «001», «010», «011», «100», «101», «110» и «111». В (2) использованы следующие обозначения:

$I = \left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|$ – тождественный оператор; $\sigma_x = \left|0\right\rangle\left\langle 1\right| + \left|1\right\rangle\left\langle 0\right|$, $\sigma_y = -i\left|0\right\rangle\left\langle 1\right| + i\left|1\right\rangle\left\langle 0\right|$ и $\sigma_z = \left|0\right\rangle\left\langle 0\right| - \left|1\right\rangle\left\langle 1\right|$ – операторы Паули.

Получив два кубита обратно от Алисы, Боб выполняет измерение над всеми тремя кубитами в ГХЦ – базисе и тем самым достоверно определяет трехбитовую строку, которую она послала.

В режиме контроля подслушивания Алиса сначала сообщает Бобу по обычному (не квантовому) каналу связи о переключении в этот режим. Отметим, что нет необходимости полностью защищать этот канал, он может быть открыт, но только для пассивного прослушивания. Перед началом протокола Алиса и Боб должны аутентифицировать друг друга, иначе весь протокол становится уязвимым к атаке "человек в середине". Таким образом, Ева не должна иметь возможности изменять сообщения, передаваемые по обычному каналу. Получив сообщение от Алисы, Боб случайным образом выбирает один из двух измерительных базисов: $B_z = \left\{\left|0\right\rangle\left\langle 0\right|; \left|1\right\rangle\left\langle 1\right|\right\}$ или $B_x = \left\{\left|+\right\rangle\left\langle +\right|; \left|-\right\rangle\left\langle -\right|\right\}$, где $\left|+\right\rangle = \left(\left|0\right\rangle + \left|1\right\rangle\right)/\sqrt{2}$ и $\left|-\right\rangle = \left(\left|0\right\rangle - \left|1\right\rangle\right)/\sqrt{2}$, а затем выполняет измерение состояния своего “домашнего” фотона в выбранном базисе.

В результате измерения в базисе B_z Боб получит $\left|0\right\rangle$ с вероятностью $1/2$, а состояние триплета после измерения будет $\left|000\right\rangle$. 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 $\left|0\right\rangle$, $\left|0\right\rangle$. С вероятностью $1/2$ Боб получит $\left|1\right\rangle$ и состояние триплета будет $\left|111\right\rangle$. Тогда Алиса, выполнив измерения в том же базисе, должна получить $\left|1\right\rangle$, $\left|1\right\rangle$. 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 приготавливает 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 $|\Psi^+\rangle=(|00\rangle+|11\rangle)/\sqrt{2}$ и $|\Psi^-\rangle=(|00\rangle-|11\rangle)/\sqrt{2}$ – 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.

3. Атака на пинг – понг протокол с ГХЦ – триплетами

Аналогично стратегии атаки на пинг – понг протокол с белловскими состояниями [2, 4] 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".

Кроме режима передачи сообщения, легитимные пользователи с определенной вероятностью q переключаются также в режим контроля подслушивания в квантовом канале. 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 $\rightarrow$ 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 неотличимо для Евы от полностью смешанного, так как 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 $\rho_2 = Tr_1(\rho_B)=\frac{1}{2}|0\rangle\langle 0|+\frac{1}{2}|1\rangle\langle 1|$. Таким образом, аналогично случаю атаки на оригинальный пинг – понг протокол [2], можно заменить состояние пересылаемой пары кубитов на априорное смешанное состояние, что в данном случае соответствует ситуации, как если бы Боб посылал пару кубитов в одном из состояний $|00\rangle$, $|01\rangle$, $|10\rangle$, или $|11\rangle$ с одинаковой вероятностью $p=1/4$.

Следовательно, 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 $\left\{\left|\varphi_{ijkl}\right\rangle\right\}$ – 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:

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

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

После выполнения Алисой кодирующих операций U_{000}, …, U_{111} (2) с частотами p_1, …, p_8 соответственно, оператор плотности системы “передаваемые кубиты – проба Евы” будет иметь вид:

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

где

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

Максимальная классическая информация $I_{\max}$, которая доступна Еве после измерения над составной системой “передаваемые кубиты – проба”, определяется энтропией Холево [1]:

$$I_{\max}=S\left(\rho^{(1)}\right)-\sum_i p_i S\left(\rho_i^{(1)}\right)=S\left(\rho^{(1)}\right), \tag{9}$$

где $\rho_i^{(1)}=\left|\psi_i^{(1)}\right\rangle\left\langle\psi_i^{(1)}\right|$; S – энтропия фон Неймана и все $S\left(\rho_i^{(1)}\right)$ равны нулю, так как состояния (8) при выполнении условий (5) – чистые. Таким образом,

$$I_{\max}=S\left(\rho^{(1)}\right)\equiv -Tr\left\{\rho^{(1)}\log_2\rho^{(1)}\right\}=-\sum_i\lambda_i\log_2\lambda_i, \tag{10}$$

где λ_i – собственные значения оператора плотности $\rho^{(1)}$ (7).

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

$$\{|00,\varphi_{0000}\rangle,\ |01,\varphi_{0000}\rangle,|10,\varphi_{0000}\rangle,|11,\varphi_{0000}\rangle,|00,\varphi_{0001}\rangle,|01,\varphi_{0001}\rangle,|10,\varphi_{0001}\rangle,|11,\varphi_{0001}\rangle,$$
$$|00,\varphi_{0010}\rangle,\ |01,\varphi_{0010}\rangle,|10,\varphi_{0010}\rangle,|11,\varphi_{0010}\rangle,|00,\varphi_{0011}\rangle,|01,\varphi_{0011}\rangle,|10,\varphi_{0011}\rangle,|11,\varphi_{0011}\rangle\}. \quad (11)$$

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:

$$\lambda_{1,2}=\frac{1}{2}(p_1+p_2)\pm\frac{1}{2}\sqrt{(p_1+p_2)^2-16p_1p_2\left(|\alpha_1|^2+|\gamma_1|^2\right)\left(|\beta_1|^2+|\delta_1|^2\right)};$$
$$\lambda_{3,4}=\frac{1}{2}(p_3+p_4)\pm\frac{1}{2}\sqrt{(p_3+p_4)^2-16p_3p_4\left(|\alpha_1|^2+|\beta_1|^2\right)\left(|\gamma_1|^2+|\delta_1|^2\right)};$$
$$\lambda_{5,6}=\frac{1}{2}(p_5+p_6)\pm\frac{1}{2}\sqrt{(p_5+p_6)^2-16p_5p_6\left(|\alpha_1|^2+|\gamma_1|^2\right)\left(|\beta_1|^2+|\delta_1|^2\right)};$$
$$\lambda_{7,8}=\frac{1}{2}(p_7+p_8)\pm\frac{1}{2}\sqrt{(p_7+p_8)^2-16p_7p_8\left(|\alpha_1|^2+|\beta_1|^2\right)\left(|\gamma_1|^2+|\delta_1|^2\right)}. \quad (12)$$

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

Таким образом, максимальная информация Евы

$$I_{\max}=-\sum_{i=1}^{8}\lambda_i\log_2\lambda_i\,, \quad (13)$$

где λ_i определены в (12).

Аналогичным образом рассматриваются остальные случаи в (3), т. е. когда Боб вместо $|00\rangle$ посылает $|01\rangle$, $|10\rangle$, или $|11\rangle$. Для $|10\rangle$ собственные значения матрицы плотности совпадают с (12), а для $|01\rangle$ и $|11\rangle$ имеют вид (с учетом соотношений (6)):

$$\lambda_{1,2}=\frac{1}{2}(p_1+p_2)\pm\frac{1}{2}\sqrt{(p_1+p_2)^2-16p_1p_2\left(|\alpha_1|^2+|\gamma_1|^2\right)\left(|\beta_1|^2+|\delta_1|^2\right)};$$
$$\lambda_{3,4}=\frac{1}{2}(p_3+p_4)\pm\frac{1}{2}\sqrt{(p_3+p_4)^2-16p_3p_4\left(|\alpha_1|^2+|\delta_1|^2\right)\left(|\beta_1|^2+|\gamma_1|^2\right)};$$
$$\lambda_{5,6}=\frac{1}{2}(p_5+p_6)\pm\frac{1}{2}\sqrt{(p_5+p_6)^2-16p_5p_6\left(|\alpha_1|^2+|\gamma_1|^2\right)\left(|\beta_1|^2+|\delta_1|^2\right)};$$
$$\lambda_{7,8}=\frac{1}{2}(p_7+p_8)\pm\frac{1}{2}\sqrt{(p_7+p_8)^2-16p_7p_8\left(|\alpha_1|^2+|\delta_1|^2\right)\left(|\gamma_1|^2+|\beta_1|^2\right)}. \quad (14)$$

4. Анализ стратегии атаки и оценка количества информации, утекающей к Еве

При использовании в режиме контроля подслушивания двух измерительных базисов – B_z и B_x, вероятность обнаружить атакующую операцию $\hat{E}$ Евы

$$d=q_zd_z+q_xd_x\,, \quad (15)$$

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 открытый 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 (15), 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 (12) – (14)) и, наконец, значения α_1, β_1, γ_1 и δ_1 так, чтобы они удовлетворяли соотношениям (5) и одновременно выполнялось соотношение $d_x = d_z$.

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

$$d_z = |\beta_1|^2 + |\gamma_1|^2 + |\delta_1|^2 = 1 - |\alpha_1|^2 . \tag{16}$$

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

$$d_z = |\alpha_2|^2 + |\gamma_2|^2 + |\delta_2|^2 = 1 - |\beta_2|^2 = |\beta_1|^2 + |\gamma_1|^2 + |\delta_1|^2 = 1 - |\alpha_1|^2 , \tag{17}$$

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 (16).

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:

$$\begin{aligned}
|\psi^{(1)}\rangle &= \hat{E}|++,\varphi\rangle = a_1|++,\varphi_{++++}\rangle + b_1|+-,\varphi_{+++-}\rangle + c_1|-+,\varphi_{++-+}\rangle + d_1|--,\varphi_{++--}\rangle ;\\
|\psi^{(2)}\rangle &= \hat{E}|+-,\varphi\rangle = a_2|++,\varphi_{+-++}\rangle + b_2|+-,\varphi_{+-+-}\rangle + c_2|-+,\varphi_{+--+}\rangle + d_2|--,\varphi_{+---}\rangle ;\\
|\psi^{(3)}\rangle &= \hat{E}|-+,\varphi\rangle = a_3|++,\varphi_{-+++}\rangle + b_3|+-,\varphi_{-++-}\rangle + c_3|-+,\varphi_{-+-+}\rangle + d_3|--,\varphi_{-+--}\rangle ;\\
|\psi^{(4)}\rangle &= \hat{E}|--,\varphi\rangle = a_4|++,\varphi_{--++}\rangle + b_4|+-,\varphi_{--+-}\rangle + c_4|-+,\varphi_{---+}\rangle + d_4|--,\varphi_{----}\rangle .
\end{aligned} \tag{18}$$

Далее, все формулы (4) – (14) 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 (16) переходит в выражение

$$d_x = |b_1|^2 + |c_1|^2 + |d_1|^2 = 1 - |a_1|^2 . \tag{19}$$

Используя (3) и (18), 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:

$$\begin{aligned}
\alpha_1 &= (a_1 + b_1 + c_1 + d_1)/2 , \qquad \beta_1 = (a_1 - b_1 + c_1 - d_1)/2 ,\\
\gamma_1 &= (a_1 + b_1 - c_1 - d_1)/2 , \qquad \delta_1 = (a_1 - b_1 - c_1 + d_1)/2 .
\end{aligned} \tag{20}$$

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 и d_1, можно получить различные допустимые наборы параметров атакующей операции Евы.

Приведем, как пример, два таких набора:

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

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 (12), (13) при $p_1 = ... = p_8 = 1/8$.

На рис. 1 приведена зависимость $I_{\max}$ от d_z при $|\alpha_1|^2 = 1 - d_z$, $|\beta_1|^2 = |\gamma_1|^2 = |\delta_1|^2 = d_z/3$ и $p_1 = ... = p_8 = 1/8$ (кривая 1). В этом случае выражения для собственных значений (12) матрицы плотности (7) имеют вид:

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

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

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

$$\lambda_{7,8} = \frac{1}{2}(p_7 + p_8) \pm \frac{1}{2}\sqrt{(p_7 + p_8)^2 - 16p_7p_8 \cdot \frac{2}{3}d_z\left(1 - \frac{2}{3}d_z\right)}. \qquad (21)$$

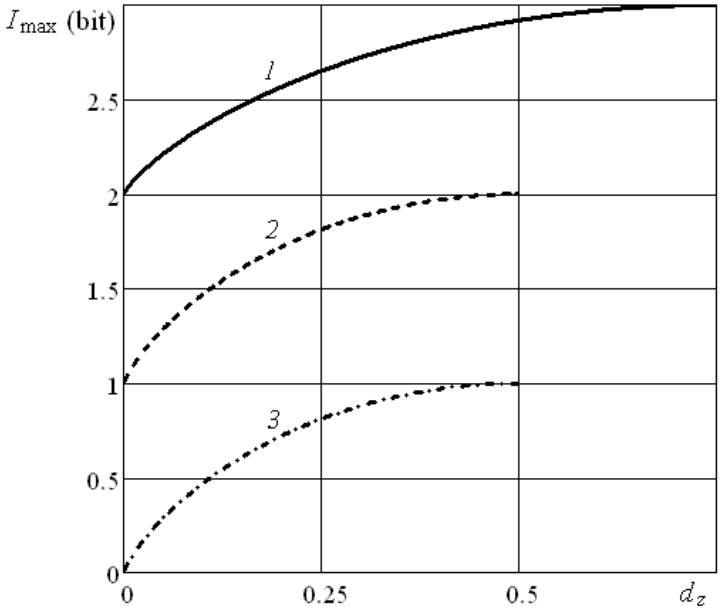

Рис. 1. Зависимость максимальной информации $I_{\max}$ Евы от вероятности d_z обнаружения атаки при измерениях в базисе B_z для трех вариантов пинг – понг протокола

Для сравнения на рис. 1 приведены также зависимости $I_{\max}$ от d_z для пинг – понг протокола с белловскими парами и квантовым сверхплотным кодированием [4] при $p_1 = ... = p_4 = 1/4$ (кривая 2) и оригинального протокола с белловскими парами и без сверхплотного кодирования [2] при $p_1 = p_2 = 1/2$ (кривая 3). Как видно из рис. 1, для протокола с ГХЦ – триплетами, как и для протокола с белловскими парами и сверхплотным кодированием, существует невидимый режим подслушивания ($d_z = 0$), если легитимные пользователи используют только один измерительный базис B_z. При этом для случая равномерного распределения частот кодирующих операций Алисы в протоколе с белловскими парами и сверхплотным кодированием Ева может получить 1 бит информации

на двоичную биграмму, т. е. 50% информации. Для протокола с ГХЦ – триплетами Ева получит 2 бита на триграмму, т. е. $\approx$66,7% информации. Поэтому для этих двух вариантов пинг – понг протокола в режиме контроля подслушивания и необходимо выполнять измерения в одном из двух базисов: B_z или B_x, выбирая один из них случайным образом для каждого цикла контроля подслушивания – Ева не имеет возможности так подобрать параметры своей пробы, чтобы d_z и d_x одновременно стремились в нулю, как следует из (16), (19) и (20) для протокола с ГХЦ – триплетами и аналогично для протокола с белловскими парами и сверхплотным кодированием [3, 4]. Отметим, что в оригинальном пинг – понг протоколе без сверхплотного кодирования в режиме контроля подслушивания используется только один базис B_z [2] и, как видно из рис. 1 (кривая 3) если информация Евы $I_{\max} > 0$, то и $d_z > 0$.

Рассмотрим теперь вопрос о том, сколько информации может получить Ева, проведя некоторое количество успешных атак, в зависимости от полной вероятности ее обнаружения. Согласно [2], вероятность того, что Ева не будет обнаружена после k успешных атак и получит информацию $I = k\, I_{\max}(d)$ определяется выражением

$$s(I,q,d) = \left(\frac{1-q}{1-q(1-d)}\right)^{\frac{I}{I_{\max}(d)}}, \qquad (22)$$

На рис. 2 приведены зависимости s от I при частоте переключения в режим контроля подслушивания $q = 0.5$, одинаковых значениях частот кодирующих операций Алисы и значениях d, соответствующих полной информации Евы, т.е. когда Ева выбирает параметры своих проб так, чтобы с достоверностью определить состояния, созданные кодирующими операциями Алисы (кривые 1 – 3). Также на рис. 2 приведена зависимость s от I для протокола с ГХЦ – триплетами при $d = 0.25$ (кривая 4), в этом случае $I_{\max} = 2{,}65$ бита на триграмму.

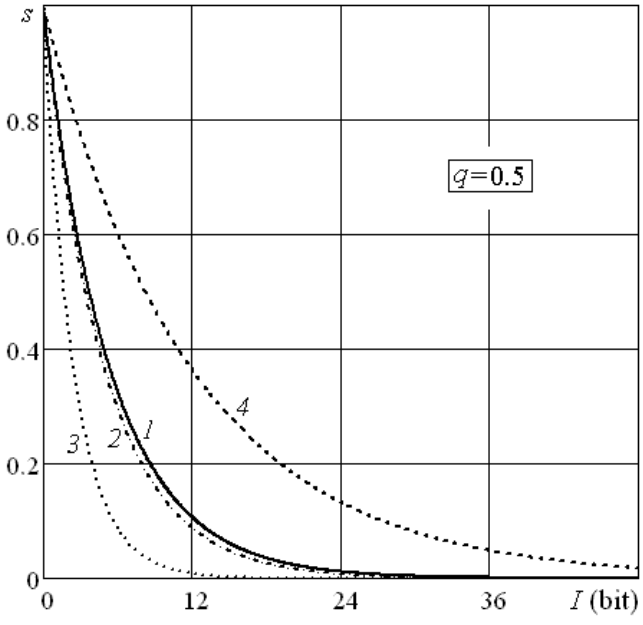

Рис. 2. Вероятность необнаружения Евы s при $q = 0.5$. Протокол:
с ГХЦ – триплетами, и сверхплотным кодированием $d = 0.75$ (1);
с белловскими парами и сверхплотным кодированием, $d = 0.5$ (2);
с белловскими парами и без сверхплотного кодирования, $d = 0.5$ (3);
с ГХЦ – триплетами и сверхплотным кодированием, $d = 0.25$ (4).

Как видно из рис. 2, количество информации, попадающей к Еве (при фиксированной величине s), меньше всего для пинг – понг протокола с белловскими парами и без

сверхплотного кодирования, несколько больше для такого же протокола со сверхплотным кодированием и больше всего для протокола с ГХЦ – триплетами. При этом информационная емкость на один раунд протокола составляет 1 бит, 2 бита и 3 бита соответственно. Таким образом, информационная емкость и безопасность различных вариантов пинг – понг протокола находятся в обратно пропорциональной зависимости. Отметим, однако, что кривые 1 и 2 лежат очень близко друг другу, что свидетельствует о практически одинаковой стойкости соответствующих протоколов к стратегии атаки, когда Ева хочет получить полную информацию о переданных битах Алисы. Так как информационная емкость протокола с ГХЦ – триплетами в 1.5 раза выше емкости протокола с белловскими парами и сверхплотным кодированием, то можно сделать вывод, что из этих двух вариантов пинг – понг протокола вариант с ГХЦ – триплетами более предпочтителен. Отметим также, что полная вероятность необнаружения подслушивания уменьшается экспоненциально с ростом успешно перехваченных бит для всех рассмотренных вариантов пинг – понг протокола (см. рис. 2). Так, даже для протокола с ГХЦ – триплетами, вероятность того, что подслушивание не будет обнаружено (при $p_1 = ... = p_8 = 1/8$, $q = 0.5$ и $d = 0.75$), равна всего 0.061 при перехвате Евой 15 бит и равна 0.011 при перехвате 24 бит.

5. Способ усиления безопасности пинг – понг протокола

Рассмотрим процедуру усиления безопасности, применяемую в квантовых протоколах распределения ключа [1, 10]. В этих протоколах Алиса сначала передает Бобу битовую последовательность через квантовый канал. В результате они получают сырой ключ некоторый длины *n*, а затем согласовывают его, исправляя ошибки. Далее, зная уровень ошибок при передаче сырого ключа, Алиса и Боб определяют величину τ – число битов, на которое надо сократить согласованный ключ, чтобы сделать информацию Евы о ключе ниже заданного малого значения. Затем Алиса генерирует случайную двоичную матрицу *K* размера $(n-\tau)\times n$ и открыто передает ее Бобу. Конечный секретный ключ (длины $n-\tau$) тогда получается умножением (по модулю 2) матрицы *K* на согласованный ключ длины *n* (процедура хеширования). При этом можно строго доказать, что при данном τ информация Евы о ключе будет ниже некоторого определенного значения [10]. Последнее можно выбрать сколь угодно малым (естественно, чем меньше информации должно быть у Евы, тем больше будет τ и соответственно тем короче будет конечный секретный ключ).

Описанный метод может быть применен для усиления безопасности пинг – понг протокола, но требует соответствующей модификации. Перед передачей Алиса разбивает сообщение на *m* блоков некоторой фиксированной длины *n*, а затем генерирует для каждого блока отдельно случайную *обратимую* двоичную матрицу K_i $(i = 1,...m)$ размера $n \times n$, умножает полученные матрицы на соответствующие блоки сообщения и передает всю полученную битовую последовательность Бобу по квантовому каналу с использованием пинг – понг протокола. Такая процедура может быть названа обратимым хешированием или хешированием с использованием двухсторонней хеш – функции, роль которой играет случайная обратимая матрица двоичных чисел. Матрицы K_i передаются Бобу по обычному открытому каналу после завершения всего протокола, но только в том случае, если Алиса и Боб убедились в отсутствии подслушивания при передаче по квантовому каналу. Затем Боб обращает полученные матрицы и, умножив их на соответствующие хешированные блоки, восстанавливает исходное сообщение.

Как следует из (22), при выборе, например, $n = 128$ бит и использовании протокола с ГХЦ – триплетами, вероятность необнаружения атаки Евы при $p_1 = ... = p_8 = 1/8$, $q = 0.5$ и $d = 0.75$ равна $4.3 \cdot 10^{-11}$, т.е. крайне маловероятно, что атака не будет обнаружена. В случае же обнаружения атаки Алиса не будет посылать случайные двоичные матрицы по обычному каналу и, следовательно, вся перехваченная Евой в квантовом канале информация не будет представлять для нее ценности. При $n = 128$ бит, $p_1 = ... = p_8 = 1/8$, $q = 0.5$ и $d = 0.25$

вероятность необнаружения атаки равна $7.4 \cdot 10^{-5}$, что также вполне приемлемо, особенно если учесть, что при таком d Ева сможет определить правильно не все биты, переданные по квантовому каналу (информация Евы в этом случае равна 113 бит). При этом Ева даже не будет точно знать, какие именно биты определены правильно. Поэтому, даже если при $d = 0.25$ после передачи блока длиной 128 бит Ева не будет обнаружена (что очень маловероятно) и Алиса передаст хеш – матрицу, Ева будет иметь не полную информацию и должна будет применить определенные классические криптоаналитические методы для восстановления исходного сообщения. Оценка стойкости протокола для случая, когда Ева определяет правильно не все переданные по квантовому каналу биты, но при этом перехватывает хеш – матрицы, будет выполнена в другой работе.

Таким образом, выбор длины хешируемого блока $n = 128$ бит обеспечивает очень высокий уровень безопасности пинг – понг протокола с ГХЦ – триплетами, а также, конечно, и протокола с белловскими парами и сверхплотным кодированием. Для оригинального пинг – понг протокола с белловскими парами и без сверхплотного кодирования [2] длину хешируемого блока можно выбрать меньшей вследствие большей стойкости самого протокола (см. рис. 2).

Следует сделать следующие замечания. Во-первых, предложенный метод усиления безопасности пинг – понг протокола не требует наличия у легитимных пользователей никаких предустановленных ключей. Таким образом, основное преимущество квантовых протоколов прямой связи, а именно отсутствие необходимости распределять ключи (за исключением небольшого ключа для аутентификации, если используется протокол аутентификации с секретным ключом), сохраняется при использовании предложенного метода. С другой стороны, генерация у Алисы случайных двоичных матриц достаточно большого размера с проверкой их на обратимость, а затем обращение этих матриц у Боба требует определенного времени, что замедлит работу всего протокола. Однако квантовые протоколы прямой связи и не предназначены для передачи высокоскоростных потоков секретных данных вследствие малой скорости передачи в квантовом канале. Область применения таких протоколов ограничена приложениями, где важен, прежде всего, высокий уровень секретности, а скорость передачи не играет существенной роли. В этом случае дополнительное время, требуемое на усиление безопасности, не будет иметь особого значения. Отметим, что исходя из критериев безопасности и скорости работы протокола, пользователи всегда могут выбрать оптимальное значение длины хешируемого блока в зависимости от того, какой из этих критериев более важен. Так, для протокола с ГЦХ – триплетами и протокола с белловскими парами и сверхплотным кодированием вместо $n = 128$ бит можно выбрать $n = 64$ или даже $n = 32$ бита, что значительно ускорит работу с хеш – матрицами. При $n = 64$ и $n = 32$ бита для протокола с ГЦХ – триплетами вероятности необнаружения атаки при $p_1 = ... = p_8 = 1/8$, $q = 0.5$, $d = 0.75$ равны соответственно $6.5 \cdot 10^{-6}$ и $2.6 \cdot 10^{-3}$.

Наконец, кратко рассмотрим модификацию пинг – понг протокола для квантового канала с шумом. В этом случае, очевидно, Алиса и Боб не могут прервать протокол сразу же после возникновения первой ошибки в режиме контроля подслушивания, как описано в разделе 2 настоящей статьи, поскольку такая ошибка может быть вызвана естественным шумом в канале, а не подслушиванием. В шумном канале Алиса должна сначала передать весь первый хешированный блок. После этого Алиса и Боб оценивают уровень ошибок, которые они зарегистрировали в режиме контроля подслушивание, и сравнивают его с некоторым граничным значением. Это граничное значение должно быть установлено заранее, для чего квантовый канал должен быть предварительно протестирован с целью определения уровня естественного шума. Как отмечалось выше, современной экспериментальной ситуации соответствует уровень ошибок в несколько процентов [5]. Если зарегистрированный после передачи первого блока уровень ошибок превышает допустимое граничное значение, то протокол прерывается, иначе передается следующий блок. Отметим, что нет необходимости передавать хеш – матрицу для первого блока сразу после передачи этого блока (и аналогично

для остальных блоков) – матрицы могут быть переданы все сразу после окончания передачи по квантовому каналу. В таком случае, очевидно, безопасность всего протокола будет значительно усилена.

Отметим также, что в квантовом канале с шумом ошибки будут возникать, конечно, не только в режиме контроля подслушивания, но и при передаче самих хешированных блоков. Поэтому для режима передачи сообщения необходимо применение помехоустойчивых кодов. Это могут быть квантовые коды исправления ошибок [1]. Однако пинг – понг протокол предназначен для передачи *классической информации по квантовому каналу*, поэтому в данном случае могут применяться и классические помехоустойчивые коды, что в настоящее время, на наш взгляд, является более простым и эффективным решением.

6. Заключение

В работе проанализирована атака с использованием квантовых проб на пинг – понг протокол с ГХЦ – триплетами, а также определена полная вероятность обнаружения подслушивающего агента в зависимости от количества полученной им информации для трех вариантов пинг – понг протокола. Показано, что информационная емкость и безопасность различных вариантов пинг – понг протокола находятся в обратно пропорциональной зависимости. При этом если подслушивающий агент выбирает стратегию атаки, которая дает полную информацию, протокол с белловскими парами и сверхплотным кодированием и протокол с ГХЦ – триплетами имеют практически одинаковую стойкость к такой атаке, что говорит о преимуществе второго протокола вследствие его большей информационной емкости. Отметим, что если подслушивающий агент решит уменьшить вероятность своего обнаружения, уменьшая величину d, то он определит правильно не все биты сообщения, причем не будет даже точно знать, какие именно биты определены правильно.

В работе показано также, что количество бит, которые может перехватить подслушивающий агент до его обнаружения, даже для протокола с ГХЦ – триплетами не превышает двух – трех десятков, что не представляет большой угрозы. В тех случаях, когда и такая утечка недопустима, использование пинг – понг протокола требует дополнительных мер по усилению безопасности. Предложен один из возможных способов усиления безопасности пинг – понг протокола, состоящий в обратимом хешировании блоков сообщения. Этот способ не требует наличия у легитимных пользователей дополнительных предустановленных ключей. Также кратко рассмотрена реализация пинг – понг протокола в квантовом канале с шумом.

Литература:

1. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. – Москва: Мир, 2006.
2. *Bostrom K., Felbinger T.* Deterministic secure direct communication using entanglement // Physical Review Letters. – 2002. – V. 89, № 18. – Art. 187902.
3. *Cai Q.-Y., Li B.-W.* Improving the capacity of the Bostrom – Felbinger protocol // Physical Review A. – 2004. – V. 69, № 5. – Art. 054301.
4. *Василиу Е.В.* Анализ безопасности пинг-понг протокола с квантовым плотным кодированием // Наукові праці ОНАЗ ім. О.С. Попова. – 2007, № 1. – С. 32 – 38.
5. *Ostermeyer M., Walenta N.* Experimental demonstration of quantum key distribution with entangled photons following the ping-pong coding protocol. – 2007. – *arXiv: quant-ph/0703242v1*.
6. *Wang Ch., Deng F.G., Long G.L.* Multi – step quantum secure direct communication using multi – particle Greenberger – Horne – Zeilinger state // Optics Communications. – 2005. – V. 253, № 1. – P. 15 – 20.
7. *Wang J., Zhang Q., Tang C.J.* Multiparty controlled quantum secure direct communication using Greenberger – Horne – Zeilinger state // Optics Communications. – 2006. – V. 266, № 2. – P. 732 – 737.
8. *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.
9. *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». – Przemysl: «Nauka i studia». – 2008. – T. 10. – C. 40 – 44. – http://www.rusnauka.com/24_SVMN_2008/Informatica/26618.doc.htm
10. *Bennett C.H., Brassard G., Crepeau C., Maurer U.M.* Generalized privacy amplification // IEEE Trans. Inform. Theory. – 1995. – V. 41, № 6. – P. 1915 – 1923.

Статья получена: 2008-06-28