УДК 003.26:621.39+530.145

Е.В. Василиу

СТОЙКОСТЬ ПИНГ-ПОНГ ПРОТОКОЛА С ТРИПЛЕТАМИ ГРИНБЕРГЕРА – ХОРНА – ЦАЙЛИНГЕРА К АТАКЕ С ИСПОЛЬЗОВАНИЕМ ВСПОМОГАТЕЛЬНЫХ КВАНТОВЫХ СИСТЕМ

На основе методов квантовой теории информации анализируется атака с применением вспомогательных квантовых систем на пинг-понг протокол с трехкубитными перепутанными состояниями Гринбергера – Хорна – Цайлингера (ГХЦ). При использовании легитимными пользователями в режиме контроля подслушивания двух измерительных базисов протокол является асимптотически безопасным. Выполняется предварительный сравнительный анализ безопасности трех вариантов пинг-понг протокола. Информационная емкость и безопасность различных вариантов пинг-понг протокола находятся в обратно пропорциональной зависимости. Количество битов, которые может перехватить подслушивающий агент до его обнаружения, даже для протокола с ГХЦ-триплетами не превышает двух-трех десятков. Кратко обсуждаются способы защиты пинг-понг протокола с ГХЦ-триплетами от других известных видов атак на пинг-понг протокол.

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, основанные на фундаментальных законах квантовой механики. Так, квантовые протоколы распределения ключей обеспечивают безопасный способ создания секретного ключа, с помощью которого две авторизованные стороны, Алиса и Боб, могут затем обмениваться секретными сообщениями с применением 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 секретное сообщение, закодированное с помощью квантовых состояний кубитов, передается непосредственно через квантовый канал связи. При этом законы квантовой механики гарантируют обнаружение подслушивания 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 используются пары фотонов, максимально перепутанных по их поляризационным степеням свободы (белловские пары) [2]. При этом 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 Евой измерением состояния этого одного кубита. Декодирование становится возможным только при выполнении измерения в базисе Белла над обоими кубитами, что позволяет определить их корреляцию друг с другом, а такое измерение может выполнить только Боб.

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, с помощью которого Алиса и Боб обнаруживают операции Евы [2–4].

Отметим, что недавно этот первоначальный вариант пинг-понг протокола был реализован на экспериментальном оборудовании [5]. Для демонстрации работы протокола по квантовому каналу был передан случайный двоичный ключ длиной 10 000 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 [2] каждый передаваемый кубит (один из перепутанной пары) используется для кодирования одного классического бита. Чтобы увеличить информационную емкость источника, необходимо использовать квантовое сверхплотное кодирование. 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 с белловскими парами 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 протокола может быть усилена с помощью методов классической криптографии. Один из таких методов, основанный на шифре Хилла и состоящий в обратимом хешировании блоков сообщения посредством умножения на случайную обратимую двоичную матрицу, предложен в [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].

Отметим, что к настоящему времени выполнен ряд экспериментальных работ по генерации многокубитных ГХЦ-состояний с поляризованными фотонами. Так, в [9] создано оборудование для генерации максимально перепутанных триплетов фотонов в ГХЦ-состояниях. В работе [10] аналогичное оборудование создано для генерации различных четырехфотонных состояний, в том числе состояний ГХЦ, а в [11] – для шестифотонных перепутанных по поляризации состояний. Таким образом, современное оборудование уже позволяет генерировать небольшие группы перепутанных по поляризации фотонов и оперировать с ними, что открывает возможность практической реализации пинг-понг протокола с многокубитными ГХЦ-состояниями.

Схема пинг-понг протокола с использованием ГХЦ-триплетов и квантового сверхплотного кодирования, разработанная на основе оригинальной версии протокола [2] и многошагового протокола [6], предложена в [12]. Эта схема кратко изложена в следующем разделе статьи. В работе [2] была проанализирована атака подслушивающего агента с использованием квантовых проб на оригинальный пинг-понг протокол, в [4] аналогичный анализ выполнен для пинг-понг протокола с белловскими парами и квантовым сверхплотным кодированием. Целью настоящей работы является анализ атаки на пинг-понг протокол с ГХЦ-триплетами и последующая сравнительная оценка безопасности различных вариантов пинг-понг протокола.

1. Пинг-понг протокол с ГХЦ-триплетами

Существует восемь полностью перепутанных ортогональных трехкубитных ГХЦ-состояний:

$$\begin{aligned} \left|\Psi_{1,2}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|000\right\rangle \pm \left|111\right\rangle\right); \quad \left|\Psi_{3,4}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|100\right\rangle \pm \left|011\right\rangle\right); \\ \left|\Psi_{5,6}\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|010\right\rangle \pm \left|101\right\rangle\right); \quad \left|\Psi_{7,8}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|110\right\rangle \pm \left|001\right\rangle\right), \end{aligned} \tag{1}$$

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, например, горизонтальной и вертикальной (или левой круговой и правой круговой) поляризациям фотона.

Боб приготавливает три фотона в состоянии $|\Psi_1\rangle$. 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 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 [12]

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

и соответствуют трехбитовым комбинациям «000», «001», «010», «011», «100», «101», «110» и «111». В выражении (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 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. Получив сообщение от Алисы, 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.

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 (пренебрегаем здесь возможными ошибками при излучении, детектировании и передаче фотонов и считаем, что используется идеальное оборудование). В этом случае 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 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.

2. Вывод выражения для максимальной информации Евы при атаке 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 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» на пути Алиса $\rightarrow$ Боб.

Кроме режима передачи сообщения, легитимные пользователи с определенной вероятностью q переключаются 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 E, что и позволяет легитимным пользователем обнаружить атаку. Отметим, что в режиме контроля подслушивания фотоны не передаются обратно от Алисы к Бобу и Ева не выполняет своего финального измерения. Таким образом, легитимные пользователи могут выявить только атакующую операцию E, которую Ева проводит на линии Боб $\rightarrow$ Алиса.

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

Состояние пересылаемой Бобом пары кубитов неотличимо для Евы от полностью смешанного, так как его редуцированная матрица плотности $\rho_B = Tr_3\left(|\Psi_1\rangle\langle\Psi_1|\right) = \left(|00\rangle\langle 00| + |11\rangle\langle 11|\right)/2$, где индекс 3 у символа операции «частичный след» обозначает номер кубита, по которому берется след. Таким образом, аналогично анализу 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

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

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

Матричное представление атакующей операции Евы имеет вид

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

Из условия унитарности операции E следуют такие соотношения между параметрами пробы Евы:

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

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 сначала случай, когда Боб посылает $|00\rangle$, т. е. состояние квантовой системы «передаваемые кубиты – проба Евы» после атаки E становится $|\psi^{(1)}\rangle$ (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» будет иметь вид

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

где

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

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

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

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

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

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

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

$$\{|00,\varphi_{0000}\rangle, |01,\varphi_{0000}\rangle, |10,\varphi_{0000}\rangle, |11,\varphi_{0000}\rangle, |00,\varphi_{0001}\rangle, |01,\varphi_{0001}\rangle, |10,\varphi_{0001}\rangle, |11,\varphi_{0001}\rangle, \tag{11}$$

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

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

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

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

Таким образом, максимальная информация Евы

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

где λ_i определены в (12).

Аналогично рассматриваются остальные случаи в (3), т. е. когда Боб вместо $\left|00\right\rangle$ посылает $\left|01\right\rangle$, $\left|10\right\rangle$, или $\left|11\right\rangle$. При учете соотношений (6) для $\left|10\right\rangle$ собственные значения матрицы плотности совпадают с (12), а для $\left|01\right\rangle$ и $\left|11\right\rangle$ имеют вид

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

3. Анализ стратегии атаки на протокол с ГХЦ-триплетами и сравнительная оценка безопасности трех вариантов пинг-понг протокола

При использовании в режиме контроля подслушивания двух измерительных базисов B_z и B_x вероятность обнаружить атакующую операцию E Евы определяется выражением

$$d=q_zd_z+q_xd_x\,, \tag{15}$$

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 выберет 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, такое, 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 Алиса 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, такие, 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). Как следует из (3) и (6), то же самое выражение для d_z получается и когда Боб посылает $|10\rangle$ и $|11\rangle$. 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 $|--\rangle$ с одинаковой вероятностью $p = 1/4$. Тогда формулы (3) заменяются на следующие:

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

Далее, все формулы (4)–(14) остаются справедливыми при замене $|00\rangle \to |++\rangle$, $|01\rangle \to |+-\rangle$, $|10\rangle \to |-+\rangle$, $|11\rangle \to |--\rangle$, $\alpha_1 \to a_1$, $\beta_1 \to b_1$, $\gamma_1 \to c_1$, $\delta_1 \to d_1$, $\alpha_2 \to a_2$ 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:

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

Применяя 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.

Так, примером такого набора параметров является

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

где $I_{\max}$ получено по формулам (12), (13) при $p_1 = ... = p_8 = 1/8$.

На рис. 1 показана 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) принимают вид

$$\lambda_{1,2} = \lambda_{3,4} = \lambda_{5,6} = \lambda_{7,8} = \frac{1}{8} \pm \frac{1}{2} \sqrt{\frac{1}{16} - \frac{1}{4} \cdot \frac{2}{3} d_z \left(1 - \frac{2}{3} d_z \right)} . \tag{21}$$

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 без сверхплотного кодирования [2] при $p_1 = p_2 = 1/2$ (кривая 3).

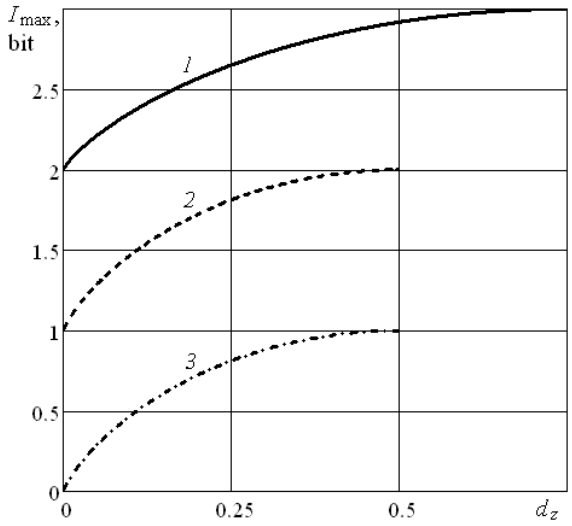

Рис. 1. Зависимость максимальной информации Евы от вероятности обнаружения атаки при измерениях в базисе B_z: *1* – протокол с ГХЦ-триплетами; *2* – с белловскими парами и сверхплотным кодированием; *3* – с белловскими парами и без сверхплотного кодирования

Из рис. 1 видно, что 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 необходимо выполнять измерения в одном из двух базисов B_z или B_x, выбирая один из них случайным образом для каждого цикла контроля подслушивания. При этом, как следует из (16), (19) и (20) для протокола с ГХЦ-триплетами и аналогично для протокола с белловскими парами и сверхплотным кодированием [3, 4], Ева не имеет возможности так подобрать параметры своей пробы, чтобы d_z и d_x одновременно стремились к нулю. 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 *n* успешных атак и получит информацию $I = n\, I_{\max}(d)$, определяется выражением

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

На рис. 2 изображены 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.

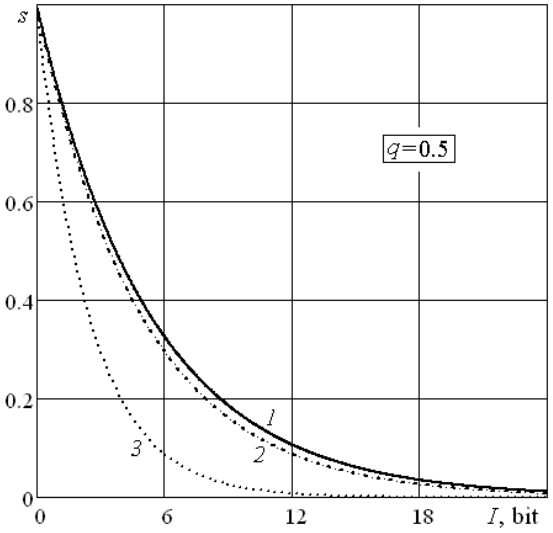

Рис. 2. Вероятность необнаружения Евы *s* при $q = 0{,}5$:
1 – протокол с ГХЦ-триплетами, $d = 0{,}75$; *2* – с белловскими парами и сверхплотным кодированием, $d = 0{,}5$; *3* – с белловскими парами и без сверхплотного кодирования, $d = 0{,}5$

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 цикл протокола составляет 1, 2 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 к 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 предпочтительнее. 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.

4. Другие возможные атаки на пинг-понг протокол с ГЦХ-триплетами

Рассмотрим другие известные атаки на оригинальный пинг-понг протокол [13–15] и проанализируем возможность таких атак на протокол с ГХЦ-триплетами, а также способы защиты этого протокола от подобных атак.

В работе [13] предложена атака на оригинальный пинг-понг протокол, использующая два дополнительных фотона, которые перепутываются с передаваемым фотоном применением определенных квантовых гейтов. Эта атака не может быть обнаружена в режиме контроля подслушивания (стандартном для оригинального протокола), но создает 50 %-е потери в канале, что может быть легко обнаружено легитимными пользователями, если естественный уровень шума в канале невелик. В работе [14] атака была усовершенствована таким образом, что дополнительные потери в канале не создаются, однако оба варианта этой атаки создают дополнительный «передаваемый» фотон, который может быть зарегистрирован Алисой и Бобом и свидетельствует об операциях Евы [13, 14]. Также атаки [13, 14] создают дополнительный уровень ошибок в 25 % в режиме передачи сообщения, что также могут обнаружить легитимные пользователи. Еще один способ обнаружить такую атаку состоит в применении двух базисов B_z и B_x в режиме контроля подслушивания вместо одного базиса B_z, как в оригинальном пинг-понг протоколе. При использовании двух базисов вероятность обнаружения атаки составляет 25 % [14].

В протоколе с ГХЦ-триплетами используются два базиса в режиме контроля подслушивания. Таким образом, атака на этот протокол, аналогичная рассмотренной в [13, 14], может быть обнаружена. Возможно, существуют и другие атаки на протокол с ГХЦ-триплетами с использованием составных квантовых проб и применением определенных последовательностей квантовых гейтов. Этот вопрос требует дополнительных исследований.

Любой вариант пинг-понг протокола также уязвим к двум видам атак, хорошо известных и в классической криптографии: атаке «человек посередине» и атаке «отказ в обслуживании». Для атаки «человек посередине» Ева должна полностью контролировать классический канал связи между Алисой и Бобом, т. е. иметь возможность изменять все сообщения, которыми они обмениваются в режиме контроля подслушивания. Защита от этой атаки хорошо известна: легитимные пользователи должны снабжать кодом аутентичности [16] все передаваемые в классическом канале сообщения, и этот способ защиты пригоден для любого варианта пинг-понг протокола, в том числе протокола с ГХЦ-триплетами.

Атака «отказ в обслуживании», впервые рассмотренная в [15] для оригинального пинг-понг протокола, заключается в следующем. Ева не перепутывает свою пробу с передаваемым кубитом на пути Боб $\rightarrow$ Алиса, а просто измеряет состояние кубита на обратном пути Алиса $\rightarrow$ Боб (в режиме передачи сообщения), тем самым разрушая запутанность между домашним и передаваемым кубитами. При этом Ева не получит никакой информации, но разрушит квантовый канал связи между Алисой и Бобом, так как результаты измерений Боба станут случайными и никак не зависящими от кодирующих операций Алисы. Разумеется, подобным образом Ева может изме-

рять состояния двух передаваемых кубитов (или даже только одного) в протоколе с ГХЦ-триплетами и разрушать запутанность ГХЦ-состояния.

Метод обнаружения атаки «отказ в обслуживании» был предложен в [15] и состоит в небольшой модификации режима контроля подслушивания: часть кубитов в этом режиме Алиса не измеряет, а отправляет обратно Бобу. Боб проводит измерение в базисе Белла и определяет, сохранилось ли начальное перепутанное состояние, которое он приготовил. При этом в случае атаки Евы вероятность того, что Боб получит неверный результат, равна 0,5, и в таком случае протокол необходимо прервать [15]. Аналогичным образом эта атака может быть обнаружена и для протокола с ГХЦ-триплетами: часть передаваемых пар кубитов Алиса в режиме контроля подслушивания должна возвращать Бобу, а он должен проводить измерения в ГХЦ-базисе и определять сохранность приготовленного им начального состояния $|\Psi_1\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$. Отметим, что такой способ выявления атаки «отказ в обслуживании» пригоден только для идеального квантового канала. Для шумного канала необходимо разработать отдельный способ обнаружения этой атаки.

Заключение

В работе рассмотрена атака с использованием квантовых проб на пинг-понг протокол с ГХЦ-триплетами, а также вычислена 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 о переданных битах, 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.

Количество битов, 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 секретности. Детальный анализ способов усиления секретности различных вариантов пинг-понг протокола с учетом полученных оценок попадающей к подслушивающему агенту информации будет предметом другой работы.

Список литературы

1. Нильсен, М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – М. : Мир, 2006. – 824 с.

2. Bostrom, K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – Vol. 89, № 18. – Art. 187902.

3. Cai, Q.-Y. Improving the capacity of the Bostrom – Felbinger protocol / Q.-Y. Cai, B.-W. Li // Physical Review A. – 2004. – Vol. 69, № 5. – Art. 054301.

4. Василиу, Е.В. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32–38.

5. Ostermeyer, M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. – 2008. – Vol. 281, № 17. – P. 4540–4544.

6. Wang, Ch. Multi-step quantum secure direct communication using multi-particle Greenberger – Horne – Zeilinger state / Ch. Wang, F.G. Deng, G.L. Long // Optics Communications. – 2005. – Vol. 253, № 1. – P. 15–20.

7. Wang, J. Multiparty controlled quantum secure direct communication using Greenberger – Horne – Zeilinger state / J. Wang, Q. Zhang, C.J. Tang // Optics Communications. – 2006. – Vol. 266, № 2. – P. 732–737.

8. Василиу, Е.В. Безопасность пинг-понг протокола квантовой связи для передачи текстовых сообщений / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 2. – С. 36–44.

9. Experimental high-intensity three-photon entangled source / H.-X. Lu [et al.] // Physical Review A. – 2008. – Vol. 78, № 3. – Art. 033819.

10. Xu, J.-S. Generation of a High-Visibility Four-Photon Entangled State and Realization of a Four-Party Quantum Communication Complexity Scenario / J.-S. Xu, Ch.-F. Li, G.-C. Guo // Physical Review A. – 2006. – Vol. 74, № 5. – Art. 052311.

11. Experimental entanglement of six photons in graph states / Ch.-Y. Lu [et al.] // Nature Physics. – 2007. – Vol. 3. – P. 91–95.

12. Василиу, Е.В. Пинг-понг протокол с трех- и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера / Е.В. Василиу, Л.Н. Василиу // Тр. Одесского политехн. ун-та. – 2008. – Вып. 1 (29). – С. 171–176.

13. Wojcik, A. Eavesdropping on the «Ping-Pong» Quantum Communication Protocol / A. Wojcik // Physical Review Letters. – 2003. – Vol. 90, № 15. – Art. 157901.

14. Zhang, Zh.-J. Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss / Zh.-J. Zhang, Y. Li, Zh.-X. Man // Physics Letters A. – 2005. – Vol. 341, № 5–6. – P. 385–389.

15. Cai, Q.-Y. The «Ping-Pong» Protocol Can Be Attacked without Eavesdropping / Q.-Y. Cai // Physical Review Letters. – 2003. – Vol. 91, № 10. – Art. 109801.

16. Фергюсон, Н. Практическая криптография; пер. с англ. / Н. Фергюсон, Б. Шнайер. – М.: Изд. дом «Вильямс», 2005. – 424 с.

Поступила 13.11.08

Одесская национальная академия связи им. А.С. Попова,
Одесса, Кузнечная, 1
e-mail: vasiliu@ua.fm

Ye.V. Vasiliu

SECURITY OF THE PING-PONG PROTOCOL WITH GREENBERGER – HORNE – ZEILINGER TRIPLETS AGAINST ATTACK WITH THE USE OF AUXILIARY QUANTUM SYSTEMS

The attack using auxiliary quantum systems on the ping-pong protocol with three-qubit entangled Greenberger – Horne – Zeilinger states is analyzed. It is shown, that the protocol is asymptotic secure using two measuring bases by legitimate users in a control mode similarly to the ping-pong protocol with the Bell states. The preliminary comparative security analysis of three variants of the ping-pong protocol is carried out. It is shown, that the information capacity and the security of various variants of the ping-pong protocol are in the inverse proportion. It is shown also, that the amount of bits, which the eavesdropper can intercept before its detection, even for the protocol with GHZ-triplets, does not exceed two-three tens. Protection methods of the ping-pong protocol with GHZ-triplets against other known kinds of attacks on the ping-pong protocol are briefly discussed.