На основі методів квантової теорії інформації проаналізована атака пасивного перехвату з використанням допоміжних квантових систем на пінг – понг протокол з повністю переплутаними парами тривимірних квантових систем – кутритів. Отримано вираз для кількості інформації агента, що підслуховує, як функції від імовірності виявлення атаки. Показано, що стійкість до атаки пінг – понг протоколу з парами кутритів вище стійкості протоколу з парами кубітів

Ключові слова: пінг – понг протокол з кутритами, атака пасивного перехопленя, кількість інформації зловмисника, асимптотична безпека

На основе методов квантовой теории информации проанализирована атака пассивного перехвата с использованием вспомогательных квантовых систем на пинг – понг протокол с полностью перепутанными парами трехмерных квантовых систем – кутритов. Получено выражение для количества информации подслушивающего агента как функции от вероятности обнаружения атаки. Показано, что стойкость к атаке пинг – понг протокола с парами кутритов выше стойкости протокола с парами кубитов

Ключевые слова: пинг – понг протокол с кутритами, атака пассивного перехвата, количество информации подслушивающего агента, асимптотическая безопасность

On the basis of methods of quantum information theory the eavesdropping attack with the use of auxiliary quantum systems on ping – pong protocol with completely entangled pair of three – dimensional quantum systems – qutrits is analyzed. The formula for quantity of the eavesdropper's information as functions from probability of attack's detection is deduced. It is shown, that the resistance against the attack of ping – pong protocol with pairs of qutrits is above the resistance of the protocol with pair of qubits

Key words: ping – pong protocol with qutrits, eavesdropping attack, amount of eavesdropper's information, asymptotic security

УДК 003.26:621.39+530.14

АНАЛИЗ АТАКИ ПАССИВНОГО ПЕРЕХВАТА НА ПИНГ – ПОНГ ПРОТОКОЛ С ПОЛНОСТЬЮ ПЕРЕПУТАННЫМИ ПАРАМИ КУТРИТОВ

Е.В. Василиу
Кандидат физико-математических наук, доцент
Кафедра информатизации и управления
Одесская национальная академия связи им. А.С. Попова
ул. Кузнечная, 1, г. Одесса, Украина, 65029
Контактный тел.: 8-067-302-99-49
E-mail: vasiliu@ua.fm

Р. С. Мамедов
Аспирант, начальник телекоммуникационного узла
ПО "Азтелеком"
ул. М.Э. Расудзаде, 1, г. Ширван, Азербайджанская республика
E-mail: r.s.mamedov@mail.ru

1. Введение

В настоящее время квантовая криптография является одним из быстро развивающихся приложений квантовой теории информации и предлагает новый, основанный на законах квантовой физики, подход к решению важной проблемы защиты телекоммуникационных каналов от прослушивания неавторизованными лицами. Одно из направлений квантовой криптографии – квантовые протоколы безопасной связи [1

– 4], в которых секретное сообщение, закодированное в состояниях квантовых систем, передается по квантовому каналу связи без предварительного шифрования этого сообщения. Таким образом, квантовые протоколы безопасной связи являются бесключевыми протоколами, что позволяет обойти сложную проблему генерации, хранения и распределения секретных ключей.

Одним из протоколов квантовой безопасной связи является пинг – понг протокол, который может быть реализован с полностью перепутанными состояниями пар или групп кубитов. Разработано несколько вариантов пинг – понг протокола с кубитами, а также исследована их стойкость к различным атакам [1 – 9]. Использование вместо кубитов квантовых систем с бóльшей размерностью позволит увеличить информационную емкость источника. Так, протокол с полностью перепутанными парами трехмерных квантовых систем (кутритов) и квантовым сверхплотным кодированием для кутритов будет иметь емкость $\log_2 9 = 3.17$ битов на цикл вместо двух битов на цикл для протокола с парами кубитов. Отметим, что с технологической точки зрения оперировать с кутритами пока сложнее, чем с кубитами, однако ряд экспериментов по созданию перепутанных пар кутритов выполнен к настоящему времени [10,11].

Недавно предложен протокол квантовой безопасной связи с перепутанными парами кутритов, использующий схему пинг – понг протокола, а также передачу кутритов блоками [12]. Однако в [12] не рассмотрены полностью даже операции, необходимые для режима контроля подслушивания, не говоря уже о полном анализе атаки перехвата на предложенный протокол. Таким образом, к настоящему времени пинг – понг протокол с перепутанными парами кутритов не разработан полностью, а также не проведен анализ его стойкости к атакам. Целью настоящей работы является анализ атаки пассивного перехвата на пинг – понг протокол с перепутанными парами кутритов, а также сравнение стойкости этого протокола со стойкостью протоколов с кубитами.

2. Пинг – понг протокол с полностью перепутанными парами кутритов

Существует девять полностью перепутанных ортонормированных состояний пары кутритов (белловские состояния пары кутритов) [12]:

$$|\Psi_{00}\rangle = \left(|00\rangle + |11\rangle + |22\rangle\right)/\sqrt{3};$$

$$|\Psi_{10}\rangle = \left(|00\rangle + e^{2\pi i/3}|11\rangle + e^{4\pi i/3}|22\rangle\right)/\sqrt{3};$$

$$|\Psi_{20}\rangle = \left(|00\rangle + e^{4\pi i/3}|11\rangle + e^{2\pi i/3}|22\rangle\right)/\sqrt{3};$$

$$|\Psi_{01}\rangle = \left(|01\rangle + |12\rangle + |20\rangle\right)/\sqrt{3};$$

$$|\Psi_{11}\rangle = \left(|01\rangle + e^{2\pi i/3}|12\rangle + e^{4\pi i/3}|20\rangle\right)/\sqrt{3};$$

$$|\Psi_{21}\rangle = \left(|01\rangle + e^{4\pi i/3}|12\rangle + e^{2\pi i/3}|20\rangle\right)/\sqrt{3};$$

$$|\Psi_{02}\rangle = \left(|02\rangle + |10\rangle + |21\rangle\right)/\sqrt{3};$$

$$|\Psi_{12}\rangle = \left(|02\rangle + e^{2\pi i/3}|10\rangle + e^{4\pi i/3}|21\rangle\right)/\sqrt{3};$$

$$|\Psi_{22}\rangle = \left(|02\rangle + e^{4\pi i/3}|10\rangle + e^{2\pi i/3}|21\rangle\right)/\sqrt{3}. \quad (1)$$

Состояния (1) могут быть преобразованы одно в другое применением локальных унитарных операций к одному из кутритов пары [12]. Таким образом, имеется возможность реализовать квантовое сверхплотное кодирование для пары кутритов, т.е., передавая по квантовому каналу связи только один из кутритов перепутанной пары, передать при этом два классических трита информации.

Принимающая сторона (Боб) готовит одно из двухкутритных состояний (1), пусть это будет состояние $|\Psi_{00}\rangle$, а затем посылает один из кутритов передающей стороне (Алисе). Пусть Боб оставляет у себя первый кутрит из пары – "домашний" кутрит, и посылает Алисе второй – "передаваемый" кутрит.

Алиса выполняет одну из девяти кодирующих операций над полученным кутритом, в соответствии с парой классических тритов (троичной биграммой), которую она хочет послать. Например, состояние $|\Psi_{00}\rangle$ соответствует "00", $|\Psi_{10}\rangle$ – "10", $|\Psi_{20}\rangle$ – "20" и т.д. Алиса и Боб договариваются о таком соответствии заранее. Затем Алиса отправляет передаваемый кутрит обратно Бобу, который выполняет измерение над обоими кутритами в базисе Белла для кутритов, представляющем собой набор из девяти операторов $\left\{|\Psi_{ij}\rangle\langle\Psi_{ij}|\right\}$, где i, j = 0...2. Тем самым Боб точно определяет состояние, созданное кодирующей операцией Алисы, и, соответственно, троичную биграмму, которую она послала. Описанная последовательность операций называется режимом передачи сообщения. Кодирующие операции Алисы, действующие на второй кутрит пары и преобразующие состояние $|\Psi_{00}\rangle$ в состояния $|\Psi_{00}\rangle$ ... $|\Psi_{22}\rangle$ соответственно, имеют вид [12]:

$$U_{00} = |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|;$$

$$U_{10} = |0\rangle\langle 0| + e^{2\pi i/3}|1\rangle\langle 1| + e^{4\pi i/3}|2\rangle\langle 2|;$$

$$U_{20} = |0\rangle\langle 0| + e^{4\pi i/3}|1\rangle\langle 1| + e^{2\pi i/3}|2\rangle\langle 2|;$$

$$U_{01} = |1\rangle\langle 0| + |2\rangle\langle 1| + |0\rangle\langle 2|;$$

$$U_{11} = |1\rangle\langle 0| + e^{2\pi i/3}|2\rangle\langle 1| + e^{4\pi i/3}|0\rangle\langle 2|;$$

$$U_{21} = |1\rangle\langle 0| + e^{4\pi i/3}|2\rangle\langle 1| + e^{2\pi i/3}|0\rangle\langle 2|;$$

$$U_{02} = |2\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 2|;$$

$$U_{12} = |2\rangle\langle 0| + e^{2\pi i/3}|0\rangle\langle 1| + e^{4\pi i/3}|1\rangle\langle 2|;$$

$$U_{22} = |2\rangle\langle 0| + e^{4\pi i/3}|0\rangle\langle 1| + e^{2\pi i/3}|1\rangle\langle 2|. \quad (2)$$

Поскольку подслушивающий агент (Ева) не имеет доступа к домашнему кутриту, хранящемуся в квантовой памяти у Боба в течение одного цикла протокола, то она не может получить никакой информации, просто перехватив передаваемый кутрит на пути Алиса → Боб и измерив его состояние. Состояние передаваемого кутрита полностью смешанное – его редуцированная ма-

трица плотности имеет вид $\rho_{red}=\frac{1}{3}\left(|0\rangle\langle 0|+|1\rangle\langle 1|+|2\rangle\langle 2|\right)$. Однако, Ева имеет возможность провести атаку с помощью дополнительных квантовых систем (проб), перепутываемых с передаваемым кутритом на пути Боб $\rightarrow$ Алиса (рис. 1). Затем Ева выполняет измерение над составной квантовой системой "передаваемый кутрит – проба" на пути Алиса $\rightarrow$ Боб. Поэтому, кроме режима передачи сообщения в пинг – понг протоколе необходим также режим контроля подслушивания, позволяющий обнаружить перепутывающую операцию Евы.

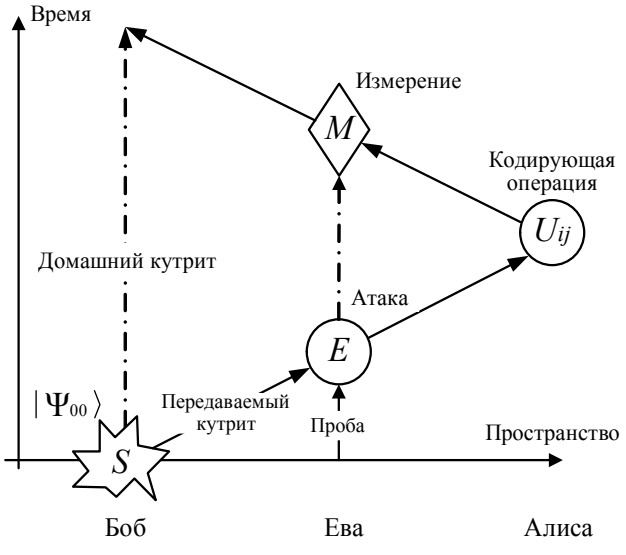

Рис. 1. Схема атаки на пинг -понг протокол с парами кутритов (S - источник перепутанных пар кутритов)

Алиса переключается в режим контроля подслушивания случайным образом с некоторой вероятностью q. В этом режиме Алиса не выполняет кодирующих операций (2), а случайно выбирает один из взаимно несмещенных (дополнительных) измерительных базисов, измеряет в этом базисе передаваемый кутрит и сообщает Бобу по классическому (не квантовому) каналу связи результат измерения и выбранный базис.

Всего имеется четыре взаимно несмещенных базиса для кутритов, из которых два называются z-базисом и x-базисом [12], а два других назовем v-базисом и t-базисом:

$$|z_0\rangle=|0\rangle,\quad |z_1\rangle=|1\rangle,\quad |z_2\rangle=|2\rangle; \tag{3}$$

$$|x_0\rangle=\left(|0\rangle+|1\rangle+|2\rangle\right)/\sqrt{3},$$

$$|x_1\rangle=\left(|0\rangle+e^{2\pi i/3}|1\rangle+e^{-2\pi i/3}|2\rangle\right)/\sqrt{3},$$

$$|x_2\rangle=\left(|0\rangle+e^{-2\pi i/3}|1\rangle+e^{2\pi i/3}|2\rangle\right)/\sqrt{3}; \tag{4}$$

$$|v_0\rangle=\left(e^{2\pi i/3}|0\rangle+|1\rangle+|2\rangle\right)/\sqrt{3},$$

$$|v_1\rangle=\left(|0\rangle+e^{2\pi i/3}|1\rangle+|2\rangle\right)/\sqrt{3},$$

$$|v_2\rangle=\left(|0\rangle+|1\rangle+e^{2\pi i/3}|2\rangle\right)/\sqrt{3}; \tag{5}$$

$$|t_0\rangle=\left(e^{-2\pi i/3}|0\rangle+|1\rangle+|2\rangle\right)/\sqrt{3};$$

$$|t_1\rangle=\left(|0\rangle+e^{-2\pi i/3}|1\rangle+|2\rangle\right)/\sqrt{3};$$

$$|t_2\rangle=\left(|0\rangle+|1\rangle+e^{-2\pi i/3}|2\rangle\right)/\sqrt{3}. \tag{6}$$

Измерение Алисы в любом из базисов дает один из трех возможных результатов – "0", "1" или "2", каждый с вероятностью 1/3. Получив от Алисы результат измерения и выбранный базис, Боб выполняет измерение состояния своего домашнего кутрита. При этом Боб должен выбрать измерительный базис в соответствии с правилами, которые вытекают из записи состояния $|\Psi_{00}\rangle$ в четырех базисах (3) – (6):

$$|\Psi_{00}\rangle=\left(|00\rangle+|11\rangle+|22\rangle\right)/\sqrt{3}=\left(|x_0x_0\rangle+|x_1x_2\rangle+|x_2x_1\rangle\right)/\sqrt{3}=$$

$$=\left(|t_0v_0\rangle+|t_1v_1\rangle+|t_2v_2\rangle\right)/\sqrt{3}=\left(|v_0t_0\rangle+|v_1t_1\rangle+|v_2t_2\rangle\right)/\sqrt{3}. \tag{7}$$

Выражения (7) получены путем прямого вычисления действия проекционных операторов в базисах (4) – (6) на состояние $|\Psi_{00}\rangle$, записанное в вычислительном базисе (3), т.е. на $|\Psi_{00}\rangle=\left(|00\rangle+|11\rangle+|22\rangle\right)/\sqrt{3}$.

Из (7) следуют правила для измерения Боба. Так, если Алиса выбрала z-базис и получила результат "0", то Боб тоже должен выбрать z-базис и его результат с определенностью будет "0". Аналогично, если результат Алисы при измерении в z-базисе "1" или "2", то и Боб в этом базисе должен получить "1" или "2" соответственно. Если Алиса выбрала x-базис, то Боб тоже должен выбрать этот базис. При результатах Алисы "0", "1" или "2" (соответствующих состояниям $|x_0\rangle$, $|x_1\rangle$ и $|x_2\rangle$) Боб с определенностью получит "0", "2" или "1" соответственно. Если же Алиса выберет v-базис, то согласно (7) Боб должен выбрать t-базис, и наоборот, а результаты измерений Боба в зависимости от результатов Алисы также следуют из (7).

Если результаты Боба отличаются от вышеприведенных, то это означает, что состояние $|\Psi_{00}\rangle$ изменено при передаче кутрита от Боба к Алисе. Это может быть обусловлено двумя причинами: атакой Евы или шумом в квантовом канале связи. Мы не рассматриваем реализацию пинг – понг протокола в канале с шумом и считаем, что легитимные пользователи используют идеальный квантовый канал. В таком случае несоответствие результата измерения Боба ожидаемому свидетельствует об атаке Евы и легитимные пользователи должны немедленно прервать сеанс связи. Однако, для пинг – понг протоколов с группами перепутанных кубитов атака Евы не приводит к тому, что Алиса и Боб обнаруживают изменение приготовленного Бобом состояния сразу же при первом контроле подслушивания [1, 5, 6]. В протоколах с кубитами атакующая операция Евы обнаруживается за один раунд контроля подслушивания с некоторой вероятностью и легитимные пользователи должны выполнить некоторое количество раундов для того, чтобы сделать вероятность обнаружения атаки сколь угодно близкой к единице [6]. Для пинг – понг протокола с парами перепутанных кутритов ситуация будет аналогичной, а конкретное число раундов контроля подслушивания, необходимых для обнаружения атаки с заданной наперед вероятностью, можно определить, проанализировав атаку Евы.

Результаты такого анализа изложены в следующем разделе статьи.

3. Атака с использованием квантовых проб на пинг – понг протокол с перепутанными парами кутритов

Согласно схеме пинг – понг протокола, Алиса сообщает Бобу по классическому открытому каналу о переключении в режим контроля подслушивания после получения от него передаваемого кутрита. Ева, прослушивая этот канал, узнает о переключении в режим контроля подслушивания после выполнения атакующей операции E, но до своего финального измерения (см. рис. 1). Следовательно, в этом случае Ева не будет выполнять измерение. Таким образом, легитимные пользователи могут выявить только атакующую операцию E на линии Боб $\rightarrow$ Алиса.

Согласно теореме расширения Стайнспринга [13], атакующая операция Евы 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 передаваемого Бобом кутрита ($\dim H_B = 3$). Таким образом, Ева может, в частности, использовать для атаки пробы, состоящие из одного ($\dim H_E = 3$) или двух ($\dim H_E = 9$) кутритов. Атака с использованием двухкутритных проб является более общей и соответственно более сильной, поэтому проанализируем эту атаку.

Так как состояние передаваемого кутрита полностью смешанное, то, аналогично пинг – понг протоколу с кубитами [2, 3, 5], в данном случае можно считать, что Боб посылает кутрит в одном из состояний $|0\rangle$, $|1\rangle$ или $|2\rangle$ с одинаковой вероятностью 1/3.

Таким образом, состояния составной системы "передаваемый кутрит – проба Евы" после атаки могут быть записаны в виде:

$$|\psi^{(0)}\rangle = E|0,\varphi\rangle = \alpha_0|0,\varphi_{00}\rangle + \beta_0|1,\varphi_{01}\rangle + \gamma_0|2,\varphi_{02}\rangle;$$

$$|\psi^{(1)}\rangle = E|1,\varphi\rangle = \alpha_1|0,\varphi_{10}\rangle + \beta_1|1,\varphi_{11}\rangle + \gamma_1|2,\varphi_{12}\rangle;$$

$$|\psi^{(2)}\rangle = E|2,\varphi\rangle = \alpha_2|0,\varphi_{20}\rangle + \beta_2|1,\varphi_{21}\rangle + \gamma_2|2,\varphi_{22}\rangle, \quad (8)$$

где $\{|\varphi_{ij}\rangle\}$, i, j = 0...2 – множество состояний двухкутритной пробы Евы.

Матричное представление атакующей операции Евы имеет вид:

$$E = \begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_0 & \beta_1 & \beta_2 \\ \gamma_0 & \gamma_1 & \gamma_2 \end{bmatrix} \quad (9)$$

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

$$\alpha_i^*\alpha_j + \beta_i^*\beta_j + \gamma_i^*\gamma_j = \delta_{ij}, \quad (10)$$

где δ_{ij} – символ Кронекера, i, j = 0...2.

Также по причине того, что состояние передаваемого кутрита полностью смешанное, должны выполняться следующие соотношения:

$$|\alpha_0|^2 = |\beta_1|^2 = |\gamma_2|^2; \ |\alpha_1|^2 = |\beta_2|^2 = |\gamma_0|^2; \ |\alpha_2|^2 = |\beta_0|^2 = |\gamma_1|^2. \quad (11)$$

Рассмотрим сначала случай, когда Боб "посылает $|0\rangle$". В этом случае состояние системы "передаваемый кутрит – проба Евы" после атаки E становится $|\psi^{(0)}\rangle$ (см. (8)).

После выполнения Алисой кодирующих операций U_{00}, U_{10}, U_{20}, U_{01}, ... (2) с частотами p_{00}, p_{10}, p_{20}, p_{01}, ... соответственно, оператор плотности системы "передаваемый кутрит – проба Евы" будет иметь вид:

$$\rho^{(0)} = \sum_{i,j=0}^{2} p_{ij} |\psi_{ij}^{(0)}\rangle\langle\psi_{ij}^{(0)}|, \quad (12)$$

где

$$|\psi_{00}^{(0)}\rangle = U_{00}|\psi^{(0)}\rangle = \alpha_0|0\rangle|\varphi_{00}\rangle + \beta_0|1\rangle|\varphi_{01}\rangle + \gamma_0|2\rangle|\varphi_{02}\rangle,$$

$$|\psi_{10}^{(0)}\rangle = U_{10}|\psi^{(0)}\rangle = \alpha_0|0\rangle|\varphi_{00}\rangle + \beta_0 e^{2\pi i/3}|1\rangle|\varphi_{01}\rangle + \gamma_0 e^{4\pi i/3}|2\rangle|\varphi_{02}\rangle,$$

$$|\psi_{20}^{(0)}\rangle = U_{20}|\psi^{(0)}\rangle = \alpha_0|0\rangle|\varphi_{00}\rangle + \beta_0 e^{4\pi i/3}|1\rangle|\varphi_{01}\rangle + \gamma_0 e^{2\pi i/3}|2\rangle|\varphi_{02}\rangle,$$

$$|\psi_{01}^{(0)}\rangle = U_{20}|\psi^{(0)}\rangle = \alpha_0|1\rangle|\varphi_{00}\rangle + \beta_0|2\rangle|\varphi_{01}\rangle + \gamma_0|0\rangle|\varphi_{02}\rangle,$$

$$|\psi_{11}^{(0)}\rangle = U_{11}|\psi^{(0)}\rangle = \alpha_0|1\rangle|\varphi_{00}\rangle + \beta_0 e^{2\pi i/3}|2\rangle|\varphi_{01}\rangle + \gamma_0 e^{4\pi i/3}|0\rangle|\varphi_{02}\rangle,$$

$$|\psi_{21}^{(0)}\rangle = U_{21}|\psi^{(0)}\rangle = \alpha_0|1\rangle|\varphi_{00}\rangle + \beta_0 e^{4\pi i/3}|2\rangle|\varphi_{01}\rangle + \gamma_0 e^{2\pi i/3}|0\rangle|\varphi_{02}\rangle,$$

$$|\psi_{02}^{(0)}\rangle = U_{02}|\psi^{(0)}\rangle = \alpha_0|2\rangle|\varphi_{00}\rangle + \beta_0|0\rangle|\varphi_{01}\rangle + \gamma_0|1\rangle|\varphi_{02}\rangle,$$

$$|\psi_{12}^{(0)}\rangle = U_{12}|\psi^{(0)}\rangle = \alpha_0|2\rangle|\varphi_{00}\rangle + \beta_0 e^{2\pi i/3}|0\rangle|\varphi_{01}\rangle + \gamma_0 e^{4\pi i/3}|1\rangle|\varphi_{02}\rangle,$$

$$|\psi_{22}^{(0)}\rangle = U_{12}|\psi^{(0)}\rangle = \alpha_0|2\rangle|\varphi_{00}\rangle + \beta_0 e^{4\pi i/3}|0\rangle|\varphi_{01}\rangle + \gamma_0 e^{2\pi i/3}|1\rangle|\varphi_{02}\rangle. \quad (13)$$

Максимальная классическая информация I_0, которая доступна Еве после измерения над составной системой "передаваемый кутрит – проба", определяется энтропией Холево [14]:

$$I_0 = S(\rho^{(0)}) - \sum_{i,j=0}^{2} p_{ij} S(\rho_{ij}^{(0)}) = S(\rho^{(0)}), \quad (14)$$

где $\rho_{ij}^{(0)} = |\psi_{ij}^{(0)}\rangle\langle\psi_{ij}^{(0)}|$; S – энтропия фон Неймана и все $S(\rho_{ij}^{(0)})$ равны нулю, так как состояния (13) при выполнении условий (10) – чистые. Таким образом,

$$I_0 = S(\rho^{(0)}) \equiv -\mathrm{Tr}\{\rho^{(0)} \log_3 \rho^{(0)}\} = -\sum_i \lambda_i \log_3 \lambda_i \ \text{(трит)}, \quad (15)$$

где λ_i – собственные значения оператора плотности $\rho^{(0)}$ (12).

Величина I_0 показывает, сколько информации может получить Ева после финального измерения над составной системой "передаваемый кутрит – проба".

Для нахождения собственных значений λ_i оператора плотности $\rho^{(0)}$ (12), этот оператор был записан в матричном виде в следующем ортогональном базисе:

$$\{|0,\varphi_{00}\rangle, |1,\varphi_{00}\rangle, |2,\varphi_{00}\rangle, |0,\varphi_{01}\rangle, |1,\varphi_{01}\rangle, |2,\varphi_{01}\rangle, |0,\varphi_{02}\rangle, |1,\varphi_{02}\rangle, |2,\varphi_{02}\rangle\}. \quad (16)$$

Полученная матрица имеет размер 9×9 и здесь не приводится ввиду ее громоздкости.

С помощью инструментария символьных вычислений программы Mathematica 7 было найдено, что уравнение на собственные значения для этой матрицы плотности может быть разложено на произведение трех кубических уравнений следующего вида:

$$\lambda^3-(p_{00}+p_{10}+p_{20})\lambda^2+3\left(|\alpha_0|^2|\beta_0|^2+|\alpha_0|^2|\gamma_0|^2+|\beta_0|^2|\gamma_0|^2\right)\times$$

$$\times(p_{00}p_{10}+p_{00}p_{20}+p_{10}p_{20})\lambda-27|\alpha_0|^2|\beta_0|^2|\gamma_0|^2p_{00}p_{10}p_{20}=0;$$

$$\lambda^3-(p_{01}+p_{11}+p_{21})\lambda^2+3\left(|\alpha_0|^2|\beta_0|^2+|\alpha_0|^2|\gamma_0|^2+|\beta_0|^2|\gamma_0|^2\right)\times$$

$$\times(p_{01}p_{11}+p_{01}p_{21}+p_{11}p_{21})\lambda-27|\alpha_0|^2|\beta_0|^2|\gamma_0|^2p_{01}p_{11}p_{21}=0;$$

$$\lambda^3-(p_{02}+p_{12}+p_{22})\lambda^2+3\left(|\alpha_0|^2|\beta_0|^2+|\alpha_0|^2|\gamma_0|^2+|\beta_0|^2|\gamma_0|^2\right)\times$$

$$\times(p_{02}p_{12}+p_{02}p_{22}+p_{12}p_{22})\lambda-27|\alpha_0|^2|\beta_0|^2|\gamma_0|^2p_{02}p_{12}p_{22}=0\ .(17)$$

Аналогичным образом рассматриваются остальные случаи в (8), т. е. когда Боб вместо $|0\rangle$ "посылает $|1\rangle$ или $|2\rangle$". В этих случаях собственные значения матриц плотности $\rho^{(1)}$ и $\rho^{(2)}$, с учетом соотношений (11), определяются теми же уравнениями (17).

Как следует из первого выражения в (8), в случае, когда Боб "посылает $|0\rangle$" и в режиме контроля подслушивания используется измерительный базис z, вероятность обнаружить атаку

$$d_z=|\beta_0|^2+|\gamma_0|^2=1-|\alpha_0|^2. \qquad (18)$$

Аналогично, если Боб "посылает $|1\rangle$ или $|2\rangle$", то

$$d_z=|\alpha_1|^2+|\gamma_1|^2=1-|\beta_1|^2=1-|\alpha_0|^2\ ,$$

$$d_z=|\alpha_2|^2+|\beta_2|^2=1-|\gamma_2|^2=1-|\alpha_0|^2 \qquad (19)$$

соответственно, с учетом соотношений (11). Таким образом, общее выражение для вероятности обнаружения атаки при использовании в режиме контроля подслушивания z-базиса имеет вид (18).

Используя соотношение (18), из уравнений (17) можно для случая симметричной атаки Евы ($|\beta_0|^2=|\gamma_0|^2=d_z/2$) исключить параметры проб α_0, β_0 и γ_0, введя в уравнения (17) вероятность обнаружения атаки d_z. Это позволит в конечном итоге выразить количество информации Евы I_0 (15) через d_z.

Так как при симметричной атаке

$$|\alpha_0|^2|\beta_0|^2=|\alpha_0|^2|\gamma_0|^2=(1-d_z)\frac{d_z}{2}\ ,\quad |\beta_0|^2|\gamma_0|^2=\frac{d_z^2}{4}$$

и $|\alpha_0|^2|\beta_0|^2|\gamma_0|^2=(1-d_z)\frac{d_z^2}{4}$,

то уравнения (17) принимают вид:

$$\lambda^3-(p_{00}+p_{10}+p_{20})\lambda^2+3\left(d_z-\frac{3}{4}d_z^2\right)(p_{00}p_{10}+p_{00}p_{20}+p_{10}p_{20})\lambda-$$

$$-\frac{27}{4}(d_z^2-d_z^3)p_{00}p_{10}p_{20}=0;$$

$$\lambda^3-(p_{01}+p_{11}+p_{21})\lambda^2+3\left(d_z-\frac{3}{4}d_z^2\right)(p_{01}p_{11}+p_{01}p_{21}+p_{11}p_{21})\lambda-$$

$$-\frac{27}{4}(d_z^2-d_z^3)p_{01}p_{11}p_{21}=0;$$

$$\lambda^3-(p_{02}+p_{12}+p_{22})\lambda^2+3\left(d_z-\frac{3}{4}d_z^2\right)(p_{02}p_{12}+p_{02}p_{22}+p_{12}p_{22})\lambda-$$

$$-\frac{27}{4}(d_z^2-d_z^3)p_{02}p_{12}p_{22}=0\ . \qquad (20)$$

На рис. 2 приведены зависимости I_0 от d_z при симметричной атаке Евы и различных значениях частот $p_{00}\ldots p_{22}$ кодирующих операций Алисы (табл. 1). Для получения этих зависимостей уравнения (20) решались численно при определенных значениях $p_{00}\ldots p_{22}$ и полученные девять значений $\lambda_1\ldots\lambda_9$ подставлялись в (15).

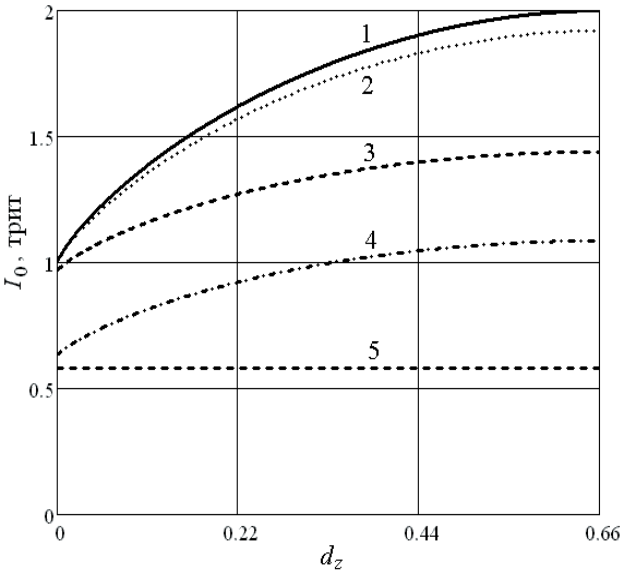

Рис. 2. Зависимость количества информации Евы I_0 от вероятности d_z обнаружения атаки при симметричной атаке

Таблица 1

Частоты $p_{00}\ldots p_{22}$ троичных биграмм и соответствующая энтропия источника $H=-\sum_{i,j=0}^{2}p_{ij}\log_3 p_{ij}$ (трит/биграмму)

№ кривой на рис. 2	p_{00}	p_{10}	p_{20}	p_{01}	p_{11}	p_{21}	p_{02}	p_{12}	p_{22}	H
1	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	1/9	2.000
2	1/6	1/9	1/18	1/6	1/18	1/9	1/18	1/9	1/6	1.921
3	2/9	0	2/9	0	2/9	0	2/9	0	1/9	1.439
4	0.4	0.1	0	0	0.4	0.1	0	0	0	1.086
5	2/3	0	0	0	1/3	0	0	0	0	0.579

Как видно из рис. 2, для большинства наборов $p_{00}\ldots p_{22}$ количество информации Евы I_0 монотонно возрастает с ростом вероятности обнаружения атаки d_z и достигает максимума при $d_z=2/3$. Это значение d_z можно считать максимальным, так как при $d_z>2/3$ количество информации Евы начинает убывать (на графиках не показано). Соответственно, Ева не будет выбирать параметры своих проб, от которых зависит d_z, так, чтобы d_z превышало 2/3 – для Евы не имеет

смысла увеличивать вероятность обнаружения атаки при уменьшении доступной ей информации. Также из рис. 2 видно, что максимум количества информации I_0 Евы, соответствующий $d_z = 2/3$, равен энтропии источника при любых значениях частот $p_{00} \ldots p_{22}$. Это означает, что при $d_z = 2/3$ и только при таком значении d_z Ева получит полную информацию (при симметричной атаке). Также факт равенства I_0 и H при $d_z = 2/3$ свидетельствует о правильной асимптотике формул (20).

Из рис. 2. видно также, что при $d_z = 0$ количество информации Евы не равно нулю, однако оно ниже своего максимального значения при $d_z = 2/3$. Таким образом, для пинг – понг протокола с перепутанными парами кутритов существует "невидимый" режим подслушивания, при котором Ева получает частичную информацию, но ее операции не могут быть обнаружены легитимными пользователями, когда они используют в режиме контроля подслушивания только один измерительный базис. Отметим, что аналогичная ситуация имеет место и для пинг – понг протокола с перепутанными группами кубитов [3,5]. Поэтому необходимо рассмотреть вероятности обнаружения атаки при использовании легитимными пользователями в режиме контроля подслушивания остальных базисов (4) – (6), а также зависимости между этими вероятностями.

4. Вероятности обнаружения атаки при использовании легитимными пользователями x- v- и t-базиса, сравнение стойкости протоколов с кутритами и кубитами

Рассмотрим атаку Евы, считая, что в силу полной смешанности состояния передаваемого кутрита он теперь находится в одном из состояний $|x_0\rangle$, $|x_1\rangle$ или $|x_2\rangle$ (4). Тогда формулы (8) заменяются на следующие:

$$\left|\psi_x^{(0)}\right\rangle = E|x_0,\varphi\rangle = a_0|x_0,\varphi_{00}\rangle + b_0|x_1,\varphi_{01}\rangle + c_0|x_2,\varphi_{02}\rangle;$$

$$\left|\psi_x^{(1)}\right\rangle = E|x_1,\varphi\rangle = a_1|x_0,\varphi_{10}\rangle + b_1|x_1,\varphi_{11}\rangle + c_1|x_2,\varphi_{12}\rangle;$$

$$\left|\psi_x^{(2)}\right\rangle = E|x_2,\varphi\rangle = a_2|x_0,\varphi_{20}\rangle + b_2|x_1,\varphi_{21}\rangle + c_2|x_2,\varphi_{22}\rangle. \quad (21)$$

Далее, все формулы (9) – (17) остаются справедливыми при замене $\alpha_0 \to a_0$, $\beta_0 \to b_0$, $\gamma_0 \to c_0$, $\alpha_1 \to a_1$, $\beta_1 \to b_1$ и т. д.

Таким образом, выражение (18) переходит в выражение

$$d_x = |b_0|^2 + |c_0|^2 = 1 - |a_0|^2. \quad (22)$$

Используя (8) и (21), можно получить следующие выражения, связывающие параметры α_0, β_0 и γ_0 с параметрами a_0, b_0 и c_0:

$$|\alpha_0|^2 = \frac{1}{3}|a_0 + b_0 + c_0|^2,\ |\beta_0|^2 = \frac{1}{3}|a_0 + e^{2\pi i/3}b_0 + e^{-2\pi i/3}c_0|^2,$$

$$|\gamma_0|^2 = \frac{1}{3}|a_0 + e^{-2\pi i/3}b_0 + e^{2\pi i/3}c_0|^2. \quad (23)$$

В табл. 2 приведены несколько рассчитанных наборов параметров a_0, b_0 и c_0, удовлетворяющих соотношениям, аналогичным (10) и (11), а также соответствующие этим наборам параметров значения d_x и d_z. Значения d_z получены с использованием (18) и первой формулы в (23).

Таблица 2

Параметры атакующей операции и соответствующие им значения d_x и d_z

a_0	b_0	c_0	d_x	d_z
Несимметричная атака: $\|b_0\|^2 \neq \|c_0\|^2$				
-0.910684	0.244017	-0.333333	0.170655	0.666667
-0.807162	0.309719	-0.502558	0.348490	0.666667
-0.709081	0.331451	-0.622370	0.497204	0.666667
-0.666667	0.333333	-0.666667	0.555556	0.666667
-0.577406	0.325969	-0.748563	0.666603	0.666667
0.530210 - 0.8i	0.169304 - 0.1i	0.014630 + 0.2i	0.078878	0.666667
-0.909127 + 0.1i	-0.133042 - 0.2i	0.125653 - 0.3i	0.163489	0.666667
0.204236 + 0.83i	0.026660 - 0.3i	0.136663 + 0.4i	0.269388	0.666667
0.737034 + 0.3i	-0.031581 - 0.5i	0.160573 - 0.3i	0.366781	0.666667
0.674712 + 0.3i	0.525520 + 0.2i	-0.220436 - 0.3i	0.454764	0.666667
-0.531662 + 0.3i	0.463325 + 0.2i	-0.531662 + 0.3i	0.627335	0.666667
-0.497557+0.293i	0.459068 + 0.2i	-0.570890 + 0.3i	0.666667	0.666667
Симметричная атака: $\|b_0\|^2 = \|c_0\|^2$				
-0.953939 + 0.1i	-0.2i	-0.2i	0.08	0.666667
0.305505 + 0.8i	0.305505 - 0.2i	0.305505 - 0.2i	0.266667	0.666667
0.027387 + 0.7i	0.463276 - 0.2i	0.463276 - 0.2i	0.50925	0.666667
0.577350	-0.288675 +0.5i	-0.288675 + 0.5i	0.666667	0.666667
0.577350i	0.5 - 0.288675i	0.5 - 0.288675i	0.666667	0.666667
0.577350	0.288675 + 0.5i	0.288675 + 0.5i	0.666667	0.222222

Как показывают расчеты, условие унитарности атакующей операции Евы приводит к важной зависимости между d_z и d_x, а именно: вне зависимости от значения одной из этих величин вторая всегда равна своему максимальному значению (см. табл. 2). Таким образом, при использовании двух измерительных базисов в режиме контроля подслушивания "невидимого" режима подслушивания уже не существует и пинг – понг протокол с белловскими парами перепутанных кутритов обладает асимптотической безопасностью, аналогично протоколам с группами перепутанных кубитов [3, 5].

Аналогичным образом атака может быть проанализирована для случаев использования легитимными пользователями v-базиса (5) и t-базиса (6). Расчеты показывают, что вышеприведенное правило для d_z и d_x справедливо для любой из пар $d_z - d_x$, $d_z - d_v$, $d_z - d_t$, $d_x - d_v$, $d_x - d_t$, $d_v - d_t$: вне зависимости от значения одной их этих величин вторая всегда равна своему максимальному значению.

Отсюда следует, что для обнаружения подслушивания легитимным пользователям достаточно выбрать два любых взаимно несмещенных базиса из четырех возможных (3) – (6) и нет необходимости использовать в режиме контроля подслушивания три или четыре базиса – это не увеличит вероятности обнаружения атаки.

При использовании в режиме контроля подслушивания двух измерительных базисов (например, z и x) вероятность обнаружить атакующую операцию Евы:

$$d = q_z d_z + q_x d_x, \qquad (24)$$

где q_z и q_x – вероятности использования Алисой и Бобом z- и x-базисов соответственно ($q_z + q_x = 1$). Наименьшие значения d_z и d_x равны нулю, но когда одна из этих величин равна нулю, другая равна своему максимальному значению $2/3$. Поскольку легитимные пользователи не знают заранее, какую стратегию атаки выберет Ева, т.е. в каком из базисов она будет стремиться создать меньшее значение вероятности обнаружения, то значения q_z и q_x разумно будет выбрать равными друг другу, т.е. $q_z = q_x = 1/2$. Тогда наименьшее значение d получится, когда либо $d_z = 0$ и $d_x = 2/3$, либо наоборот. Согласно (24), при таких условиях $d = (1/2)\cdot(2/3) = 1/3$, т.е. минимальное значение вероятности обнаружения атаки при использовании в режиме контроля подслушивания двух измерительных базисов (с равными вероятностями) равно $1/3$.

Отметим, что при такой стратегии Ева получит лишь частичную информацию о переданной строке тритов. Если же Ева захочет получить всю информацию, то она должна будет так выбрать параметры своих проб, чтобы $d_z = d_x = 2/3$ и при этом, согласно (24), $d = 2/3$.

Сравним теперь зависимости количества информации Евы от вероятности обнаружения атаки для протокола с белловскими парами кутритов и протоколов с группами кубитов. На рис. 3 показаны зависимости I_0 от d_z для протокола с парами кутритов при $p_{00} = \ldots = p_{22} = 1/9$, а также для протокола с парами кубитов и квантовым сверхплотным кодированием [3], протокола с ГХЦ – триплетами [5] и протокола с ГХЦ – четверками кубитов [15] при одинаковых значениях частот кодирующих операций Алисы. Видно, что кривая $I_0(d_z)$ для протокола с кутритами лежит близко к соответствующей кривой для протокола с ГХЦ – триплетами кубитов. При этом информационные емкости этих двух вариантов пинг – понг протокола также близки: 3.17 бита на цикл для протокола с парами кутритов и 3 бита на цикл для протокола с ГХЦ – триплетами кубитов.

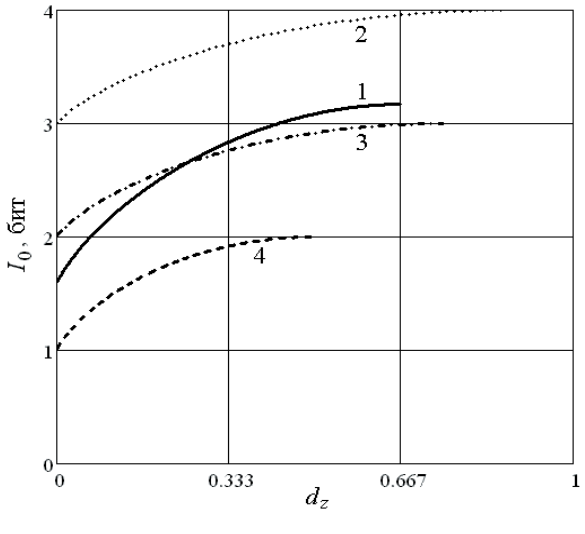

Рис. 3. Зависимости количества информации Евы от вероятности обнаружения атаки.
Протокол: с белловскими парами кутритов (1); с ГХЦ – четверками кубитов (2); с ГХЦ – триплетами кубитов (3); с белловскими парами кубитов (4)

В табл. 3 приведены минимальные и максимальные значения вероятности обнаружения атаки для этих четырех вариантов пинг – понг протокола при использовании в режиме контроля подслушивания двух измерительных базисов с одинаковыми вероятностями $q_z = q_x = 1/2$. Как видно из табл. 3, значения d_{min} и d_{max} для протокола с белловскими парами кутритов также наиболее близки к соответствующим значениям для протокола с ГХЦ – триплетами кубитов.

Таблица 3

Минимальные d_{min} и максимальные d_{max} значения вероятности обнаружения атаки при использовании в режиме контроля подслушивания двух измерительных базисов с одинаковыми вероятностями

Протокол	d_{min}	d_{max}
с белловским парами кутритов	1/3	2/3
с белловскими парами кубитов	1/4	1/2
с ГХЦ – триплетами кубитов	3/8	3/4
с ГХЦ – четверками кубитов	7/16	7/8

5. Выводы

В работе впервые проанализирована атака пассивного перехвата на пинг– понг протокол с белловскими парами трехмерных квантовых систем – кутритов. Получена матрица плотности составной квантовой системы "передаваемый кутрит – проба подслушивающего агента" и вычислением собственных значений матрицы плотности получено выражение для количества информации подслушивающего агента как функции от вероятности обнаружения атаки.

Показано, что при использовании для реализации протокола белловских пар кутритов вместо белловских пар кубитов увеличивается не только информационная емкость, но и уровень стойкости протокола к атаке, так как максимальная вероятность обнаружения подслушивания (при однократном контроле подслушивания) для протокола с кутритами равна $2/3$, а для протокола с кубитами – $1/2$. Стойкость протокола с парами кутритов оказывается приблизительно такой же, как протокола с ГХЦ – триплетами кубитов. При этом для протокола с парами кутритов, аналогично протоколам с группами кубитов, существует "невидимый" режим подслушивания, если легитимные пользователи используют в режиме контроля подслушивания только один измерительный базис. Использование второго измерительного базиса устраняет возможность необнаружимой атаки и, следовательно, является необходимым.

При использовании в режиме контроля подслушивания двух измерительных базисов пинг – понг протокол с белловскими парами кутритов, опять таки аналогично протоколам с группами кубитов, обладает только асимптотической безопасностью, так как для обнаружения подслушивания с вероятностью, сколь угодно близкой к единице, легитимным пользователям необходимо выполнить некоторое количество раундов

контроля подслушивания. При этом, так как режим контроля подслушивания необходимо чередовать с режимом передачи сообщения (иначе подслушивающий агент вообще не будет производить атакующих операций, так как будет знать, что сообщение не передается), то некоторое количество информации будет попадать к подслушивающему агенту. Оценка этого количества в зависимости от параметров протокола и стратегии подслушивания, а также необходимые меры по усилению безопасности пинг – понг протокола с кутритами, будут предметом следующих работ.

Литература

1. Boström K., Felbinger T. Deterministic secure direct communication using entanglement // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.
2. Cai Q.-Y., Li B.-W. Improving the capacity of the Boström-Felbinger protocol // Physical Review A. – 2004. – V. 69, № 5. – 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., Василиу Л.Н. Пинг – понг протокол с трех– и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера // Труды Одесского политехнического университета. – 2008. – Вып. 1 (29). – С. 171 – 176.
5. Василиу Е.В. Стойкость пинг-понг протокола с триплетами Гринбергера – Хорна – Цайлингера к атаке с использованием вспомогательных квантовых систем // Информатика: Объединенный институт проблем информатики НАН Беларуси. – 2009, № 1 (21). – С. 117 – 128.
6. Василиу Е.В., Василиу Л.Н. Анализ асимптотической безопасности трех вариантов пинг – понг протокола квантовой безопасной связи // Современный научный вестник. – Белгород: "Руснаучкнига". – 2009, № 3 (59). – С. 74 – 80.
   http://www.rusnauka.com/10_NPE_2008/Informatica/303-17.doc.htm
7. Zhang Zh.-J., Li Y., Man Zh.-X. Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss // Physics Letters A. – 2005. – V. 341, № 5–6. – P. 385 – 389.
8. Cai Q.-Y. The «ping-pong» protocol can be attacked without eavesdropping // Physical Review Letters. – 2003. – V. 91, № 10. – 109801.
9. Boström K., Felbinger T. On the security of the ping-pong protocol // Physics Letters A. – 2008. – V. 372, № 22. – P. 3953 – 3956.
10. Thew T., Acin A., Zbinden H., Gisin N. Experimental realization of entangled qutrits for quantum communication // Quantum Information and Computation. – 2004. – V. 4, № 2. – P. 93 – 101.
11. Vaziri A., Pan J., Jennewein T., Weihs G., Zeilinger A. Concentration of higher dimensional entanglement: qutrits of photon orbital angular momentum // Physical Review Letters. – 2003. – V. 91, № 22. – 227902.
12. Wang Ch., Deng F.-G., Li Y.-S., Liu X.-S., Long G. L. Quantum secure direct communication with high dimension quantum superdense coding // Physical Review A. – 2005. – V. 71, № 4. – 044305.
13. Stinespring W.F. Positive functions on C*-algebras // Proceedings of the American Mathematical Society. – 1955. – V. 6. – P. 211 – 216.
14. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. – М.: Мир, 2006. – 824 с.
15. Васіліу Є., Ніколаєнко С. Підсилення безпеки пінг – понг протоколу квантового безпечного зв'язку з n-кубітними ГХЦ – станами // Комп'ютерні науки та інженерія: Матеріали III Міжнародної конференції молодих вчених CSE-2009. – Львів: Видавництво Національного університету "Львівська політехніка", 2009. – С. 299 – 301.