УДК 003.26:621.39+530.145

Мамедов Р.С.

ПИНГ-ПОНГ ПРОТОКОЛ КВАНТОВОЙ БЕЗОПАСНОЙ СВЯЗИ С ЧЕТЫРЕХКУБИТНЫМИ ПЕРЕПУТАННЫМИ W-СОСТОЯНИЯМИ

Разработан новый пинг-понг протокол квантовой прямой безопасной связи с использованием перепутанных четырехкубитных W-состояний. Проанализированы два вида атак пассивного перехвата на протокол. Разработан метод модификации режима контроля подслушивания для обнаружения атаки "перехвата – повторной посылки" кубитов. Показано, что характеристики протокола с четырехкубитными W-состояниями практически совпадают с характеристиками протокола с трехкубитными GHZ-состояниями. Показано, что пинг-понг протокол с четырехкубитными W-состояниями не имеет преимуществ по сравнению с другими протоколами с четырехкубитными состояниями, которые исследованы к настоящему времени, и наилучшим из пинг-понг протоколов с четырехкубитными состояниями по критериям стойкости и эффективности является протокол с кластерными состояниями.

Ключевые слова: квантовые технологии защиты информации, квантовая безопасная связь, пинг-понг протокол, четырехкубитные перепутанные состояния, атака пассивного перехвата, криптостойкость протокола.

Введение. Квантовое перепутывание является одним из основных статических ресурсов квантовой информатики и главным элементом многих квантовых вычислительных и коммуникационных протоколов [1]. В частности, большинство квантовых протоколов прямой безопасной связи, позволяющих напрямую, т.е. без шифрования, передавать конфиденциальные сообщения, используют перепутанные квантовые состояния групп кубитов или кудитов [2].

Свойства двухкубитных подлинно перепутанных состояний (состояний Белла) к настоящему времени хорошо изучены, также достаточно хорошо изучена стойкость к различным атакам протоколов квантовой безопасной связи, использующих эти состояния [3–5]. Подлинное перепутывание означает, что соответствующее состояние не может быть записано, как тензорное произведение состояний меньшего числа кубитов [1]. Для трех кубитов существует шесть различных типов перепутанных состояний, из которых два – подлинно перепутанные, это трехкубитные состояния Вернера (W-состояния) и состояния Гринбергера–Хорна–Цайлингера (GHZ-состояния). Для четырех кубитов имеется, по крайней мере, девять различных типов перепутанных состояний, некоторые их которых являются подлинно перепутанными, но их свойства изучены пока далеко не полностью [6]. Поскольку увеличение числа кубитов в перепутанном состоянии позволяет увеличить информационную емкость протокола, а использование квантового сверхплотного кодирования позволяет уменьшить уровень ошибок при передаче, то разработка новых квантовых коммуникационных протоколов с использованием многокубитного перепутывания и квантового сверхплотного кодирования является важной и актуальной научной задачей.

К настоящему времени предложены различные протоколы квантовой безопасной связи, использующие многокубитные перепутанные состояния [2–5, 7–16]. Эти протоколы можно разделить на два класса – протоколы с использованием одного перепутанного состояния на один цикл протокола и протоколы с передачей кубитов из разных (идентичных) перепутанных состояний большими блоками. Размер этих блоков должен значительно превышать размер самого сообщения. К первому классу относятся различные варианты пинг-понг протокола, недостатком которых является асимптотическая стойкость к атаке пассивного перехвата, а достоинством – отсутствие необходимости в использовании квантовой памяти большого объема [2,3,5,11–15]. Протоколы с передачей кубитов блоками обладают более высокой стойкостью, чем пинг-понг протоколы, но требуют для своей реализации большой квантовой памяти [4,7–10,16]. Работы по созданию квантовой памяти активно ведутся в настоящее время, но такая память, пригодная для массового технологического использования, пока не создана.

Как известно, из двух типов трехкубитных подлинно перепутанных состояний для реализации сверхплотного кодирования лучше использовать GHZ-состояния: с их помощью можно передать три бита классической информации, передавая по каналу связи два кубита, в то время как с помощью W-состояний, используя сверхплотное кодирование, можно

передать только один бит [6]. Поэтому трехкубитные W-состояния почти не используются в квантовых коммуникационных протоколах.

Что касается четырехкубитных истинно перепутанных состояний, то лучшим ресурсом для квантового сверхплотного кодирования являются кластерные (Ω) состояния [6] и χ-состояния [17], с использованием которых можно передать четыре бита информации, передавая по каналу два кубита. Другие четырехкубитные перепутанные состояния позволяют передать меньше битов при том же количестве передаваемых кубитов [6], однако, разработка и анализ стойкости протоколов с использованием таких состояний также представляют интерес с точки зрения нахождения оптимального протокола не только по критерию эффективности, но и по критерию стойкости.

Пинг-понг протоколы с четырехкубитными кластерными и GHZ-состояниями разработаны в [11] и [12] соответственно, также проанализирована стойкость этих протоколов до атаки пассивного перехвата [13,14]. **Цель** настоящей работы – разработка методов кодирования информации и контроля подслушивания (пассивного перехвата) для пинг-понг протокола с четырехкубитными W-состояниями, а также детальный анализ двух видов атак перехвата информации на этот протокол.

Пинг-понг протокол с четырехкубитными W-состояниями. Существуют восемь ортонормированных перепутанных четырехкубитных W-состояний:

$$W_1 = \left(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle\right)/2; \quad W_2 = \left(-|0001\rangle - |0010\rangle + |0100\rangle + |1000\rangle\right)/2;$$
$$W_3 = \left(|0011\rangle + |0000\rangle + |0110\rangle + |1010\rangle\right)/2; \quad W_4 = \left(|0011\rangle + |0000\rangle - |0110\rangle - |1010\rangle\right)/2;$$
$$W_5 = \left(|0000\rangle - |0011\rangle + |0101\rangle + |1001\rangle\right)/2; \quad W_6 = \left(|0000\rangle - |0011\rangle - |0101\rangle - |1001\rangle\right)/2;$$
$$W_7 = \left(|0010\rangle - |0001\rangle - |0111\rangle - |1011\rangle\right)/2; \quad W_8 = \left(-|0010\rangle + |0001\rangle - |0111\rangle - |1011\rangle\right)/2, \quad (1)$$

где $|0\rangle$ та $|1\rangle$ – базисные состояния одного кубита, образующие так называемый *z*-базис и соответствующие, например, вертикальной и горизонтальной поляризациям фотона.

Восемь состояний (1) образуют базис в подпространстве гильбертова пространства четырех кубитов и, следовательно, могут быть точно отличены друг от друга измерением в таком базисе. Соответствующие восемь операторов проективных измерений имеют вид $P_i = |W_i\rangle\langle W_i|$ (i=1,…,8). Таким образом, используя состояния (1) можно передать 3 бита информации за один цикл протокола, в отличие от четырехкубитных кластерных состояний, а также четырехкубитных GHZ-состояний, где за один цикл передается 4 бита [11,12].

Состояния (1) могут быть преобразованы одно в другое действием локальных унитарных операторов (операторов Паули) на *два* любых кубита из четырех [6]. Отметим, что 16 кластерных четырехкубитных состояний также преобразуются друг в друга действием операторов Паули на два кубита [11], а 16 GHZ-состояний – действием на три кубита [12]. Таким образом, используя квантовое сверхплотное кодирование, в пинг-понг протоколе с четырехкубитными W-состояниями по квантовому каналу нужно передавать два кубита на каждом цикле протокола, как и в протоколе с четырехкубитными кластерными состояниями. Следовательно, стойкость этих двух протоколов к естественным помехам в канале будет одинакова и выше стойкости протокола с четырехкубитными GHZ-состояниями.

Первым этапом разработки нового протокола квантовой прямой безопасной связи, в данном случае нового пинг-понг протокола, является разработка метода квантового кодирования классической информации, т.е. нахождения множества локальных унитарных операторов, преобразующих одно из состояний (1), например $|W_1\rangle$, в остальные семь. Затем каждому из состояний (1) ставится в соответствие четырехбитовая строка. Разумеется, последняя операция является произвольной, и ее могут выполнять каждый раз сами участники протокола.

Найденное множество кодирующих операций, в которых операторы Паули $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$, $\sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$ и $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$ действуют только на третий и четвертый кубиты (на первый и второй действует тождественный оператор $I = |0\rangle\langle 0| + |1\rangle\langle 1|$), приведено в табл. 1.

Схема пинг-понг протокола с четырехкубитными W-состояниями аналогична схемам других пинг-понг протоколов [3,5,11,12,15]. Боб (принимающая сообщение сторона) готовит состояние $|W_1\rangle = \big(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle\big)/2$. Он оставляет у себя первые два кубита ("домашние кубиты") и посылает третий и четвертый ("передаваемые кубиты") Алисе (передающая сторона) по квантовому каналу связи. Алиса случайным образом переключается между двумя режимами протокола: *режимом передачи сообщения* и *режимом контроля подслушивания*.

Таблица 1

Метод квантового кодирования информации для пинг-понг протокола с четырехкубитными W-состояниями

i	Состояние $\lvert W_i\rangle$	Оператор U_{ijk}, преобразующий $\lvert W_1\rangle \to \lvert W_i\rangle$	Битовая строка, соответств. $\lvert W_i\rangle$
1	$\big(\lvert 0001\rangle + \lvert 0010\rangle + \lvert 0100\rangle + \lvert 1000\rangle\big)/2$	$U_{000} = I \otimes I \otimes I \otimes I$	000
2	$\big(-\lvert 0001\rangle - \lvert 0010\rangle + \lvert 0100\rangle + \lvert 1000\rangle\big)/2$	$U_{001} = I \otimes I \otimes \sigma_z \otimes \sigma_z$	001
3	$\big(\lvert 0011\rangle + \lvert 0000\rangle + \lvert 0110\rangle + \lvert 1010\rangle\big)/2$	$U_{010} = I \otimes I \otimes \sigma_x \otimes I$	010
4	$\big(\lvert 0011\rangle + \lvert 0000\rangle - \lvert 0110\rangle - \lvert 1010\rangle\big)/2$	$U_{011} = I \otimes I \otimes i\sigma_y \otimes \sigma_z$	011
5	$\big(\lvert 0000\rangle - \lvert 0011\rangle + \lvert 0101\rangle + \lvert 1001\rangle\big)/2$	$U_{100} = I \otimes I \otimes \sigma_z \otimes \sigma_x$	100
6	$\big(\lvert 0000\rangle - \lvert 0011\rangle - \lvert 0101\rangle - \lvert 1001\rangle\big)/2$	$U_{101} = I \otimes I \otimes I \otimes i\sigma_y$	101
7	$\big(\lvert 0010\rangle - \lvert 0001\rangle - \lvert 0111\rangle - \lvert 1011\rangle\big)/2$	$U_{110} = I \otimes I \otimes \sigma_x \otimes i\sigma_y$	110
8	$\big(-\lvert 0010\rangle + \lvert 0001\rangle - \lvert 0111\rangle - \lvert 1011\rangle\big)/2$	$U_{111} = I \otimes I \otimes i\sigma_y \otimes \sigma_x$	111

В режиме передачи сообщения Алиса выполняет кодирующую операцию над двумя полученными ею кубитами в соответствии со своей текущей трехбитовой строкой (см. табл. 1) и посылает эти кубиты обратно Бобу. Боб, получив кубиты от Алисы, выполняет измерение в четырехкубитном W-базисе и тем самым определяет состояние $|W_i\rangle$, созданное кодирующей операцией Алисы, а соответственно и посланные ею биты.

Аналогично другим пинг-понг протоколам [3–5, 13–15], злоумышленник (называемый по традиции Евой) может провести атаку пассивного перехвата информации, перепутывая свою вспомогательную квантовую систему (пробу) с передаваемыми кубитами на пути Боб $\to$ Алиса, а затем выполняя измерение над составной квантовой системой "передаваемые кубиты – проба" на пути Алиса $\to$ Боб. Для обнаружения этой атаки и необходим режим контроля подслушивания. В этом режиме легитимные стороны выполняют измерения над парами кубитов, образующими состояние $W_1 = \big(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle\big)/2$, после того, как Алиса получит третий и четвертый кубиты от Боба. Целью таких измерений является определить, сохранилось ли исходное, приготовленное Бобом четырехкубитное состояние W_1 после передачи третьего и четвертого кубитов по каналу от Боба к Алисе. Можно разработать несколько различных методов таких измерений для состояния W_1, однако для выполнения контроля подслушивания достаточно одного метода. Рассмотрим такой метод.

Алиса и Боб выполняют свои измерения в двухчастичных взаимно несмещенных базисах $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ и $\{|++\rangle,|+-\rangle,|-+\rangle,|--\rangle\}$, где $|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$ и $|-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$. Алиса выбирает один из этих базисов случайным образом. После своего измерения она сообщает Бобу по обычному открытому, но аутентифицированному каналу выбранный ею базис и полученный результат измерения. Аутентификация всех сообщений, которые передаются обычным каналом, необходима для предотвращения атаки "человек посредине". Потом Боб в том же базисе, что и Алиса, измеряет состояние своей пары кубитов. Результаты измерений Алисы и Боба по описанной схеме приведены в табл. 2.

Таким образом, легитимные пользователи должны выполнить некоторое количество раундов контроля подслушивания, достаточное для того, чтобы получить значимую статистику результатов своих измерений и определить уровень ошибок, сравнивая полученную статистику с вероятностями в табл. 2. Затем этот полученный уровень ошибок сравнивается с заранее известным уровнем естественных помех в квантовом канале. Если полученный уровень ошибок значительно превышает естественный, то это приписывается атаке Евы и протокол прерывается.

Таблица 2

Метод контроля подслушивания для пинг-понг протокола с четырехкубитными W-состояниями

Результат Алисы (кубиты 3,4)	Вероятн.	Результат Боба (кубиты 1,2)	Вероятн.	Результат Алисы (кубиты 3,4)	Вероятн.	Результат Боба (кубиты 1,2)	Вероятн.
Базис $\{\|00\rangle,\|01\rangle,\|10\rangle,\|11\rangle\}$				Базис $\{\|++\rangle,\|+-\rangle,\|-+\rangle,\|--\rangle\}$			
00	1/2	01	1/2	$++$	3/8	$++$	2/3
		10	1/2			$+-$	1/6
01	1/4	00	1			$-+$	1/6
10	1/4	00	1	$+-$	1/8	$++$	1/2
11	0	–	–			$--$	1/2
				$-+$	1/8	$++$	1/2
						$--$	1/2
				$--$	3/8	$--$	2/3
						$+-$	1/6
						$-+$	1/6

Анализ атаки "перехвата – повторной посылки" кубитов. Состояния пары кубитов, посылаемых в протоколе от Боба к Алисе и обратно, являются смешанным. Однако, в отличие от протокола с кластерными состояниями, эти состояния не полностью смешаны. Так, приведенная матрица плотности пары передаваемых кубитов, когда полное четырехкубитное состояние есть $|W_1\rangle$, имеет вид:

$$\rho_{3,4(|W_1\rangle)}=Tr_{1,2}(|W_1\rangle\langle W_1|)=\begin{pmatrix}0.5 & 0 & 0 & 0\\ 0 & 0.25 & 0 & 0\\ 0 & 0 & 0.25 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}, \quad (2)$$

когда состояния есть $|W_2\rangle$:

$$\rho_{3,4(|W_2\rangle)} = Tr_{1,2}\left(|W_2\rangle\langle W_2|\right) = \begin{pmatrix} 0.5 & 0 & 0 & 0 \\ 0 & 0.25 & 0 & 0 \\ 0 & 0 & 0.25 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (3)$$

а, например, когда состояние есть $|W_4\rangle$:

$$\rho_{3,4(|W_4\rangle)} = Tr_{1,2}\left(|W_4\rangle\langle W_4|\right) = \begin{pmatrix} 0.25 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0 \\ 0 & 0 & 0 & 0.25 \end{pmatrix}, \quad (4)$$

и т.д.

Таким образом, на протокол с четырехкубитными W-состояниями можно выполнить атаку, перехватывая два передаваемых кубита на пути Алиса $\rightarrow$ Боб, измеряя их состояния в базисе $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ и посылая Бобу два новых кубита в том состоянии, которое было получено в результате измерения. При этом Ева сможет получить только частичную информацию. Так, если в результате измерения Ева получает $|11\rangle$, то она может сделать вывод, что было послано одно из W-состояний, кроме $|W_1\rangle$ и $|W_2\rangle$. Если же в результате измерения получено $|01\rangle$, значит было послано любое состояние, кроме $|W_3\rangle$ и $|W_4\rangle$, и т.д.

Следует отметить, что при атаке "перехвата – повторной посылки" кубитов Ева полностью разрушает перепутанность "домашних" и "передаваемых" кубитов. Следовательно, измерения Боба становятся случайными и не зависящими от кодирующих операций Алисы. Поэтому Боб не получит никакой информации при такой атаке, т.е. Ева, кроме получения частичной информации о передаваемом сообщении, выполняет также атаку типа "отказ в обслуживании".

Обнаружить атаку "перехвата – повторной посылки" кубитов можно путем небольшой модификации метода контроля подслушивания, описанного в предыдущем разделе статьи. Часть кубитов в этом режиме Алиса должна не измерять, а отправлять назад Бобу. Боб, получив эти кубиты (вместе с сообщением от Алисы, что она не выполнила измерение), измеряет четырехкубитное состояние в W-базисе и определяет, сохранилось ли начальное перепутанное состояние $|W_1\rangle$, которое он приготовил. Расчеты показывают, что в случае атаки (в идеальном квантовом канале) вероятность неверного результата у Боба достаточно высока и равняется 0.625. Разумеется, в квантовом канале с шумом, легитимные пользователи должны выполнить некоторое количество таких измерений и сравнить полученный уровень ошибок с заранее известным уровнем естественных помех в канале. Как видно, в канале с невысоким уровнем естественных помех атака "перехвата – повторной посылки" кубитов будет легко обнаружена, и протокол должен быть прерван. Однако до этого Ева сможет получить некоторую информацию, и, следовательно, протокол нуждается в дополнительном методе увеличения его стойкости. Такой метод увеличения стойкости был разработан для защиты от атаки пассивного перехвата с использованием дополнительных квантовых систем пинг-понг протоколов в шумном канале [18]. Этот же метод пригоден и для защиты протокола от атаки "перехвата – повторной посылки" кубитов.

Анализ атаки пассивного перехвата с использованием дополнительных квантовых систем (проб). Схема атаки пассивного перехвата с использованием проб одинакова для всех вариантов пинг-понг протокола: Ева должна сначала выполнить атакующую операцию $\hat{E}$, перепутывая свою пробу с передаваемыми кубитами на пути Боб $\rightarrow$ Алиса, а после выполнения Алисой кодирующей операции, выполнить измерение над составной системой "передаваемые кубиты – проба".

Согласно теореме Стайнспринга [1], 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 $\dim H_B = 4$ – размерность гильбертова пространства передаваемых Бобом двух кубитов. Таким образом, Ева может использовать для атаки четырехкубитные пробы ($\dim H_E = 16$). Атака с использованием четырехкубитных проб будет наиболее общей. Проанализируем ее.

Состояние пары передаваемых Бобом кубитов определяется матрицей плотности (2). Таким образом, для анализа атаки можно считать, что Боб "посылает" кубиты в состоянии $|00\rangle$ с вероятностью 1/2, $|01\rangle$ с вероятностью 1/4 или $|10\rangle$ также с вероятностью 1/4. Будем пока считать для удобства, что Боб также "посылает" $|11\rangle$, а потом исключим этот случай из анализа, т.е. положим, что Боб "посылает" $|11\rangle$ с нулевой вероятностью.

Состояния составной системы "передаваемые кубиты – проба Евы" после перепутывающей операции $\hat{E}$ могут быть записаны в виде:

$$
\begin{aligned}
|\psi^{(1)}\rangle &= \mathrm{E}|00,\phi\rangle = \alpha_1|00,\phi_{0000}\rangle + \beta_1|01,\phi_{0001}\rangle + \gamma_1|10,\phi_{0010}\rangle + \delta_1|11,\phi_{0011}\rangle;\\
|\psi^{(2)}\rangle &= \mathrm{E}|01,\phi\rangle = \alpha_2|00,\phi_{0100}\rangle + \beta_2|01,\phi_{0101}\rangle + \gamma_2|10,\phi_{0110}\rangle + \delta_2|11,\phi_{0111}\rangle;\\
|\psi^{(3)}\rangle &= \mathrm{E}|10,\phi\rangle = \alpha_3|00,\phi_{1000}\rangle + \beta_3|01,\phi_{1001}\rangle + \gamma_3|10,\phi_{1010}\rangle + \delta_3|11,\phi_{1011}\rangle;\\
|\psi^{(4)}\rangle &= \mathrm{E}|11,\phi\rangle = \alpha_4|00,\phi_{1100}\rangle + \beta_4|01,\phi_{1101}\rangle + \gamma_4|10,\phi_{1110}\rangle + \delta_4|11,\phi_{1111}\rangle,
\end{aligned}
\qquad (5)
$$

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

В матричном виде операция Евы имеет вид:

$$
\mathrm{E} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \delta_1 & \delta_2 & \delta_3 & \delta_4 \end{pmatrix}. \qquad (6)
$$

Из условия унитарности операции $\hat{E}$ вытекают следующие соотношения между параметрами пробы:

$$
\alpha_i^*\alpha_j + \beta_i^*\beta_j + \gamma_i^*\gamma_j + \delta_i^*\delta_j = \varepsilon_{ij}, \qquad (7)
$$

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

$$
\begin{aligned}
&\sum_{i=1}^{4}\alpha_i^*\alpha_i = \sum_{i=1}^{4}\beta_i^*\beta_i = \sum_{i=1}^{4}\gamma_i^*\gamma_i = \sum_{i=1}^{4}\delta_i^*\delta_i = 1,\\
&\sum_{i=1}^{4}\alpha_i^*\beta_i = \sum_{i=1}^{4}\beta_i^*\alpha_i = \sum_{i=1}^{4}\alpha_i^*\gamma_i = \sum_{i=1}^{4}\gamma_i^*\alpha_i = \sum_{i=1}^{4}\alpha_i^*\delta_i = \sum_{i=1}^{4}\delta_i^*\alpha_i = \sum_{i=1}^{4}\beta_i^*\gamma_i = \sum_{i=1}^{4}\gamma_i^*\beta_i = \ldots = 0.
\end{aligned}
\qquad (8)
$$

Из (7) и (8) следует соотношения:

$$
\begin{aligned}
&|\alpha_1|^2 = |\beta_2|^2 = |\gamma_3|^2 = |\delta_4|^2; \quad |\alpha_2|^2 = |\beta_3|^2 = |\gamma_4|^2 = |\delta_1|^2;\\
&|\alpha_3|^2 = |\beta_4|^2 = |\gamma_1|^2 = |\delta_2|^2; \quad |\alpha_4|^2 = |\beta_1|^2 = |\gamma_2|^2 = |\delta_3|^2.
\end{aligned}
\qquad (9)
$$

Рассмотрим сначала случай, когда Боб "посылает" $|00\rangle$, т.е. состояние квантовой системы "передаваемые кубиты – проба" после атаки становится $|\psi^{(1)}\rangle$ (см. (5)). После выполнения Алисой кодирующих операций U_{000}, U_{001}, U_{010}, … (табл. 1) с частотами p_1, p_2, p_3, … соответственно, оператор плотности системы " передаваемые кубиты – проба " имеет вид:

$$\rho^{(1)} = \sum_{i=1}^{8} p_i \left|\psi_i^{(1)}\right\rangle\left\langle\psi_i^{(1)}\right|, \tag{10}$$

где

$$\begin{aligned}
\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_{0101}\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_{0110}\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_{0111}\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.
\end{aligned} \tag{11}$$

Максимальное количество классической информации I_0, доступное Еве после измерения над составной системой "передаваемые кубиты – проба", определяется энтропией Холево [1]:

$$I_0 = S\left(\rho^{(1)}\right) - \sum_{i=1}^{8} p_i S\left(\rho_i^{(1)}\right), \tag{12}$$

где $\rho_i^{(1)} = \left|\psi_i^{(1)}\right\rangle\left\langle\psi_i^{(1)}\right|$ и S – энтропия фон Неймана. Так как состояния (11) – чистые, то все $S\left(\rho_i^{(1)}\right)$ равны нулю и

$$I_0 = S\left(\rho^{(1)}\right) \equiv -Tr\left\{\rho^{(1)}\log_2\rho^{(1)}\right\} = -\sum_{i=1}^{16}\lambda_i\log_2\lambda_i \quad \text{(бит)}, \tag{13}$$

где λ_i – собственные значения оператора плотности $\rho^{(1)}$ (10).

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

$$\begin{aligned}
&\{\left|00,\varphi_{0000}\right\rangle, \left|01,\varphi_{0000}\right\rangle, \left|10,\varphi_{0000}\right\rangle, \left|11,\varphi_{0000}\right\rangle, \left|00,\varphi_{0001}\right\rangle, \left|01,\varphi_{0001}\right\rangle, \left|10,\varphi_{0001}\right\rangle, \left|11,\varphi_{0001}\right\rangle,\\
&\left|00,\varphi_{0010}\right\rangle, \left|01,\varphi_{0010}\right\rangle, \left|10,\varphi_{0010}\right\rangle, \left|11,\varphi_{0010}\right\rangle, \left|00,\varphi_{0011}\right\rangle, \left|01,\varphi_{0011}\right\rangle, \left|10,\varphi_{0011}\right\rangle, \left|11,\varphi_{0011}\right\rangle\}.
\end{aligned} \tag{14}$$

Полученная матрица имеет размер 16×16 и зависит от 12-ти параметров (8 частот кодирующих операций Алисы и 4 параметра проб Евы). Ввиду ее громоздкости здесь эта матрица не приводится.

С помощью инструментария символьных вычислений пакета Wolfram Mathematica 8.0 было найдено, что матрица плотности (10) имеет 8 ненулевых собственных значений:

$$\begin{aligned}
\lambda_{1,2}^{(|00\rangle)} &= \frac{1}{2}(p_1+p_2) \pm \frac{1}{2}\sqrt{(p_1+p_2)^2 - 16p_1p_2\left(|\beta_1|^2+|\gamma_1|^2\right)\left(|\alpha_1|^2+|\delta_1|^2\right)},\\
\lambda_{3,4}^{(|00\rangle)} &= \frac{1}{2}(p_3+p_4) \pm \frac{1}{2}\sqrt{(p_3+p_4)^2 - 16p_3p_4\left(|\beta_1|^2+|\gamma_1|^2\right)\left(|\alpha_1|^2+|\delta_1|^2\right)},\\
\lambda_{5,6}^{(|00\rangle)} &= \frac{1}{2}(p_5+p_6) \pm \frac{1}{2}\sqrt{(p_5+p_6)^2 - 16p_5p_6\left(|\beta_1|^2+|\gamma_1|^2\right)\left(|\alpha_1|^2+|\delta_1|^2\right)},\\
\lambda_{7,8}^{(|00\rangle)} &= \frac{1}{2}(p_7+p_8) \pm \frac{1}{2}\sqrt{(p_7+p_8)^2 - 16p_7p_8\left(|\beta_1|^2+|\gamma_1|^2\right)\left(|\alpha_1|^2+|\delta_1|^2\right)}.
\end{aligned} \tag{15}$$

Аналогичным образом анализируются остальные случаи в (5), т. е. когда вместо $\left|00\right\rangle$ Боб "посылает" $\left|01\right\rangle$ или $\left|10\right\rangle$ (согласно формуле (2), Боб *не* "посылает" $\left|11\right\rangle$). Для $\left|10\right\rangle$

собственные значения матрицы плотности $\rho^{(3)}=\sum_{i=1}^{8}p_i\left|\psi_i^{(3)}\right\rangle\left\langle\psi_i^{(3)}\right|$ совпадают с формулами (15), а для $\left|01\right\rangle$ собственные значения матрицы плотности $\rho^{(2)}=\sum_{i=1}^{8}p_i\left|\psi_i^{(2)}\right\rangle\left\langle\psi_i^{(2)}\right|$ с учетом соотношений (9) имеют вид:

$$\lambda_{1,2}^{(|01\rangle)}=\frac{1}{2}(p_1+p_2)\pm\frac{1}{2}\sqrt{(p_1+p_2)^2-16p_1p_2\left(|\alpha_1|^2+|\beta_1|^2\right)\left(|\gamma_1|^2+|\delta_1|^2\right)},$$
$$\lambda_{3,4}^{(|01\rangle)}=\frac{1}{2}(p_3+p_4)\pm\frac{1}{2}\sqrt{(p_3+p_4)^2-16p_3p_4\left(|\alpha_1|^2+|\beta_1|^2\right)\left(|\gamma_1|^2+|\delta_1|^2\right)},$$
$$\lambda_{5,6}^{(|01\rangle)}=\frac{1}{2}(p_5+p_6)\pm\frac{1}{2}\sqrt{(p_5+p_6)^2-16p_5p_6\left(|\alpha_1|^2+|\beta_1|^2\right)\left(|\gamma_1|^2+|\delta_1|^2\right)},$$
$$\lambda_{7,8}^{(|01\rangle)}=\frac{1}{2}(p_7+p_8)\pm\frac{1}{2}\sqrt{(p_7+p_8)^2-16p_7p_8\left(|\alpha_1|^2+|\beta_1|^2\right)\left(|\gamma_1|^2+|\delta_1|^2\right)}. \quad (16)$$

Как следует из первого выражения в (5), в случае, когда Боб "посылает" $\left|00\right\rangle$ и в режиме контроля подслушивания используется *z*-базис, вероятность обнаружить атаку

$$d_z=|\beta_1|^2+|\gamma_1|^2+|\delta_1|^2=1-|\alpha_1|^2. \quad (17)$$

Аналогично, если Боб "посылает" $\left|01\right\rangle$ или $\left|10\right\rangle$, то из второго и третьего выражения в (5) следует:

$$d_z=|\alpha_2|^2+|\gamma_2|^2+|\delta_2|^2=1-|\beta_2|^2=1-|\alpha_1^2| \quad \text{и} \quad d_z=|\alpha_3|^2+|\beta_3|^2+|\delta_3|^2=1-|\gamma_3|^2=1-|\alpha_1^2| \quad (18)$$

соответственно, с учетом соотношений (9). Таким образом, общее выражение для вероятности обнаружения атаки при использовании в режиме контроля подслушивания *z*-базиса имеет вид (17).

Поскольку из (2) следует, что Боб "посылает" кубиты в состоянии $\left|00\right\rangle$ с вероятностью 1/2, в состоянии $\left|01\right\rangle$ с вероятностью 1/4 и в состоянии $\left|10\right\rangle$ с вероятностью 1/4, то количество информации, которое может получить злоумышленник за один раунд протокола:

$$I_0=\frac{1}{2}S\left(\rho^{(1)}\right)+\frac{1}{4}\left[S\left(\rho^{(2)}\right)+S\left(\rho^{(3)}\right)\right]=-\frac{3}{4}\sum_{i=1}^{8}\lambda_i^{(|00\rangle)}\log_2\lambda_i^{(|00\rangle)}-\frac{1}{4}\sum_{i=1}^{8}\lambda_i^{(|01\rangle)}\log_2\lambda_i^{(|01\rangle)}. \quad (19)$$

Рассмотрим далее *симметричную* атаку, т.е. атаку при условиях

$$|\beta_1|^2=|\gamma_1|^2=|\delta_1|^2=d_z/3. \quad (20)$$

В этом случае, используя соотношение (17), из формул (15) и (16) можно исключить параметры проб α_1, β_1, γ_1 и δ_1, введя в эти формулы вероятность обнаружения атаки d_z. Это позволит в конечном итоге выразить количество информации злоумышленника (19) через d_z. В результате для симметричной атаки при условиях (20) получим:

$$I_0=-\sum_{i=1}^{8}\lambda_i\log_2\lambda_i, \quad (21)$$

так как собственные значения (15) и (16) в этом случае одинаковы и равны:

$$\lambda_{1,2}=\frac{1}{2}(p_1+p_2)\pm\frac{1}{2}\sqrt{(p_1+p_2)^2-16p_1p_2\cdot\frac{2}{3}d_z\left(1-\frac{2}{3}d_z\right)},$$
$$\lambda_{3,4}=\frac{1}{2}(p_3+p_4)\pm\frac{1}{2}\sqrt{(p_3+p_4)^2-16p_3p_4\cdot\frac{2}{3}d_z\left(1-\frac{2}{3}d_z\right)},$$

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

$$\lambda_{7,8}=\frac{1}{2}(p_7+p_8)\pm\frac{1}{2}\sqrt{(p_7+p_8)^2-16p_7p_8\cdot\frac{2}{3}d_z\left(1-\frac{2}{3}d_z\right)}. \quad (22)$$

Сравнивая этот результат с результатами анализа симметричной атаки пассивного перехвата на пинг-понг протокол с GHZ-триплетами кубитов [14], видим, что максимальная информация злоумышленника одинакова для этих двух пинг-понг протоколов. Следовательно, стойкость к атаке пассивного перехвата с использованием квантовых проб протокола с четырехкубитными W-состояниями и протокола с трехкубитными GHZ-состояниями *одинакова*. Отметим, что в обоих этих протоколах по квантовому каналу связи пересылаются два кубита из перепутанного четырех- и трехкубитного состояния соответственно, информационная емкость этих двух протоколов также одинакова и равна трем битам на цикл.

На рис. 1а представлены зависимости количества информации злоумышленника I_0 от вероятности d_z обнаружения атаки для симметричной атаки и одинаковых значениях частот кодирующих операций Алисы $p_1=p_2=\ldots=p_8=1/8$. Для сравнения также приведены соответствующие кривые для протоколов с четырехкубитными GHZ- и кластерными состояниями [13]. На рис. 1б показана приведенная информация злоумышленника $I_{red}(d_z)=I_0(d_z)/I_{\max}$, где $I_{\max}=4$ бита для протоколов с четырехкубитными GHZ- и кластерными состояниями и $I_{\max}=3$ бита для протокола с четырехкубитными W-состояниями.

Как видно из рис. 1б, при заданном проценте перехватываемой информации I_{red} вероятность обнаружить атаку d_z для пинг-понг протокола с четырехкубитными W-состояниями выше, чем для протокола с четырехкубитными GHZ-состояниями, но ниже, чем для протокола с четырехкубитными кластерными состояниями (в диапазоне небольших значений d_z). Однако, при $d_z\geq 0.35$ кривые для протоколов с четырехкубитными W- и GHZ-состояниями практически совпадают.

Также, как видно из рис. 1, для пинг-понг протокола с W-состояниями, аналогично другим пинг-понг протоколам с использованием квантового сверхплотного кодирования [4,5,13–15], существует "невидимый" режим подслушивания ($d_z=0$), при котором Ева получает частичную информацию, но ее атака не может быть обнаружена легитимными пользователями, когда они используют в режиме контроля подслушивания только один измерительный базис. Возможность такой "невидимой" атаки устраняется при использовании легитимными пользователями в режиме контроля подслушивания второго измерительного базиса $x=\{|+\rangle\langle+|,|-\rangle\langle-|\}$. Это может быть показано аналогично протоколу с четырехкубитными кластерными состояниями [13].

Также, как видно из рис. 1, для пинг-понг протокола с W-состояниями, аналогично другим пинг-понг протоколам с использованием квантового сверхплотного кодирования [4,5,13–15], существует "невидимый" режим подслушивания ($d_z=0$), при котором Ева получает частичную информацию, но ее атака не может быть обнаружена легитимными пользователями, когда они используют в режиме контроля подслушивания только один измерительный базис. Возможность такой "невидимой" атаки устраняется при использовании легитимными пользователями в режиме контроля подслушивания второго измерительного базиса $x=\{|+\rangle\langle+|,|-\rangle\langle-|\}$. Это может быть показано аналогично протоколу с четырехкубитными кластерными состояниями [13]. При этом, для любого значения величины d_z, величина d_x – вероятность обнаружить атаку при однократном контроле подслушивания в *x*-базисе – равна своему максимальному значению $d_{\max}=0.75$, и наоборот.

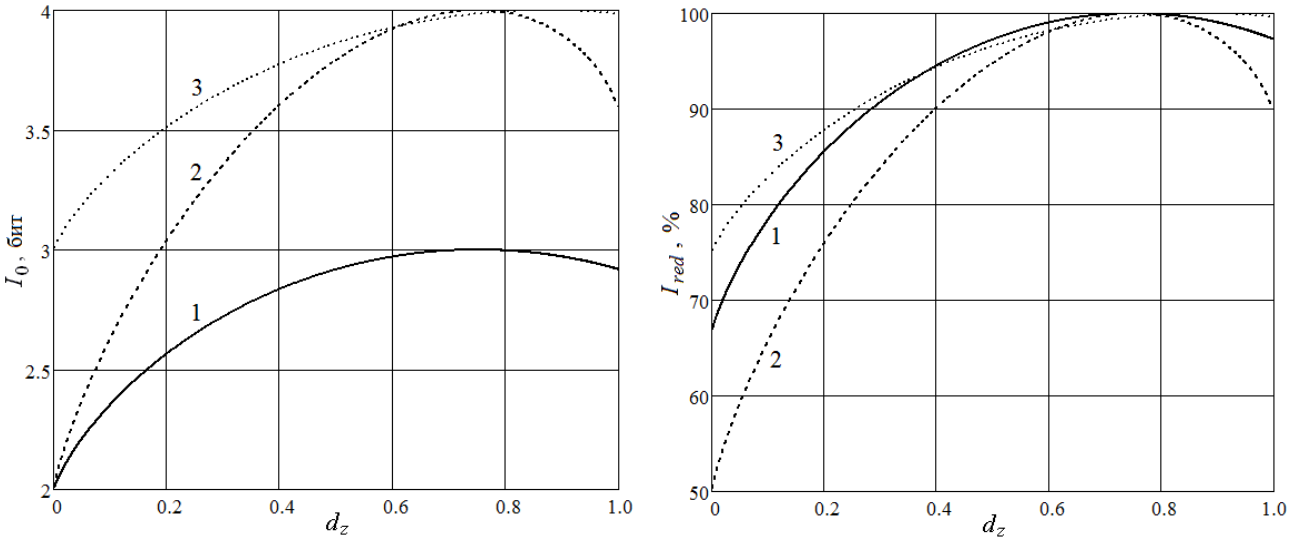
Минимальное значение вероятности обнаружения атаки при равновероятном использовании базисов z и x при однократном контроле подслушивания равно 0.375, как и для протокола с четырехкубитными кластерными состояниями [13].

Необходимо еще раз подчеркнуть, что в квантовом канале с шумом неверные результаты измерений, т.е. результаты, не совпадающие с табл. 2, будут обусловлены двумя причинами: атакой пассивного перехвата и естественным шумом в канале, и не существует способа различить неверные результаты, обусловленные этими двумя причинами. Поэтому, как отмечалось выше, при использовании шумного квантового канала легитимные пользователи должны выполнить некоторое количество раундов контроля подслушивания, достаточное для того, чтобы получить значимую статистику результатов своих измерений. Минимальный уровень неверных результатов, обусловленных атакой, в 37.5% достаточно высок для того, чтобы легитимные пользователи сделали вывод о наличии атаки, если уровень естественного шума в канале значительно ниже этого числа.

Для идеального квантового канала вероятность того, что Ева не будет обнаружена после m успешных атак и получит информацию $I = mI_0$, определяется формулой [3]:

$$s(I,q,d) = \left(\frac{1-q}{1-q(1-d)}\right)^m = \left(\frac{1-q}{1-q(1-d)}\right)^{\frac{I}{I_0}}, \qquad (23)$$

где q – вероятность перехода в режим контроля подслушивания.



а) б)

Рис. 1. Зависимости информации злоумышленника I_0 (а) и приведенной информации I_{red} (б) для протоколов с четырехкубитными W- (1), кластерными (2) и GHZ-состояниями (3).

На рис. 2 показаны зависимости $s(I,q,d)$ для тех же трех пинг-понг протоколов с четырехкубитными перепутанными состояниями, что на рис. 1, при $q = 0.5$ и $d = d_{\max}$ для соответствующего протокола: $d_{\max} = 0.75$ для протоколов с W- и кластерными состояниями и $d_{\max} = 0.875$ для протокола с ГХЦ-состояниями. При $d = d_{\max}$ Ева получает полную информацию о переданных битах сообщения (см. рис. 1).

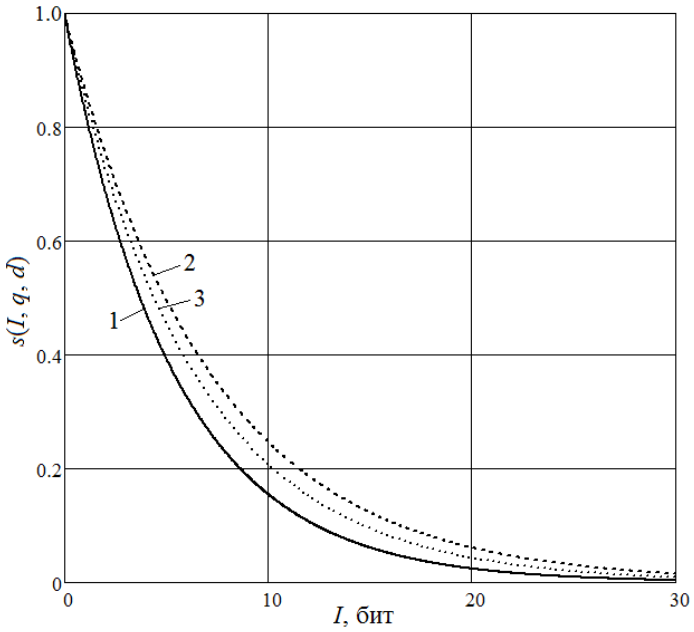


Рис. 2. Полная вероятность необнаружения атаки для протоколов с четырехкубитными W- (1), кластерными (2) и GHZ-состояниями (3)

Как видно из рис. 2, полная вероятность необнаружения атаки уменьшается экспоненциально с ростом перехватываемой информации. При этом для заданного s количество перехватываемой информации наименьшее для протокола с четырехкубитными W-состояниями и наибольшее для протокола с четырехкубитными кластерными состояниями. Однако разница в количестве перехватываемой информации невелика. Так, например, при $s = 0.2$ в протоколе с W-состояниями может быть перехвачено приблизительно 8.5 бит, а в протоколе с кластерными состояниями – приблизительно 11.5 бит. Таким образом, стойкость трех рассмотренных пинг-понг протоколов с четырехкубитными состояниями к атаке пассивного перехвата с использованием квантовых проб практически одинакова.

Выводы. В работе разработан новый пинг-понг протокол квантовой прямой безопасной связи с использованием перепутанных четырехкубитных W-состояний. Разработаны метод квантового кодирования классической информации и метод контроля подслушивания для протокола. Проанализированы два вида атак пассивного перехвата на протокол. Разработан метод модификации режима контроля подслушивания для обнаружения атаки "перехвата – повторной посылки" кубитов. Показано, что стойкость протокола к атаке перехвата с использованием квантовых проб такая же, как и стойкость протокола с трехкубитными GHZ-состояниями.

Проведен сравнительный анализ стойкости к атаке пассивного перехвата с использованием проб трех протоколов с четырехкубитными перепутанными состояниями: протокола с W-состояниями, GHZ-состояниями и кластерными состояниями. Показано, что стойкость этих протоколов к такой атаке практически одинакова. Стойкость же этих протоколов к естественному шуму в канале будет различна: она одинакова для протоколов с четырехкубитными W- и кластерными состояниями (по каналу пересылаются два кубита за цикл) и меньше для протокола с четырехкубитными GHZ-состояниями (по каналу пересылаются три кубита). При этом характеристики протокола с четырехкубитными W-состояниями почти полностью совпадают с характеристиками протокола с трехкубитными GHZ-состояниями. Эти два пинг-понг протокола имеют одинаковую информационную емкость, а также одинаковую стойкость как к атаке пассивного перехвата с использованием квантовых проб, так и к естественному шуму в канале. Стойкость этих двух протоколов к атаке "перехвата – повторной посылки" кубитов немного различна: вероятность обнаружения атаки в идеальном канале при однократном контроле для протокола с четырехкубитными W-состояниями равна 0.625, а для протокола с трехкубитными GHZ-состояниями – 0.5.

Таким образом, пинг-понг протокол с четырехкубитными W-состояниями не имеет особых преимуществ по сравнению с другими протоколами с четырехкубитными состояниями [11–14]. Наилучшим из исследованных протоколов с четырехкубитными состояниями по критериям стойкости и эффективности является протокол с кластерными состояниями [13]: он имеет наибольшую информационную емкость при наименьшем количестве пересылаемых по квантовому каналу кубитов, а его стойкость к атаке пассивного

перехвата с использованием проб практически такая же, как и у других протоколов с четырехкубитными состояниями (а при $d < d_{\max}$ его стойкость наибольшая, см. рис. 1б). Пинг-понг протокол с четырехкубитными кластерными состояниями также неуязвим к атаке "перехвата – повторной посылки" кубитов, поскольку для всех шестнадцати ортогональных состояний, используемых в этом протоколе, пара передаваемых кубитов находится в полностью смешанном состоянии [13], в отличие от протоколов с GHZ- и W-состояниями.

Как показывают результаты расчетов, пинг-понг протокол с четырехкубитными W-состояниями обладает только асимптотической стойкостью как к атаке "перехвата – повторной посылки" кубитов, так и к атаке пассивного перехвата с использованием квантовых проб и, следовательно, нуждается в дополнительном методе увеличения его стойкости. Такой метод увеличения стойкости пинг-понг протоколов, пригодный для защиты пинг-понг протокола с четырехкубитными W-состояниями от обеих проанализированных в статье атак, предложен в [18].

ЛИТЕРАТУРА:

1. Нильсен М. Квантовые вычисления и квантовая информация. / М. Нильсен, И. Чанг. – Москва: Мир, 2006. – 824 с.
2. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк // Захист інформації. – 2010, № 1. – С. 77–89.
3. Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.
4. Deng F.-G. Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block / F.-G. Deng, G.L. Long, X.-S. Liu // Physical Review A. – 2003. – V. 68, № 4. – 042317.
5. 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.
6. Pradhan B. Teleportation and superdense coding with genuine quadripartite entangled states / B. Pradhan, P. Agrawal, A. K. Pati // [Електронний ресурс] http://arxiv.org/abs/0705.1917.
7. 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. – V. 253, № 1. – P. 15 – 20.
8. Wang J. Multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state / J. Wang, Q. Zhang, C.J. Tang // Optics Communications. – 2006. – V. 266, № 2. – P. 732 – 737.
9. Li X.-H. Multiparty Quantum Remote Secret Conference / X.-H. Li, C.-Y. Li, F.-G. Deng et al // Chinese Physics Letters. – 2007. – V. 24, № 1. – P. 23 – 26.
10. Jin X.-R. Three-party quantum secure direct communication based on GHZ states / X.-R. Jin, X. Ji, Y.-Q. Zhang et al // Physics Letters A. – 2006. – V. 354, № 1-2. – P. 67 – 70.
11. Василиу Е.В. Три новых протокола квантовой безопасной связи с четырехкубитными кластерными состояниями / Е.В. Василиу, Р.С. Мамедов // Цифрові технології. – 2009, № 6. – С. 94–103.
12. Василиу Е.В. Пинг-понг протокол с трех– и четырехкубитными состояниями Гринбергера–Хорна–Цайлингера / Е.В. Василиу, Л.Н. Василиу // Труды Одесского политехнического университета. – 2008.– Вып. 1(29). – С. 171–176.
13. Василіу Є.В. Аналіз атаки пасивного перехоплення на пінг-понг протокол з чотирикубітними кластерними станами як елемент синтезу квантової системи безпечного зв'язку / Є.В. Василіу, Р.С. Мамедов // Наукові праці ОНАЗ ім. О.С. Попова. – 2010, № 1. – С. 38–48.
14. Василиу Е.В. Анализ атаки на пинг – понг протокол с триплетами Гринбергера – Хорна – Цайлингера / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2008, № 1. – С. 15–24.
15. Vasiliu E.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits / Eugene V. Vasiliu // Quantum Information Processing. – 2011. – V. 10, num. 2. – P. 189–202.
16. Li J. An Improved "Ping-pong" Protocol Based on Four-qubit Genuine Entangled State / J. Li, D. Song, X. Guo, B. Jing // Chinese Journal of Electronics. – 2011. – V. 20, No.3. – P. 457–460.
17. Yeo Ye. Teleportation and Dense Coding with Genuine Multipartite Entanglement / Ye Yeo, W.K. Chua // Physical Review Letters. – 2006. – V. 96, № 6. – 060502.
18. Патент України на корисну модель № 59732. Спосіб підсилення безпеки пінг-понг протоколу квантового безпечного зв'язку / П.П. Воробієнко, Є.В. Василіу, С.В. Ніколаєнко; заявник і патентовласник Одеська національна академія зв'язку ім. О.С. Попова; заявлено 19.11.2010; опубліковано 25.05.2011, бюл. № 10.

Надійшла: 19.09.2011

Рецензент: д.т.н., проф. Корченко О.Г.