УДК 003.26:621.39+530.145

ТРИ НОВЫХ ПРОТОКОЛА КВАНТОВОЙ БЕЗОПАСНОЙ СВЯЗИ С ЧЕТЫРЕХКУБИТНЫМИ КЛАСТЕРНЫМИ СОСТОЯНИЯМИ

ВАСИЛИУ Е.В., МАМЕДОВ Р.С.

Одесская национальная академия связи им. А.С. Попова

ТРИ НОВИХ КВАНТОВИХ ПРОТОКОЛИ БЕЗПЕЧНОГО ЗВ'ЯЗКУ ІЗ ЧОТИРИКУБІТНИМИ КЛАСТЕРНИМИ СТАНАМИ

ВАСІЛІУ Є.В., МАМЕДОВ Р.С.

Одеська національна академія зв’язку ім. О.С. Попова

THREE NEW PROTOCOLS OF QUANTUM SECURE COMMUNICATION WITH FOUR-QUBIT CLUSTER STATES

VASILIU E.V., MAMEDOV R.S.

Odessa national academy of telecommunications n.a. O.S. Popov

Аннотация. *Предложено три новых квантовых протокола безопасной связи с четырехкубитными кластерными состояниями: пинг-понг протокол между двумя сторонами, протокол между двумя сторонами с передачей кубитов блоками и пинг-понг протокол вида «двое $\rightarrow$ одному». Для предложенных протоколов разработаны схемы квантового кодирования информации и схемы проективных квантовых измерений для контроля подслушивания. Показано преимущество в использовании для пинг-понг протоколов кластерных состояний по сравнению с состояниями Гринбергера – Хорна – Цайлингера.*

Анотація. *Запропоновано три нових квантових протоколи безпечного зв'язку із чотирикубітними кластерними станами: пінг-понг протокол між двома сторонами, протокол між двома сторонами з передаванням кубітів блоками та пінг-понг протокол виду "двоє $\rightarrow$ одному". Для запропонованих протоколів розроблено схеми квантового кодування інформації й схеми проективних квантових вимірювань для контролю підслуховування. Показано перевагу у використанні для пінг-понг протоколів кластерних станів у порівнянні зі станами Грінбергера - Хорна - Цайлінгера.*

Summary. *Three new protocols of quantum secure communication with four-qubit cluster states: the ping-pong protocol between two parties, the protocol between two parties with qubit transferring in blocks and the ping-pong protocol form “two to one” are offered. For the offered protocols schemes of information coding and schemes of quantum projective measurements for eavesdropping check are developed. Advantage in use for ping-pong protocols of cluster states in comparison with Greenberger – Horne – Zeilinger states is shown.*

1. ВВЕДЕНИЕ

Квантовое перепутывание является одним из основных ресурсов квантовой информатики и существенным элементом многих квантовых вычислительных и коммуникационных протоколов [1]. В частности, большинство квантовых протоколов безопасной связи (КПБС), позволяющих напрямую, т.е. без шифрования, передавать конфиденциальные сообщения, используют перепутанные квантовые состояния групп кубитов (двумерных квантовых системы) или кудитов (многомерных квантовых систем) [2]. В этой статье рассматриваются только протоколы с кубитами.

Существуют двухкубитные подлинно перепутанные состояния (состояния Белла), свойства которых хорошо изучены, а также хорошо изучена стойкость к атакам злоумышленника 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. Для трех кубитов существует уже шесть различных типов перепутанных состояний, из которых два – подлинно перепутанные, это состояния Вернера (В-состояния) и состояния Гринбергера –

Хорна – Цайлингера (ГХЦ-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, уменьшая в то же время уровень ошибок при передаче благодаря квантовому сверхплотному кодированию, то разработка новых квантовых коммуникационных протоколов с использованием многокубитного перепутывания является важной и актуальной научной проблемой.

К настоящему времени разработаны различные протоколы квантовой безопасной связи, использующие многокубитные перепутанные состояния [2, 7–12]. Эти протоколы можно разделить на два класса – протоколы с использованием одного перепутанного состояния на один цикл протокола и протоколы с передачей кубитов большими блоками (размер которых 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 [5,7,12,13]. Протоколы с передачей кубитов блоками обладают более высокой стойкостью, чем пинг-понг протокол, но требуют большой квантовой памяти [3,8–11], создание которой пока находится за пределами современных технологий.

Большинство предложенных КПБС с трех- и более кубитными перепутанными состояниями используют в качестве таковых состояния ГЦХ [8–13]. С этими состояниями можно реализовать квантовое сверхплотное кодирование – передать n бит информации, передавая по квантовому каналу n–1 кубитов. Кроме того, с многокубитными ГХЦ-состояниями уже работают экспериментально [14,15]. Для трех кубитов ГХЦ-состояния – лучший квантовый ресурс с точки зрения реализации сверхплотного кодирования, чем В-состояния. Однако для четырех и более кубитов это уже не так [6]. Из всех подлинно перепутанных четырехкубитных состояний лучшим ресурсом для квантового сверхплотного кодирования являются так называемые *кластерные* (Ω) состояния [6]. Экспериментальное оборудование для их генерации создано к настоящему времени [16–18]. Поэтому вопрос о возможности разработки протоколов квантовой безопасной связи с использованием четырехкубитных Ω- состояний представляет значительный, как теоретический, так и практический интерес.

Многокубитные подлинно перепутанные состояния пригодны не только для реализации КПБС между двумя сторонами, но с их помощью могут быть выполнены различные криптографические протоколы между бóльшим числом сторон. Так в [11] предложен протокол с использованием трехкубитных ГХЦ-состояний для одновременно обмена сообщениями между тремя сторонами, а в [9] – протокол (также с ГХЦ-триплетами) для передачи сообщения от одного абонента к другому под контролем третьей доверенной стороны. Аналогичные протоколы могут быть реализованы с применением многокубитных ГХЦ-состояний [10,11], однако такие протоколы с кластерными состояниями к настоящему времени не предложены.

Целью настоящей работы является разработка схем кодирования информации и контроля подслушивания (пассивного перехвата) для трех КПБС с использованием Ω-состояний: пинг-понг протокола между двумя сторонами, протокола между двумя сторонами с передачей кубитов блоками и пинг-понг протокола вида «двое $\rightarrow$ одному».

2. ПИНГ-ПОНГ ПРОТОКОЛ С ЧЕТЫРЕХКУБИТНЫМИ Ω-СОСТОЯНИЯМИ

Шестнадцать ортонормированных четырехкубитных Ω-состояний имеют вид [6]:

$$|\Omega_1\rangle=(|0000\rangle+|0110\rangle+|1001\rangle-|1111\rangle)/2;\quad |\Omega_2\rangle=(|0000\rangle+|0110\rangle-|1001\rangle+|1111\rangle)/2;$$
$$|\Omega_3\rangle=(|0000\rangle-|0110\rangle+|1001\rangle+|1111\rangle)/2;\quad |\Omega_4\rangle=(|0000\rangle-|0110\rangle-|1001\rangle-|1111\rangle)/2;$$
$$|\Omega_5\rangle=(|0001\rangle+|0111\rangle+|1000\rangle-|1110\rangle)/2;\quad |\Omega_6\rangle=(|0001\rangle+|0111\rangle-|1000\rangle+|1110\rangle)/2;$$
$$|\Omega_7\rangle=(|0001\rangle-|0111\rangle+|1000\rangle+|1110\rangle)/2;\quad |\Omega_8\rangle=(|0001\rangle-|0111\rangle-|1000\rangle-|1110\rangle)/2;$$
$$|\Omega_9\rangle=(|0010\rangle+|0100\rangle+|1011\rangle-|1101\rangle)/2;\quad |\Omega_{10}\rangle=(|0010\rangle+|0100\rangle-|1011\rangle+|1101\rangle)/2;$$
$$|\Omega_{11}\rangle=(|0010\rangle-|0100\rangle+|1011\rangle+|1101\rangle)/2;\quad |\Omega_{12}\rangle=(|0010\rangle-|0100\rangle-|1011\rangle-|1101\rangle)/2;$$
$$|\Omega_{13}\rangle=(|0011\rangle+|0101\rangle+|1010\rangle-|1100\rangle)/2;\quad |\Omega_{14}\rangle=(|0011\rangle+|0101\rangle-|1010\rangle+|1100\rangle)/2;$$
$$|\Omega_{15}\rangle=(|0011\rangle-|0101\rangle+|1010\rangle+|1100\rangle)/2;\quad |\Omega_{16}\rangle=(|0011\rangle-|0101\rangle-|1010\rangle-|1100\rangle)/2. \qquad (1)$$

Состояние $|\Omega_1\rangle$ может быть преобразовано в остальные пятнадцать действием локальных унитарных операторов (операторов Паули) на *два* любых кубита из четырех [6]. В этом состоит преимущество четырехкубитных Ω- состояний над четырехкубитными ГХЦ-состояниями – для преобразования последних необходимо локально подействовать на *три* кубита [12]. Таким образом, используя четырехкубитные Ω-состояния в пинг-понг протоколе, можно передать четыре бита информации, передавая по квантовому каналу только два кубита, а не три, как для четырехкубитных ГХЦ-состояний. Этот означает, что пинг-понг протокол с Ω-состояниями будет менее подвержен влиянию ошибок в реальных квантовых каналах с шумом, чем протокол с ГХЦ-состояниями. В табл. 1 представлены возможности квантового сверхплотного кодирования для пяти четырехкубитных подлинно перепутанных состояний, иллюстрирующие преимущества Ω-состояний над остальными для пинг-понг протокола (таблица получена на основе результатов работы [6]).

Таблица 1 – квантовое сверхплотное кодирование в пинг-понг протоколе с четырехкубитными подлинно перепутанными состояниями, бит

Кол-во пересылаемых кубитов / Состояние	1	2	3
$\|Q_1\rangle\equiv\|GHZ\rangle=(\|0000\rangle+\|1111\rangle)/\sqrt{2}$	2	3	4
$\|Q_2\rangle\equiv\|W\rangle=(\|0001\rangle+\|0010\rangle+\|0100\rangle+\|1000\rangle)/$	-	3	3
$\|Q_3\rangle\equiv\|\Omega_7\rangle=(\|0000\rangle+\|0110\rangle+\|1001\rangle-\|1111\rangle)/$	2	**4**	4
$\|Q_4\rangle=(\|0000\rangle+\|0101\rangle+\|1000\rangle+\|1110\rangle)/2$	2	3	3
$\|Q_5\rangle=(\|0000\rangle+\|1011\rangle+\|1101\rangle+\|1110\rangle)/2$	2	3	4

Первым этапом разработки нового протокола квантовой безопасной связи, в данном случае нового варианта пинг-понг протокола, является разработка схемы квантового кодирования классической информации. Для этого сначала необходимо найти множество локальных унитарных операторов, преобразующих состояние $|\Omega_1\rangle$ в состояния $|\Omega_1\rangle\ldots|\Omega_{16}\rangle$ (кодирующие операции), а затем поставить в соответствие каждому из состояний $|\Omega_i\rangle$ четырехбитовую строку. Разумеется, последняя операция является произвольной, и ее могут выполнять каждый раз сами участники протокола. Мы приводим соответствие Ω-состояний четырехбитовым строкам в табл. 2 для примера.

Найденное множество кодирующих операций, при 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 только тождественный оператор $I=|0\rangle\langle 0|+|1\rangle\langle 1|$, оставляющий состояние неизменным), приведено в табл. 2.

Таблица 2 – схема квантового кодирования классической информации для пинг-понг протокола с четырехкубитными кластерными состояниями

i	Оператор для преобразования $\|\Omega_1\rangle \to \|\Omega_i\rangle$	Битовая строка, соответствующая $\|\Omega_i\rangle$	i	Оператор для преобразования $\|\Omega_1\rangle \to \|\Omega_i\rangle$	Битовая строка, соответствующая $\|\Omega_i\rangle$
1	$I \otimes I \otimes I \otimes I$	0000	9	$I \otimes I \otimes \sigma_x \otimes I$	1000
2	$I \otimes I \otimes I \otimes \sigma_z$	0001	10	$I \otimes I \otimes \sigma_x \otimes \sigma_z$	1001
3	$I \otimes I \otimes \sigma_z \otimes I$	0010	11	$I \otimes I \otimes i\sigma_y \otimes I$	1010
4	$I \otimes I \otimes \sigma_z \otimes \sigma_z$	0011	12	$I \otimes I \otimes i\sigma_y \otimes \sigma_z$	1011
5	$I \otimes I \otimes I \otimes \sigma_x$	0100	13	$I \otimes I \otimes \sigma_x \otimes \sigma_x$	1100
6	$I \otimes I \otimes I \otimes i\sigma_y$	0101	14	$I \otimes I \otimes \sigma_x \otimes i\sigma_y$	1101
7	$I \otimes I \otimes \sigma_z \otimes \sigma_x$	0110	15	$I \otimes I \otimes i\sigma_y \otimes \sigma_x$	1110
8	$I \otimes I \otimes \sigma_z \otimes i\sigma_y$	0111	16	$I \otimes I \otimes i\sigma_y \otimes i\sigma_y$	1111

Приведем теперь пошаговое описание пинг-понг протокола с четырехкубитными Ω-состояниями и квантовым сверхплотным кодированием. По традиции назовем отправителя сообщения Алисой, получателя – Бобом.

Шаг 1. Боб приготавливает состояние $|\Omega_1\rangle = \left(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle\right)/2$.

Шаг 2. Он оставляет у себя первые два кубита и посылает третий и четвертый кубиты Алисе по квантовому каналу связи.

Шаг 3. Алиса получает кубиты от Боба. С вероятностью p она переключается в режим контроля подслушивания. Тогда выполняется шаг 4, иначе Алиса переключается в режим передачи сообщения, и выполняются шаги с 5-го по 7-ой.

Шаг 4. Контроль подслушивания в протоколах квантовой безопасной связи выполняется последовательными измерениями состояний кубитов. Сначала одна из сторон, например, Алиса, выполняет измерения в определенном базисе и сообщает выбранный базис и результаты измерений другой стороне – Бобу. Затем соответствующие измерения выполняет Боб. Для протоколов с многокубитными перепутанными состояниями возможны несколько различных вариантов таких измерений. Мы рассмотрим схему контроля подслушивания, при которой обе стороны выполняют измерения в одночастичных базисах, а Боб отправляет Алисе третий и четвертый кубиты, так как схема кодирования, приведенная в табл. 2, разработана для этого случая.

Таким образом, Алиса случайным образом выбирает один из двух измерительных базисов – B_z или B_x и выполняет измерение состояний третьего и четвертого кубитов в выбранном базисе, а затем сообщает Бобу по обычному открытому, но аутентифицированному каналу о переключении в режим контроля подслушивания. Аутентификация всех посылаемых в обычном канале сообщений необходима для предотвращения атаки «человек посередине». Затем Боб в том же базисе, что и Алиса, измеряет состояния первого и второго кубитов. Расчеты показывают, что после измерений Алисы в любом из базисов B_z или B_x состояние $|\Omega_i\rangle$ редуцируется таким образом, что результаты измерений Боба становятся определенными (получаемыми с вероятностью, равной единице) для обоих имеющихся у него кубитов. Этим кластерное состояние $|\Omega_i\rangle$ отличается от четырехкубитного ГХЦ-состояния $|GHZ\rangle = (|0000\rangle + |1111\rangle)/\sqrt{2}$, для которого при измерениях в базисе B_x с вероятностью 1 измеряется состояние только одного – последнего кубита [12].

В табл. 3 приведены результаты измерений Алисы и Боба по описанной выше схеме. Алиса, измеряя состояния третьего и четвертого кубитов в базисе B_z, получает «0» или «1» с одинаковой вероятностью $1/2$, и аналогично получает с вероятностью $1/2$ «+» или «–» при измерении в базисе B_x. Боб должен получить результаты своих измерений с вероятностью 1 как для первого, так и для второго кубитов.

Таблица 3 – схема и результаты измерений для контроля подслушивания

Результаты Алисы		Состояние после измерений Алисы	Результаты Боба	
кубит 3	кубит 4		кубит 1	кубит 2
Базис $\|B_z\rangle$				
0	0	$\|0000\rangle$	0	0
	1	$\|1001\rangle$	1	0
1	0	$\|0110\rangle$	0	1
	1	$\|1111\rangle$	1	1
Базис $\|B_x\rangle$				
+	+	$\|++++\rangle$	+	+
	–	$\|-++-\rangle$	–	+
–	+	$\|+--+\rangle$	+	–
	–	$\|----\rangle$	–	–

Если результаты измерений Боба отличаются от приведенных в табл. 3, то это означает, что состояние передаваемых кубитов было возмущено на пути от Боба к Алисе. Для идеального квантового канала это может произойти только, если Ева выполнила некоторую операцию над этими кубитами с целью последующего определения кодирующей операции Алисы, т.е. перехвата информации. Поэтому в случае несовпадения результатов измерений Боба с ожидаемыми, он немедленно сообщает об этом Алисе по обычному каналу связи и протокол прерывается.

В реальном квантовом канале с шумом Алиса и Боб должны будут выполнить некоторое количество раундов контроля подслушивания, чтобы оценить уровень ошибок при измерениях Боба и сравнить его с ожидаемым граничным уровнем естественных ошибок в канале. Превышение этого граничного уровня приписывается атаке Евы и протокол прерывается. При этом, так как режим контроля подслушивания чередуется с режимом передачи сообщения, Ева сможет получить некоторое количество информации. Оценка этого количества требует детального анализа атаки и выходит за рамки данной статьи.

Шаг 5. В соответствие со своей текущей четырехбитовой строкой Алиса выбирает одну из шестнадцати кодирующих операций (см. табл. 2) и выполняет эту операцию над третьим и четвертым кубитами. Затем Алиса отправляет эти кубиты обратно Бобу.

Шаг 6. Получив кубиты от Алисы, Боб выполняет измерение над всеми четырьмя кубитами в Ω - базисе (1), что вследствие ортогональности Ω - состояний позволяет ему достоверно определить состояние, созданное кодирующей операцией Алисы, и тем самым определить четырехбитовую строку, которую она послала.

Шаг 7. Если сообщение передано полностью, то протокол успешно закончен, иначе переход к шагу 1.

3. ПРОТОКОЛ С ЧЕТЫРЕХКУБИТНЫМИ Ω-СОСТОЯНИЯМИ И ПЕРЕДАЧЕЙ КУБИТОВ БЛОКАМИ

Дадим теперь пошаговое описание протокола с использованием большой квантовой памяти для хранения блоков кубитов.

Шаг 1. Алиса приготавливает *N* одинаковых четырехкубитных состояний $|\Omega\rangle$, присваивая каждому из них порядковый номер.

Шаг 2. Алиса берет первый и второй кубиты из каждого приготовленного состояния $|\Omega\rangle$ и формирует два упорядоченных блока кубитов – из первых и из вторых кубитов соответственно, длины *N* каждый. Затем она пересылает оба этих блока Бобу, который сохраняет их в квантовой памяти.

Шаг 3. Когда Боб получает эти блоки, он информирует об этом Алису по обычному аутентифицированному каналу, и они выполняют контроль подслушивания с использованием той же схемы, что и для пинг-понг протокола (см. табл. 3).

Алиса выбирает случайным образом некоторое количество *M* из приготовленных ею *N* состояний $|\Omega\rangle$ и для этих выбранных состояний измеряет состояния третьих, а затем четвертых кубитов, выбирая для каждого состояния случайным образом базис B_z или B_x. Затем Алиса сообщает результаты Бобу, указывая также выбранный ею базис и порядковый номер каждого состояния $|\Omega\rangle$, выбранного ею для контроля подслушивания. Например, Алиса сообщает, что она измерила состояния находящихся у нее кубитов в состоянии $|\Omega\rangle$ №5 в базисе B_z и получила «0», «0»; и так для все выполненных Алисой измерений.

Боб измеряет состояния первого и второго кубитов в тех же состояниях $|\Omega\rangle$, которые выбрала Алиса, и сравнивает, используя табл. 3, полученное им количество ошибок с ожидаемым для данного квантового канала. Если полученный Бобом уровень ошибок превышает гранично допустимый, то протокол прерывается, иначе переход к шагу 4.

Отметим, что в этом протоколе, в отличие от пинг-понг протокола, контроль подслушивания выполняется *до* передачи самого сообщения и, следовательно, никакая информация не попадает к Еве. Однако для хранения нескольких блоков кубитов длины *N* каждый обеим легитимным сторонам необходима квантовая память большого объема – ведь величина *N* должна быть достаточной для того, чтобы, выбрав из приготовленных *N* состояний $M<N$ для контроля подслушивания, они смогли обнаружить атаку пассивного перехвата с заданной наперед вероятностью. В то же время в пинг-понг протоколе квантовая память необходима только Бобу для хранения двух кубитов в течение одного раунда протокола. Таким образом, протокол с передачей кубитов блоками, в отличие от пинг-понг протокола, обладает безусловной стойкостью к атаке пассивного перехвата (при надлежащем выборе количества *M* состояний $|\Omega\rangle$ для контроля подслушивания), но требует гораздо более сложного оборудования для хранения большого количества кубитов. Отметим также, что вопрос о минимально необходимом числе *M* состояний $|\Omega\rangle$, которые нужно измерить для обнаружения атаки пассивного перехвата с заданной наперед вероятностью, может быть решен только путем анализа этой атаки, что будет выполнено в отдельной работе.

Шаг 4. Алиса использует оставшиеся $N–M$ состояний $|\Omega\rangle$, назовем их информационными, для кодирования сообщения. Кодирование выполняется действием операторов Паули на третий и четвертый кубиты всех информационных состояний в соответствие с табл. 2. Затем Алиса отправляет третий и четвертый кубиты каждого информационного состояния Бобу, сообщая при этом также порядковые номера состояний по обычному каналу.

Шаг 5. Получив кубиты от Алисы, Боб имеет теперь все четыре кубита каждого информационного состояния и выполняет измерения в Ω - базисе (1), тем самым декодируя сообщение Алисы.

Шаг 6. Если сообщение передано полностью, то протокол успешно закончен, иначе выполняется переход к шагу 1.

4. ПИНГ-ПОНГ ПРОТОКОЛ ВИДА «ДВОЕ → ОДНОМУ»

Этот протокол предусматривает, что один получатель (Боб) может одновременно принимать сообщения от двух отправителей (Алиса и Чарли) с использованием одного

приготовленного им Ω-состояния (на один раунд протокола). Дадим пошаговое описание протокола.

Шаг 1. Боб приготавливает состояние $|\Omega_1\rangle = \left(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle\right)/2$.

Шаг 2. Он оставляет у себя первые два кубита и посылает третий кубит Алисе, а четвертый – Чарли.

Шаг 3. Алиса и Чарли получают кубиты от Боба. Затем один из них, пусть это будет Алиса, с вероятностью *p* переключается в режим контроля подслушивания. Тогда выполняются шаги 4 и 5, иначе Алиса переключается в режим передачи сообщения, и выполняются шаги с 6-го по 8-ой.

Шаг 4. Алиса измеряет состояние имеющегося у нее третьего кубита в одном из базисов – B_z или B_x, выбирая их случайным образом. Затем она сообщает выбранный ею базис Чарли. Чарли измеряет состояние имеющегося у него четвертого кубита в том же базисе.

Шаг 5. Алиса и Чарли сообщают Бобу выбранный базис и результаты их измерений. Боб измеряет состояния первого и второго кубита в том же базисе. Результаты измерений, соответствующие невозмущенному при передачи кубитов состоянию $|\Omega_1\rangle$, т.е. отсутствию подслушивания в идеальном квантовом канале, представлены в табл. 4. Если результаты Боба не совпадают с ожидаемыми, то протокол прерывается, иначе переход к шагу 1.

Таблица 4 – схема и результаты измерений для контроля подслушивания в пинг-понг протоколе вида двое $\rightarrow$ одному

Результат Алисы	Результат Чарли	Состояние после измерений	Результаты Боба	
кубит 3	кубит 4	Алисы и Чарли	кубит 1	кубит 2
Базис $\|B_z\rangle$				
0	0	$\|0000\rangle$	0	0
	1	$\|1001\rangle$	1	0
1	0	$\|0110\rangle$	0	1
	1	$\|1111\rangle$	1	1
Базис $\|B_x\rangle$				
+	+	$\|++++\rangle$	+	+
	–	$\|--++\rangle$	–	+
–	+	$\|+--+\rangle$	+	–
	–	$\|----\rangle$	–	–

Для реального квантового канала с шумом необходимо будет, как и для пинг-понг протокола между двумя сторонами, выполнить некоторое количество раундов контроля подслушивания, чтобы оценить уровень ошибок и сравнить его с известным граничным уровнем естественных ошибок в канале. Если уровень ошибок приемлем, то протокол продолжается, иначе – прерывается.

Шаг 6. В режиме передачи сообщения Алиса и Чарли выполняют одну из четырех операций I, σ_z, σ_x или $i\sigma_y$, каждый над своим кубитом, и после этого отправляют кубиты обратно Бобу. Схема кодирования, позволяющая в данном случае, как Алисе, так и Чарли, передать по два бита информации Бобу, представлена в табл. 5.

Таблица 5 – Схема кодирования информации для пинг-понг протокола вида «двое $\rightarrow$ одному»

Операция Алисы над 3-им кубитом	Операция Чарли над 4-ым кубитом	Состояние, которое будет у Боба	Биты Алисы	Биты Чарли
I	*I*	$\|\Omega_1\rangle$	00	00
I	σ_z	$\|\Omega_2\rangle$	00	01
I	σ_x	$\|\Omega_3\rangle$	00	10

I	$i\sigma_y$	$\|\Omega_8\rangle$	00	11
σ_z	I	$\|\Omega_3\rangle$	01	00
σ_z	σ_z	$\|\Omega_4\rangle$	01	01
σ_z	σ_x	$\|\Omega_7\rangle$	01	10
σ_z	$i\sigma_y$	$\|\Omega_6\rangle$	01	11
σ_x	I	$\|\Omega_9\rangle$	10	00
σ_x	σ_z	$\|\Omega_{10}\rangle$	10	01
σ_x	σ_x	$\|\Omega_{13}\rangle$	10	10
σ_x	$i\sigma_y$	$\|\Omega_{14}\rangle$	10	11
$i\sigma_y$	I	$\|\Omega_{11}\rangle$	11	00
$i\sigma_y$	σ_z	$\|\Omega_{12}\rangle$	11	01
$i\sigma_y$	σ_x	$\|\Omega_{15}\rangle$	11	10
$i\sigma_y$	$i\sigma_y$	$\|\Omega_{16}\rangle$	11	11

Шаг 7. Боб выполняет измерение над всеми четырьмя кубитами в Ω - базисе (1), и тем самым определяет четыре бита посланной ему информации – два от Алисы и два от Чарли.

Шаг 8. Если оба сообщения переданы полностью, то протокол закончен. Иначе переход к шагу 1. Заметим, что если одно из предназначенных Бобу сообщений короче другого, то по завершении первого Боб может перейти на протокол между двумя сторонами, описанный в разделе 2 настоящей статьи, и завершить прием оставшейся части второго сообщения.

Описанный протокол вида «двое $\rightarrow$ одному» с Ω-состояниями имеет преимущество перед аналогичным протоколом с четырехкубитными ГХЦ-состояниями. В последнем случае для преобразования одного ГХЦ-состояния в пятнадцать остальных необходимо действовать операторами Паули на три кубита [12], т.е. Боб должен будет отправить два кубита (вместо одного при использовании Ω-состояний) Алисе и один Чарли (или наоборот), что увеличит вероятность ошибки при передаче кубитов в реальном квантовом канале.

Отметим, что описанная схема контроля подслушивания обеспечивает асимптотическую стойкость протокола к атаке внешнего агента, но не защищает от нечестных действий того из отправителей, кто принимает решение о переходе в режим контроля подслушивания. Эта сторона протокола, вероятно, будет иметь возможность прочитать сообщение второго отправителя (или, по крайней мере, получить о нем некоторую частичную информацию). Одним из вариантов защиты в случае, если получатель сообщения считает такую атаку возможной, будет небольшое изменение схемы контроля подслушивания, а именно решение о переходе в этот режим должен принимать получатель.

Отметим также, что не представляет сложности разработка схемы протокола «двое $\rightarrow$ одному» на случай передачи кубитов блоками.

5. ОБСУЖДЕНИЕ И ВЫВОДЫ

В работе предложено три новых квантовых протокола безопасной связи с использованием четырехкубитных кластерных состояний: пинг-понг протокол между двумя сторонами, протокол между двумя сторонами с передачей кубитов блоками и пинг-понг протокол вида «двое $\rightarrow$ одному». Разработаны схемы кодирования информации для этих протоколов и схемы измерений для процедур контроля подслушивания. Даны детальные пошаговые описания предложенных протоколов.

Использование кластерных состояний четырех кубитов вместо четырехкубитных ГХЦ-состояний позволяет эффективнее реализовать квантовое сверхплотное кодирование и тем самым повысить устойчивость пинг-понг протоколов, как между двумя сторонами, так и вида «двое $\rightarrow$ одному», к шуму в квантовом канале. В протоколах с кластерными состояниями для каждого состояния необходимо передавать от получателя к

отправителю (отправителям) и обратно два кубита из четырех, а в протоколах с ГХЦ-состояниями – три кубита. В протоколе с передачей кубитов блоками все четыре кубита каждого состояния, кластерного или ГХЦ, передаются один раз от Алисы к Бобу. Поэтому такой протокол заведомо более устойчив к декогеренции в квантовом канале, и с этой точки зрения не имеет значения, какие состояния использовать – кластерные или ГХЦ.

Протокол с передачей кубитов блоками обладает более высокой стойкостью к атаке пассивного перехвата, чем пинг-понг протокол, поскольку в первом протоколе информация передается только после того, как легитимные пользователи убедятся в отсутствии подслушивания в квантовом канале. Однако процедура контроля подслушивания для всех предложенных в работе протоколов позволяет обнаружить атаку только с некоторой вероятностью. Вопрос о параметрах этой процедуры, обеспечивающих обнаружение подслушивания с любой, сколь угодно близкой к единице, вероятностью, требует дальнейших исследований.

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. *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.
4. *Boström K.* On the security of the ping-pong protocol / K. Boström, T. Felbinger // Physics Letters A. – 2008. – V. 372, № 22. – P. 3953–3956.
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. *Bostrom K.* Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.
8. *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.
9. *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.
10. *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.
11. *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.
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. *Василиу Е.В.* Синтез основанной на пинг–понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. – 2009, № 1. – С. 83 – 91.
14. *Experimental* high-intensity three-photon entangled source / H.-X. Lu, J. Zhang, X.-Q. Wang et al // Physical Review A. – 2008. – V. 78, № 3. – 033819.
15. *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. – V. 74. – 052311.
16. *Experimental* one-way quantum computing // P. Walther, K. J. Resch, T. Rudolph et al // Nature. – 2005. – V. 434, № 7030. – P. 169–176.
17. *Experimental* realization of one-way quantum computing with two-photon four-qubit cluster states // K. Chen, Che-M. Li, Q. Zhang et al // Physical Review Letters. – 2008. – V. 99, № 12. – 120503.
18. *Generation* of high-fidelity four-photon cluster state and quantum-domain demonstration of one-way quantum computing / Yu. Tokunaga, S. Kuwashiro, T. Yamamoto et al // Physical Review Letters. – 2008. – V. 100, № 21. – 210501.