УДК 003.26:621.39

Е.В. Василиу, канд. физ.-мат. наук,
Одес. нац. акад. связи им. А.С. Попова,
Л.Н. Василиу, физик-теоретик,
Одес. нац. политехн. ун-т

ПИНГ- ПОНГ ПРОТОКОЛ С ТРЕХ- И ЧЕТЫРЕХКУБИТНЫМИ СОСТОЯНИЯМИ ГРИНБЕРГЕРА-ХОРНА-ЦАЙЛИНГЕРА

Є.В. Василіу, Л.М. Василіу. **Пінг-понг протокол з три- та чотирикубітними станами Грінбергера-Хорна-Цайлінгера.** Запропоновано два нових варіанта пінг-понг протоколу квантового безпечного прямого зв'язку з використанням три- та чотирикубітних станів Грінбергера-Хорна-Цайлінгера. Розроблено схеми вимірів для режиму контролю підслуховування. Дано детальні покрокові описи запропонованих протоколів.

E.V. Vasiliu, L.N. Vasiliu. **Ping- pong protocol with three- and four-qubit Greenberger-Horne-Zeilinger states.** Two new versions of ping-pong protocol of a quantum secure direct communication using three- and four-qubit Greenberger-Horne-Zeilinger states are offered. Schemes of measurements are developed for an interception control mode. Detailed step-by-step descriptions of the offered protocols are given.

Квантовые коммуникации стали одним из важнейших приложений квантовой механики и теории передачи информации, поскольку они предлагают новый подход к решению важной проблемы передачи секретных сообщений. Так, квантовые протоколы распределения ключей обеспечивают безопасный способ создания секретного ключа, используя который две авторизованные стороны, Алиса и Боб, могут обмениваться конфиденциальными сообщениями [1]. Недавно была предложена новая концепция квантовой криптографии, получившая название квантовой безопасной прямой связи (КБПС) [2]. В протоколах КБПС секретный ключ вообще не используется, а секретное сообщение, закодированное с помощью квантовых состояний кубитов, передается непосредственно через квантовый канал. При этом законы квантовой механики гарантируют обнаружение подслушивания в канале, для чего легитимные стороны должны выполнить определенную последовательность квантовых измерений над некоторой частью переданных кубитов. Обнаружив подслушивающего агента, Еву, Алиса и Боб прекращают передачу сообщения.

Одним из протоколов КБПС является пинг-понг протокол, в котором в качестве кубитов используется пара фотонов, максимально перепутанных по их поляризационным степеням свободы, — состояния Белла [2]. Для передачи бита используется только один из этих фотонов, поэтому Ева, перехватив фотон и измерив его поляризацию, не может получить значение бита, не имея доступа ко второму фотону. Тем не менее, используя квантовые пробы и выполняя соответствующие унитарные операции и последующие измерения над составными (фотоны-пробы) квантовыми системами, Ева имеет возможность перехватить некоторую часть сообщения. Поэтому в пинг-понг протоколе предусмотрен специальный режим контроля подслушивания, используя который Алиса и Боб обнаруживают операции Евы [2…4].

В первоначальном варианте пинг-понг протокола каждый передаваемый кубит (один из перепутанной пары) используется для кодирования одного классического бита. Возможно увеличение информационной емкости канала путем использования квантового сверхплотного кодирования, в этом случае с помощью одного кубита можно передать два бита информации [3, 4]. Дальнейшее увеличение информационной емкости предполагает использование вместо перепутанных пар кубитов их троек, четверок и т.д. Известен один из протоколов, использующих полностью перепутанные триплеты кубитов, так называемый многошаговый протокол КБПС [5], а также другой протокол с использованием триплетов Гринбергера-Хорна-Цайлингера (ГХЦ), позволяющий секретно передать сообщение от Алисы к Бобу под контролем третьей

доверенной стороны [6]. Достоинством этих протоколов является высокий уровень стойкости к атакам подслушивающего агента, а недостатком — необходимость у легитимных сторон квантовой памяти большого объема для хранения состояний кубитов до завершения всего протокола. В отличие от таких протоколов, пинг-понг протокол не требует большой квантовой памяти, однако является квазибезопасным, т.е. любая эффективная атака Евы будет обнаружена, но прежде она сможет получить некоторую небольшую часть сообщения [2, 4]. Однако безопасность пинг-понг протокола может быть усилена с использованием методов классической криптографии, аналогично тому, как это делается для квантовых протоколов распределения ключей. Поэтому значительный интерес представляет разработка вариантов пинг-понг протокола с использованием перепутанных состояний трех и большего числа кубитов, которые, с одной стороны, обладают значительной информационной емкостью, а, с другой стороны, легче реализуемы технически, чем протоколы [5, 6].

Целью являлась разработка двух вариантов пинг-понг протокола: с использованием трехкубитных и с использованием четырехкубитных состояний ГХЦ, а также разработка процедур контроля подслушивания, необходимых для обеспечения квазибезопасности этих протоколов.

Существует восемь полностью перепутанных ортонормированных ГХЦ — состояний триплета кубитов $|\Psi_1\rangle \dots |\Psi_8\rangle$ (табл. 1), которые образуют базис в гильбертовом пространстве трех кубитов и соответственно могут быть точно отличены друг от друга соответствующим измерением [5, 6]. Таким образом, выполнив измерение, принимающая сторона получит один из восьми возможных вариантов, что соответствует трем битам информации.

Состояния $|\Psi_1\rangle \dots |\Psi_8\rangle$ могут быть трансформированы одно в другое применением однокубитных унитарных операторов к любым двум из трех кубитов [5, 6]. Предполагая, что начальным состоянием, которое готовит Боб, является $|\Psi_1\rangle$, построим набор унитарных операторов, преобразующих $|\Psi_1\rangle$ в $|\Psi_1\rangle \dots |\Psi_8\rangle$, соответственно. Всего существует шестнадцать таких операторов, из которых необходимо выбрать восемь. Набор унитарных операторов для преобразования $|\Psi_1\rangle$ в $|\Psi_1\rangle \dots |\Psi_8\rangle$, построенных так, чтобы они содержали минимально возможное количество нетождественных операций, приведен в табл. 1 (отметим, что на третий кубит всегда действует тождественный оператор). Также здесь приведены трехбитовые строки, которые будут соответствовать каждому из состояний $|\Psi_1\rangle \dots |\Psi_8\rangle$, о таком соответствии Алиса и Боб должны договориться до начала протокола.

Таблица 1

Набор унитарных операторов для преобразования состояния $|\Psi_1\rangle$ в состояния $|\Psi_1\rangle \dots |\Psi_8\rangle$

k	Состояние	Оператор для преобразования $\|\Psi_1\rangle \to \|\Psi_k\rangle$	Трехбитовая строка, соответствующая $\|\Psi_k\rangle$
1	$\|\Psi_1\rangle = (\|000\rangle + \|111\rangle)/\sqrt{2}$	$I \otimes I \otimes I$	000
2	$\|\Psi_2\rangle = (\|000\rangle - \|111\rangle)/\sqrt{2}$	$I \otimes \sigma_z \otimes I$	001
3	$\|\Psi_3\rangle = (\|100\rangle + \|011\rangle)/\sqrt{2}$	$\sigma_x \otimes I \otimes I$	010
4	$\|\Psi_4\rangle = (\|100\rangle - \|011\rangle)/\sqrt{2}$	$i\sigma_y \otimes I \otimes I$	011
5	$\|\Psi_5\rangle = (\|010\rangle + \|101\rangle)/\sqrt{2}$	$I \otimes \sigma_x \otimes I$	100
6	$\|\Psi_6\rangle = (\|010\rangle - \|101\rangle)/\sqrt{2}$	$I \otimes i\sigma_y \otimes I$	101
7	$\|\Psi_7\rangle = (\|110\rangle + \|001\rangle)/\sqrt{2}$	$\sigma_x \otimes \sigma_x \otimes I$	110
8	$\|\Psi_8\rangle = (\|110\rangle - \|001\rangle)/\sqrt{2}$	$i\sigma_y \otimes \sigma_x \otimes I$	111

В таблице 1 $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ — тождественный оператор; $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$ и $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ — операторы Паули.

Опишем теперь детально пинг-понг протокол с использованием ГХЦ — триплетов и квантового сверхплотного кодирования.

Шаг 1. Боб приготавливает три кубита в состоянии $|\Psi_1\rangle$.

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

Шаг 3. Алиса получает два кубита от Боба. С вероятностью *p* она переключается в режим контроля подслушивания и выполняет шаг 4, иначе Алиса переключается в режим передачи сообщения и выполняет шаги с 5-го по 7-й.

Шаг 4. Контроль подслушивания может быть выполнен квантовыми измерениями состояний кубитов таким образом, чтобы при этих измерениях разрушилась запутанность состояния $|\Psi_1\rangle$. Возможны несколько вариантов таких измерений для состояния $|\Psi_1\rangle$. Рассмотрим один из вариантов.

Алиса сообщает Бобу по обычному незащищенному каналу о переключении в режим контроля подслушивания. Тогда Боб случайным образом выбирает один из двух измерительных базисов — $B_z = \{|0\rangle\ \langle 0|\ ;\ |1\rangle\ \langle 1|\}$ или $B_x = \{|+\rangle\ \langle +|\ ;\ |-\rangle\ \langle -|\}$, где $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ и $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, а затем выполняет измерение состояния своего кубита в выбранном базисе.

В результате измерения в базисе B_z Боб получит $|0\rangle$ с вероятностью 1/2, а состояние триплета после измерения будет $|000\rangle$. Тогда Боб сообщает Алисе по обычному каналу, что он выбрал базис B_z, а также сообщает результат своего измерения. Алиса выполняет измерения состояний двух своих кубитов также в базисе B_z, при этом ее результат должен быть $|0\rangle$, $|0\rangle$. С вероятностью 1/2 Боб получит результат $|1\rangle$ и состояние триплета будет $|111\rangle$. Тогда Алиса, выполнив измерения в том же базисе, должна получить $|1\rangle$, $|1\rangle$. Если же результаты Алисы отличаются от приведенных, это свидетельствует либо о вмешательстве Евы, либо об ошибках, возникающих при передаче кубитов по квантовому каналу. Будем считать, что Алиса и Боб используют идеальный квантовый канал. Тогда в случае несовпадения результатов Алисы с теми, которые она должна получить, Алиса и Боб делают вывод о наличии подслушивания и прерывают передачу. Если же результаты измерений Алисы правильные, то переход к шагу 1.

Аналогично, если Боб выбирает базис B_x, то он с вероятностью 1/2 получит $|+\rangle$ и состояние триплета будет $|\Psi^+\rangle \otimes |+\rangle$, или Боб получит $|-\rangle$ и состояние триплета будет $|\Psi^-\rangle \otimes |-\rangle$, где $|\Psi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ и $|\Psi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ — два из состояний Белла. Тогда после получения сообщения от Боба о выбранном базисе и результате измерения Алиса измеряет два своих кубита в базисе Белла и в первом случае должна получить $|\Psi^+\rangle$, а во втором $|\Psi^-\rangle$. Если это не так, то протокол прерывается, иначе переход к шагу 1.

Отметим, что использование двух базисов для контроля подслушивания необходимо по причине того, что в противном случае, т.е. при использовании только одного измерительного базиса, Ева имеет возможность провести необнаруживаемую атаку на пинг-понг протокол. В частности, при атаке на протокол с белловскими состояниями и квантовым сверхплотным кодированием Ева может получить до 50 % информации в невидимом режиме подслушивания [3]. Однако в силу вероятностного характера переключения Алисы и Боба в режим контроля подслушивания, а также возможности для Евы выбрать определенные параметры своих квантовых проб, даже при использовании двух измерительных базисов атака Евы не всегда будет обнаружена сразу, что и означает квазибезопасность пинг-понг протокола. Это свойство будет прису-

ще всем вариантам пинг-понг протокола независимо от того, сколько перепутанных кубитов используется, и может быть устранено дополнительными процедурами классической криптографии.

Шаг 5. В соответствие со своей текущей трехбитовой строкой, Алиса выбирает одну из восьми кодирующих операций (см. таблицу 1), выполняет эту операцию над двумя своими кубитами, а затем отправляет эти кубиты обратно Бобу по квантовому каналу. Отметим, что если Ева не выполняла никаких операций над двумя кубитами, посланными первоначально от Боба к Алисе, то она не сможет получить никакой информации, перехватив эти кубиты на пути от Алисы к Бобу, поскольку она не имеет доступа к третьему кубиту, находящемуся у Боба. Согласно законам квантовой механики невозможно, выполнив измерения только над двумя кубитами, достоверно различить полностью перепутанные трехкубитные состояния $|\Psi_1\rangle \dots |\Psi_8\rangle$. Таким образом, контроль подслушивания, выполняемый после передачи Боб $\rightarrow$ Алиса, обеспечивает квазисекретность пинг-понг протокола.

Шаг 6. Получив кубиты от Алисы, Боб выполняет измерение над всеми тремя кубитами в ГХЦ-базисе, что позволяет ему достоверно определить состояние, созданное кодирующей операцией Алисы, и тем самым определить трехбитовую строку, которую она послала. ГХЦ-базис представляет собой набор из восьми операторов: $GHZ = \{|\Psi_k\rangle \langle\Psi_k|\}$, где $k = 1 \dots 8$.

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

Рассмотрим теперь пинг-понг протокол с использованием шестнадцати четырехкубитных ГХЦ-состояний, который позволяет передать четыре классических бита за один цикл протокола. Четырехкубитные ГХЦ-состояния могут быть преобразованы одно в другое применением однокубитных унитарных операторов к любым трем из четырех кубитов. Предполагая, что начальным состоянием, которое готовит Боб, является $|\Psi_1\rangle$, построим набор унитарных операторов, преобразующих $|\Psi_1\rangle$ в $|\Psi_1\rangle \dots |\Psi_{16}\rangle$, соответственно (табл. 2).

Таблица 2

Набор унитарных операторов для преобразования состояния $|\Psi_1\rangle$ в состояния $|\Psi_1\rangle \dots |\Psi_{16}\rangle$

k	Состояние $\lvert\Psi_k\rangle$	Оператор для преобразования $\lvert\Psi_1\rangle \rightarrow \lvert\Psi_k\rangle$	Четырехбитовая строка, соответствующая $\lvert\Psi_k\rangle$
1	$\lvert\Psi_1\rangle = (\lvert 0000\rangle + \lvert 1111\rangle)/\sqrt{2}$	$I \otimes I \otimes I \otimes I$	0000
2	$\lvert\Psi_2\rangle = (\lvert 0000\rangle - \lvert 1111\rangle)/\sqrt{2}$	$\sigma_z \otimes I \otimes I \otimes I$	0001
3	$\lvert\Psi_3\rangle = (\lvert 0010\rangle + \lvert 1101\rangle)/\sqrt{2}$	$I \otimes I \otimes \sigma_x \otimes I$	0010
4	$\lvert\Psi_4\rangle = (\lvert 0010\rangle - \lvert 1101\rangle)/\sqrt{2}$	$I \otimes I \otimes i\sigma_y \otimes I$	0011
5	$\lvert\Psi_5\rangle = (\lvert 1000\rangle + \lvert 0111\rangle)/\sqrt{2}$	$\sigma_x \otimes I \otimes I \otimes I$	0100
6	$\lvert\Psi_6\rangle = (\lvert 1000\rangle - \lvert 0111\rangle)/\sqrt{2}$	$i\sigma_y \otimes I \otimes I \otimes I$	0101
7	$\lvert\Psi_7\rangle = (\lvert 0100\rangle + \lvert 1011\rangle)/\sqrt{2}$	$I \otimes \sigma_x \otimes I \otimes I$	0110
8	$\lvert\Psi_8\rangle = (\lvert 0100\rangle - \lvert 1011\rangle)/\sqrt{2}$	$I \otimes i\sigma_y \otimes I \otimes I$	0111
9	$\lvert\Psi_9\rangle = (\lvert 1010\rangle + \lvert 0101\rangle)/\sqrt{2}$	$\sigma_x \otimes I \otimes \sigma_x \otimes I$	1000
10	$\lvert\Psi_{10}\rangle = (\lvert 1010\rangle - \lvert 0101\rangle)/\sqrt{2}$	$\sigma_x \otimes I \otimes i\sigma_y \otimes I$	1001
11	$\lvert\Psi_{11}\rangle = (\lvert 0110\rangle + \lvert 1001\rangle)/\sqrt{2}$	$I \otimes \sigma_x \otimes \sigma_x \otimes I$	1010
12	$\lvert\Psi_{12}\rangle = (\lvert 0110\rangle - \lvert 1001\rangle)/\sqrt{2}$	$I \otimes \sigma_x \otimes i\sigma_y \otimes I$	1011
13	$\lvert\Psi_{13}\rangle = (\lvert 1100\rangle + \lvert 0011\rangle)/\sqrt{2}$	$\sigma_x \otimes \sigma_x \otimes I \otimes I$	1100
14	$\lvert\Psi_{14}\rangle = (\lvert 1100\rangle - \lvert 0011\rangle)/\sqrt{2}$	$\sigma_x \otimes i\sigma_y \otimes I \otimes I$	1101

15	$\|\Psi_{15}\rangle = (\|1110\rangle + \|0001\rangle)/\sqrt{2}$	$\sigma_x \otimes \sigma_x \otimes \sigma_x \otimes I$	1110
16	$\|\Psi_{16}\rangle = (\|1110\rangle - \|0001\rangle)/\sqrt{2}$	$\sigma_x \otimes \sigma_x \otimes i\sigma_y \otimes I$	1111

Приведем пошаговое описание пинг-понг протокола с ГХЦ-четверками кубитов и квантовым сверхплотным кодированием.

Шаг 1. Боб приготавливает четверку кубитов в состоянии $|\Psi_1\rangle$.

Шаг 2. Он оставляет у себя четвертый кубит и посылает Алисе первые три по квантовому каналу связи.

Шаг 3. Алиса получает три кубита от Боба. С вероятностью *p* она переключается в режим контроля подслушивания и выполняет шаг 4, иначе Алиса переключается в режим передачи сообщения и выполняет шаги с 5-го по 7-й.

Шаг 4. Как и для протокола с ГХЦ-триплетами, контроль подслушивания можно выполнить, измеряя состояния кубитов таким образом, чтобы при измерениях разрушилась запутанность состояния $|\Psi_1\rangle$. Рассмотрим один из возможных вариантов.

Алиса сообщает Бобу по обычному незащищенному каналу о переключении в режим контроля подслушивания. Тогда Боб случайным образом выбирает один из измерительных базисов — B_z или B_x, а затем измеряет состояние своего кубита в выбранном базисе.

В результате измерения в базисе B_z Боб получит $|0\rangle$ с вероятностью $1/2$ и состояние четверки кубитов после измерения будет $|0000\rangle$. Боб сообщает Алисе, что он выбрал базис B_z, а также сообщает результат своего измерения. Алиса выполняет измерения состояний своих трех кубитов также в базисе B_z, при этом ее результат должен быть $|0\rangle$, $|0\rangle$, $|0\rangle$. Аналогично, с вероятностью $1/2$ Боб получит результат $|1\rangle$ и состояние четверки станет $|1111\rangle$. Тогда Алиса, выполнив измерение в том же базисе, должна получить $|1\rangle$, $|1\rangle$, $|1\rangle$.

Если Боб выбирает измерительный базис B_x, то он получит результат $|+\rangle$ или $|-\rangle$ с равной вероятностью. Тогда Алиса должна выполнить измерения в этом же базисе. Для каждого из возможных результатов Боба, при отсутствии подслушивания, Алиса может получить четыре разных последовательности результатов, но только эти последовательности (табл. 3).

Таблица 3

Результаты измерений Алисы и Боба в базисе B_x при контроле подслушивания в пинг-понг протоколе с ГХЦ-четверками кубитов

Результат Боба	Результаты Алисы			Результат Боба	Результаты Алисы		
кубит 4	кубит 1	кубит 2	кубит 3	кубит 4	кубит 1	кубит 2	кубит 3
$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	$\|-\rangle$
	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$		$\|-\rangle$	$\|+\rangle$	$\|+\rangle$
	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$		$\|+\rangle$	$\|-\rangle$	$\|+\rangle$
	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$		$\|+\rangle$	$\|+\rangle$	$\|-\rangle$

Если результаты измерений Боба и Алисы согласуются, то переход к шагу 1, иначе протокол прерывается.

Шаг 5. В соответствии со своей текущей четырехбитовой строкой Алиса выбирает одну из шестнадцати кодирующих операций (см. таблицу 2) и выполняет эту операцию над тремя своими кубитами. Алиса отправляет эти три кубита обратно Бобу по квантовому каналу.

Шаг 6. Получив кубиты от Алисы, Боб выполняет измерение над всеми четырьмя кубитами в ГХЦ-базисе для четырех кубитов, что позволяет ему достоверно определить состояние,

созданное кодирующей операцией Алисы, и тем самым определить четырехбитовую строку, которую она послала.

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

Таким образом, предложено два новых варианта пинг-понг протокола КБПС: с ГХЦ-триплетами и с ГХЦ-четверками кубитов, позволяющих передать за один цикл протокола три и четыре бита информации, соответственно. Разработаны схемы измерений для процедуры контроля подслушивания, которая необходима для обеспечения квазибезопасности протоколов. Даны детальные пошаговые описания предложенных протоколов.

Литература

1. Нильсен М. Квантовые вычисления и квантовая информация / Нильсен М., Чанг И. — М.: Мир, 2006. — 824 с.
2. Boström K. Deterministic secure direct communication using entanglement / Boström K., Felbinger T. // Physical Rev. Letters. — 2002. — Vol. 89, № 18. — Art. 187902.
3. Василиу Е.В. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием // Зб. наук. пр. ОНАЗ ім. О.С. Попова. — Одеса, 2007. — № 1. — С. 32 — 38.
4. Cai Q.Y. Improving the capacity of the Boström — Felbinger protocol / Cai Q.Y., Li B.W. // Physical Review A. — 2004. — V. 69, № 5. — Art. 054301.
5. Wang Ch. Multi-step quantum secure direct communication using multi-particle Greenberger-Horne-Zeilinger state / Wang Ch., Deng F.G., Long G.L. // Optics Communications. — 2005. — Vol. 253, № 1. — P. 15 — 20.
6. Wang J. Multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state / Wang J., Zhang Q., Tang C.J. // Optics Communications. — 2006. — Vol. 266, № 2. — P. 732 — 737.

Поступила в редакцию 10 января 2008 г.