УДК 003.26:621.39+530.145

ПІНГ–ПОНГ ПРОТОКОЛ З ПОВНІСТЮ ПЕРЕПЛУТАНИМИ СТАНАМИ ПАР ТА ТРИПЛЕТІВ ТРИВИМІРНИХ КВАНТОВИХ СИСТЕМ

ВАСІЛІУ Є.В.

PING-PONG PROTOCOL WITH COMPLETELY ENTANGLED STATES OF PAIRS AND TRIPLETS OF THREE-DIMENSIONAL QUANTUM SYSTEMS

VASILIU E.V.

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

Анотація. *Запропоновано два нових варіанти пінг-понг протоколу квантового безпечного зв’язку з використанням повністю переплутаних станів пар та триплетів тривимірних квантових систем. Ці варіанти пінг-понг протоколу мають більшу інформаційну місткість, ніж відповідні варіанти протоколу з парами та триплетами переплутаних кубітів. Розроблено схеми кодування та схеми вимірювань для режиму контролю підслуховування. Дано детальні описи запропонованих протоколів.*

Summary. *Two new versions of the ping-pong protocol of a quantum secure direct communication using completely entangled states of pairs and triplets of three-dimensional quantum systems are offered. These variants of the ping-pong protocol possess greater information capacity, than corresponding variants of the protocol with pairs and triplets of entangled qubits. The coding schemes and the measurements schemes for an eavesdropping control mode are developed. Detailed descriptions of the offered protocols are given.*

Захист від витоку конфіденційної інформації до неавторизованих осіб є однією з найважливіших проблем сучасного інформаційного суспільства. Виниклий в середині 80-х років XX століття новий напрям захисту інформації в телекомунікаційних мережах, що отримав назву квантової криптографії, швидко розвивається в останнє десятиріччя [1]. Одним з напрямів квантової криптографії є квантовий безпечний прямий зв’язок, де легітимні користувачі обмінюються квантовими частками по квантовому каналу зв’язку і виконують певні операції і вимірювання над цими частками, а також обмінюються додатковою інформацією по звичайному (не квантовому) каналу зв’язку з автентифікацією [2 – 14]. Практично в якості квантових часток використовують фотони, а як квантові канали – оптоволоконні лінії зв’язку. При цьому безпека передачі інформації з використанням квантових протоколів безпечного зв’язку гарантується законами квантової фізики.

На теперішній час запропоновано декілька десятків різних за призначенням протоколів квантового безпечного зв’язку. Серед них протоколи для безпосередньої передачі повідомлень між двома користувачами [2 – 5], протоколи для передачі повідомлень від одного користувача до іншого під контролем третьої довіреної сторони [6, 7], протоколи для передачі повідомлень від одного користувача до багатьох і від багатьох до одного, а також протоколи квантових конференцій [8 – 11]. Більшість із цих протоколів ґрунтується на створенні і подальшому розподілі між користувачами переплутаних станів двох або більшої кількості кубітів (дворівневих квантових систем). Крім того, більшість із запропонованих протоколів для забезпечення секретності вимагають передачі кубітів блоками, причому довжина цих блоків, як правило, повинна значно перевищувати довжину самого повідомлення, що передається. Ці блоки кубітів кожний з користувачів повинен зберігати до завершення всього протоколу, для чого необхідна довгочасна квантова пам’ять великого об’єму. Технологія створення такої квантової пам’яті активно розробляється на даний час, також і у зв’язку з проблемою створення квантових комп’ютерів, проте ця технологія поки що далека від масового застосування в стандартному телекомунікаційному устаткуванні. Тому певну перевагу мають протоколи, в яких необхідно зберігати в квантовій пам'яті тільки один або невелику групу кубітів протягом одного циклу протоколу. До таких протоколів відноситься так званий пінг-понг протокол [2], призначений для безпечної передачі повідомлень від одного легітимного користувача (Аліси) до іншого (Боба).

Початковий варіант пінг-понг протоколу [2] з використанням пар повністю переплутаних кубітів має інформаційну місткість в 1 біт на цикл протоколу. Використовуючи квантове щільне кодування, можна збільшити інформаційну місткість до 2 бітів на цикл [12, 13]. Далі, для реалізації протоколу можна використовувати переплутані трійки, четвірки і т.д. кубітів [14]. Пінг-понг протокол з групою з n переплутаних кубітів та квантовим щільним кодуванням має інформаційну місткість n бітів на цикл. На даний час в експерименті досягнуто переплутування групи з 10 кубітів, проте поки що це технологічно достатньо складна операція [15].

З іншого боку, інформаційну місткість пінг-понг протоколу можна збільшити, використовуючи замість кубітів багатовимірні квантові системи (кудити) та квантове щільне кодування для кудитів. Так, протокол з переплутаними парами тривимірних квантових систем (кутритів) буде мати місткість $\log_2 9 \approx 3{,}17$ бітів на цикл замість двох бітів на цикл для протоколу з парами кубітів, а протокол з переплутаними трійками кутритів – $\log_2 27 \approx 4{,}75$ бітів на цикл. З технологічної точки зору оперувати з кутритами поки складніше, ніж з кубітами, проте ряд експериментів по створенню переплутаних пар кутритів вже виконаний [16, 17]. Крім того, відомо, що квантові протоколи розподілу ключів з використанням багатовимірних квантових систем мають більш високий рівень безпеки, а також більш стійкі до шуму в квантовому каналі, ніж протоколи з використанням кубітів [18, 19]. Для квантових протоколів безпечного зв'язку і, зокрема, для пінг-понг протоколу це питання до теперішнього часу не досліджено.

Щоб визначити, чи є перевага у використовуванні кудитів для пінг-понг протоколу та інших квантових протоколів безпечного зв'язку з точки зору їх стійкості до атак, необхідно спочатку розробити такі протоколи, а потім дослідити їх стійкість до найбільш сильних атак, що допускаються законами квантової механіки. В роботі [20] запропонований протокол квантового безпечного зв'язку з парами переплутаних кутритів, що використовує ідею пінг-понг протоколу, а також передачу кутритів блоками, що потребує наявності великої квантової пам'яті. Проте в цій роботі не розглянуті повністю навіть операції, необхідні для контролю підслуховування, не говорячи вже про аналіз сильних атак на запропонований протокол. Метою цієї роботи є розробка всіх процедур, необхідних для реалізації пінг-понг протоколу, що не потребує великої квантової пам'яті, з парами та триплетами повністю переплутаних кутритів та квантовим щільним кодуванням. Аналіз атак на ці варіанти протоколу, який дозволить визначити їх стійкість і порівняти її із стійкістю варіантів пінг-понг протоколу з кубітами, буде виконаний в окремій роботі.

1. ПІНГ-ПОНГ ПРОТОКОЛ З ПАРАМИ ПОВНІСТЮ ПЕРЕПЛУТАНИХ КУТРИТІВ

Всі варіанти пінг-понг протоколу з кубітами мають асимптотичну безпеку, тобто атака агента, що підслуховує (Єви), буде виявлена, проте до цього вона зможе отримати деяку кількість інформації, залежну від кількості переплутаних кубітів, що використовуються для реалізації протоколу [2, 21]. Тому безпека всіх варіантів пінг-понг протоколу з кубітами повинна бути підсилена з використанням спеціального методу оборотного хешування, що дозволяє зробити перехоплену Євою на початковому етапі протоколу інформацію даремною для неї [22]. Ми припускаємо, що така процедура знадобиться і для протоколів з кутритами, оскільки ці протоколи теж будуть мати асимптотичну безпеку. Це випливає з аналогії процедур контролю підслуховування для пінг-понг протоколів з кубітами і з кутритами. Ці процедури ґрунтуються на загальних властивостях переплутаних станів, які не залежать від розмірності квантових систем, а саме на тому, що акт перехоплення руйнує переплутаність і тим самим виявляються операції агента, що підслуховує, в квантовому каналі.

Оскільки атаки на протоколи з кутритами поки що не проаналізовані, то неможливо повністю розробити відповідну процедуру підсилення безпеки і нижче розглядається пінг-понг протокол з парами кутритів та протокол з триплетами кутритів без додаткового підсилення безпеки. В цій роботі розробляються тільки процедури контролю підслуховування, необхідні для забезпечення асимптотичної безпеки цих двох варіантів пінг-понг протоколу з кутритами.

Існує дев'ять повністю переплутаних ортонормованих станів пари кутритів $|\Psi_{00}\rangle \ldots |\Psi_{22}\rangle$ (табл. 1), які утворюють базис в гильбертовому просторі двох кутритів і є узагальненням станів Бела на кутрити [23]. Ці стані перетворюються друг у друга дією локального унітарного оператору на будь-який один з кутритів. Припустимо, що початковим станом, який в пінг-понг протоколі готує приймаюча сторона – Боб, є $|\Psi_{00}\rangle$. Тоді необхідно побудувати набір унітарних операцій над одним з двох кутритів в стані $|\Psi_{00}\rangle$, перетворюючих цей стан в стани $|\Psi_{00}\rangle \ldots |\Psi_{22}\rangle$ відповідно (над другим кутритом при цьому не потрібно проводити ніяких операцій, тобто можна сказати, що на нього діє тотожний оператор). Відповідний набір операцій отриманий в [23] в матричному вигляді. Приведемо їх в операторному вигляді (див. табл. 1). Також в табл. 1 приведені рядки з двох тритів, які будуть відповідати кожному із станів $|\Psi_{00}\rangle \ldots |\Psi_{22}\rangle$. Про таку відповідність (схему кодування) Аліса і Боб повинні домовитися до початку протоколу.

Таблиця 1 – Набір унітарних операцій для перетворення $|\Psi_{00}\rangle$ в $|\Psi_{00}\rangle \ldots |\Psi_{22}\rangle$ – схема кодування інформації

Стан $\lvert\Psi_{ij}\rangle$	Оператор U_{ij} для перетворення $\lvert\Psi_{00}\rangle$ в $\lvert\Psi_{ij}\rangle$, який діє на другий кутрит	Рядок тритів, що відповідає $\lvert\Psi_{ij}\rangle$
$\lvert\Psi_{00}\rangle = (\lvert 00\rangle + \lvert 11\rangle + \lvert 22\rangle)/\sqrt{3}$	$U_{00} = \lvert 0\rangle\langle 0\rvert + \lvert 1\rangle\langle 1\rvert + \lvert 2\rangle\langle 2\rvert$	00
$\lvert\Psi_{10}\rangle = (\lvert 00\rangle + e^{2\pi i/3}\lvert 11\rangle + e^{4\pi i/3}\lvert 22\rangle)/\sqrt{3}$	$U_{10} = \lvert 0\rangle\langle 0\rvert + e^{2\pi i/3}\lvert 1\rangle\langle 1\rvert + e^{4\pi i/3}\lvert 2\rangle\langle 2\rvert$	10
$\lvert\Psi_{20}\rangle = (\lvert 00\rangle + e^{4\pi i/3}\lvert 11\rangle + e^{2\pi i/3}\lvert 22\rangle)/\sqrt{3}$	$U_{20} = \lvert 0\rangle\langle 0\rvert + e^{4\pi i/3}\lvert 1\rangle\langle 1\rvert + e^{2\pi i/3}\lvert 2\rangle\langle 2\rvert$	20
$\lvert\Psi_{01}\rangle = (\lvert 01\rangle + \lvert 12\rangle + \lvert 20\rangle)/\sqrt{3}$	$U_{01} = \lvert 1\rangle\langle 0\rvert + \lvert 2\rangle\langle 1\rvert + \lvert 0\rangle\langle 2\rvert$	01
$\lvert\Psi_{11}\rangle = (\lvert 01\rangle + e^{2\pi i/3}\lvert 12\rangle + e^{4\pi i/3}\lvert 20\rangle)/\sqrt{3}$	$U_{11} = \lvert 1\rangle\langle 0\rvert + e^{2\pi i/3}\lvert 2\rangle\langle 1\rvert + e^{4\pi i/3}\lvert 0\rangle\langle 2\rvert$	11
$\lvert\Psi_{21}\rangle = (\lvert 01\rangle + e^{4\pi i/3}\lvert 12\rangle + e^{2\pi i/3}\lvert 20\rangle)/\sqrt{3}$	$U_{21} = \lvert 1\rangle\langle 0\rvert + e^{4\pi i/3}\lvert 2\rangle\langle 1\rvert + e^{2\pi i/3}\lvert 0\rangle\langle 2\rvert$	21
$\lvert\Psi_{02}\rangle = (\lvert 02\rangle + \lvert 10\rangle + \lvert 21\rangle)/\sqrt{3}$	$U_{02} = \lvert 2\rangle\langle 0\rvert + \lvert 0\rangle\langle 1\rvert + \lvert 1\rangle\langle 2\rvert$	02
$\lvert\Psi_{12}\rangle = (\lvert 02\rangle + e^{2\pi i/3}\lvert 10\rangle + e^{4\pi i/3}\lvert 21\rangle)/\sqrt{3}$	$U_{12} = \lvert 2\rangle\langle 0\rvert + e^{2\pi i/3}\lvert 0\rangle\langle 1\rvert + e^{4\pi i/3}\lvert 1\rangle\langle 2\rvert$	12
$\lvert\Psi_{22}\rangle = (\lvert 02\rangle + e^{4\pi i/3}\lvert 10\rangle + e^{2\pi i/3}\lvert 21\rangle)/\sqrt{3}$	$U_{22} = \lvert 2\rangle\langle 0\rvert + e^{4\pi i/3}\lvert 0\rangle\langle 1\rvert + e^{2\pi i/3}\lvert 1\rangle\langle 2\rvert$	22

Опишемо тепер детально пінг-понг протокол з використанням пар повністю переплутаних кутритів.

Аліса заздалегідь розбиває свій рядок тритів на пари тритів. Якщо її повідомлення спочатку є бітовим рядком, то його необхідно перетворити в рядок тритів.

Крок 1. Боб готує пару кутритів в стані $|\Psi_{00}\rangle$, використовуючи, наприклад, метод [17]. В цьому випадку кутрит є одиночним фотоном, а пара таких кутритів – фотонів переплутується по їх орбітальному кутовому моменту.

Крок 2. Боб залишає у себе перший кутрит ("домашній") і посилає Алісі другий ("що передається") по квантовому каналу зв'язку, наприклад, оптоволоконної лінії (мал. 1).

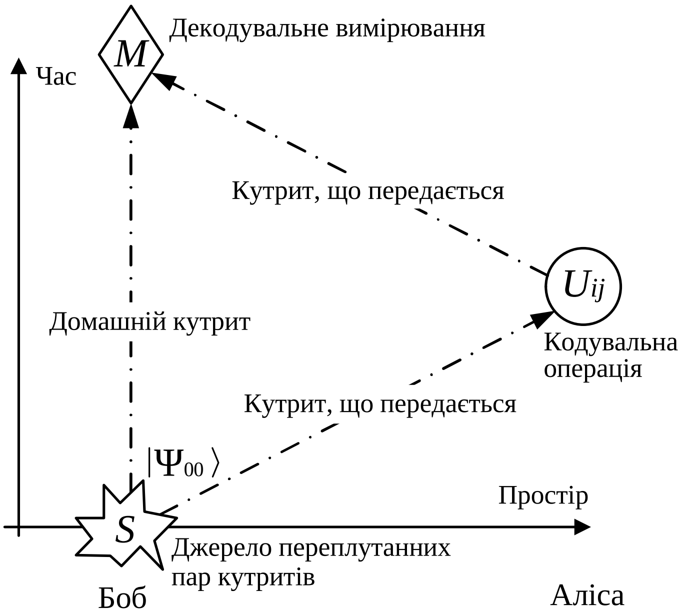

Рисунок 1 – Режим передавання повідомлення

Крок 3. Аліса отримує кутрит, що передається, від Боба. З імовірністю q вона переходить в режим контролю підслуховування і виконується крок 4, інакше Аліса переходить в режим передачі повідомлення і виконуються кроки з 5-го по 7-ий.

Крок 4. Контроль підслуховування виконується квантовими вимірюваннями станів кутритів. При цьому стан кожного з кутритів вимірюється окремо – один Алісою, інший Бобом, а вимірювання, як і для пінг-понг протоколу з кубітами, необхідно виконувати в двох різних базисах, перемикаючись між ними випадковим чином. У разі застосування тільки одного вимірювального базису для контролю підслуховування Єва має можливість так підібрати параметри своїх допоміжних квантових систем, які використовуються для атаки, що легітимні користувачі не виявлять операцій Єви.

Краще всього для контролю підслуховування використовувати взаємно незміщені (додаткові) базиси, для яких будь-які два базисні вектори, що відносяться до різних базисів, задовольняють співвідношенню $\langle e_i | e_j \rangle = 1/\sqrt{d}$, де d – розмірність гільбертового простору квантової системи (d = 3 для кутритів).

Для кутритів існує чотири взаємно незміщені базиси, з яких два називаються z-базисом та x-базисом [20], а інші назвемо v-базисом і t-базисом:

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

$$\begin{aligned} |x_0\rangle &= \left(|0\rangle + |1\rangle + |2\rangle\right)/\sqrt{3}, \\ |x_1\rangle &= \left(|0\rangle + e^{2\pi i/3}|1\rangle + e^{-2\pi i/3}|2\rangle\right)/\sqrt{3}, \\ |x_2\rangle &= \left(|0\rangle + e^{-2\pi i/3}|1\rangle + e^{2\pi i/3}|2\rangle\right)/\sqrt{3}; \end{aligned} \tag{2}$$

$$\begin{aligned} |v_0\rangle &= \left(e^{2\pi i/3}|0\rangle + |1\rangle + |2\rangle\right)/\sqrt{3}, \\ |v_1\rangle &= \left(|0\rangle + e^{2\pi i/3}|1\rangle + |2\rangle\right)/\sqrt{3}, \\ |v_2\rangle &= \left(|0\rangle + |1\rangle + e^{2\pi i/3}|2\rangle\right)/\sqrt{3}; \end{aligned} \tag{3}$$

$$|t_0\rangle = \left(e^{-2\pi i/3}|0\rangle + |1\rangle + |2\rangle\right)/\sqrt{3};$$
$$|t_1\rangle = \left(|0\rangle + e^{-2\pi i/3}|1\rangle + |2\rangle\right)/\sqrt{3};$$
$$|t_2\rangle = \left(|0\rangle + |1\rangle + e^{-2\pi i/3}|2\rangle\right)/\sqrt{3}. \qquad (4)$$

Аліса може вибрати для контролю підслуховування будь-які два з цих чотирьох базисів. Використання трьох, або всіх чотирьох базисів не збільшить імовірності виявлення підслуховування. В роботі обчислена таблиця результатів вимірювань Аліси і Боба у всіх чотирьох базисах. Результат зручніше представити не у вигляді таблиці, а записавши початковий стан $|\Psi_{00}\rangle$ в базисах (1) – (4):

$$|\Psi_{00}\rangle = \left(|00\rangle + |11\rangle + |22\rangle\right)/\sqrt{3} = \left(|x_0x_0\rangle + |x_1x_2\rangle + |x_2x_1\rangle\right)/\sqrt{3} =$$
$$= \left(|t_0v_0\rangle + |t_1v_1\rangle + |t_2v_2\rangle\right)/\sqrt{3} = \left(|v_0t_0\rangle + |v_1t_1\rangle + |v_2t_2\rangle\right)/\sqrt{3}. \qquad (5)$$

Після вибору Аліси Боб також повинен вибрати два базиси, але його вибір обумовлений вибором Аліси, як це випливає з (5). Так, якщо Аліса вибрала *z*-базис та *x*-базис, то Боб повинен також вибрати ці базиси. А якщо Аліса вибрала, наприклад, *x*-базис та *v*-базис, то Боб повинен вибрати *x*-базис та *t*-базис. Аліса і Боб можуть домовитися про те, які базиси вони будуть використовувати, до початку протоколу, щоб наперед налагодити свою апаратуру, хоча така попередня домовленість, в принципі, не є обов’язковою.

Таким чином, в режимі контролю підслуховування Аліса вибирає випадково один з двох взаємно незміщених базисів і вимірює в цьому базисі стан отриманого від Боба кутриту. Потім вона повідомляє Бобу по класичному (не квантовому) відкритому каналу результат вимірювання і використаний базис (мал. 2). В будь-якому з базисів Аліса отримає один з трьох можливих результатів вимірювання з однаковою імовірністю $1/3$. Потім Боб, вибравши відповідний базис і виконавши вимірювання стану свого домашнього кутриту, повинен отримати визначений результат (з імовірністю 1), згідно з (5). Так, наприклад, якщо Аліса вибрала *x*-базис і отримала результат "1", то Боб повинен теж вибрати *x*-базис і його результат повинен бути "2". Або, наприклад, якщо Аліса вибрала *v*-базис і отримала результат "0", то, згідно з (5), Боб повинен вибрати *t*-базис і отримати результат "0". Аналогічно з (5) можна отримати всі інші можливі варіанти вимірювань.

Якщо результат вимірювання Боба правильний, то підслуховування немає. Боб повідомляє про це Алісу по класичному каналу, і вони переходять до кроку 1 протоколу. Якщо результат вимірювання Боба невірний, то робиться висновок про наявність підслуховування і протокол переривається.

Відзначимо, що коли результат вимірювання Боба невірний, то це може свідчити або про втручання Єви, або про помилки, що виникають при передачі кутритів по квантовому каналу зв’язку. Не існує способу розрізнити помилки, що виникають із цих двох причин [1]. Тому в шумному квантовому каналі пінг-понг протокол повинен бути вдосконалені. Тут розглянутий пінг-понг протокол тільки для ідеального квантового каналу.

Відзначимо також, що класичний канал, по якому Аліса і Боб обмінюються повідомленнями в режимі контролю підслуховування, може бути відкритим для пасивного прослуховування і немає необхідності шифрувати повідомлення, що передаються цим каналом. Проте Єва не повинна мати можливості змінювати повідомлення, що передаються в класичному каналі, інакше, контролюючи також і квантовий канал, вона може провести атаку "людина посередині". Таким чином, легітимні користувачі повинні забезпечувати кодом автентичності всі повідомлення, що передаються в класичному каналі.

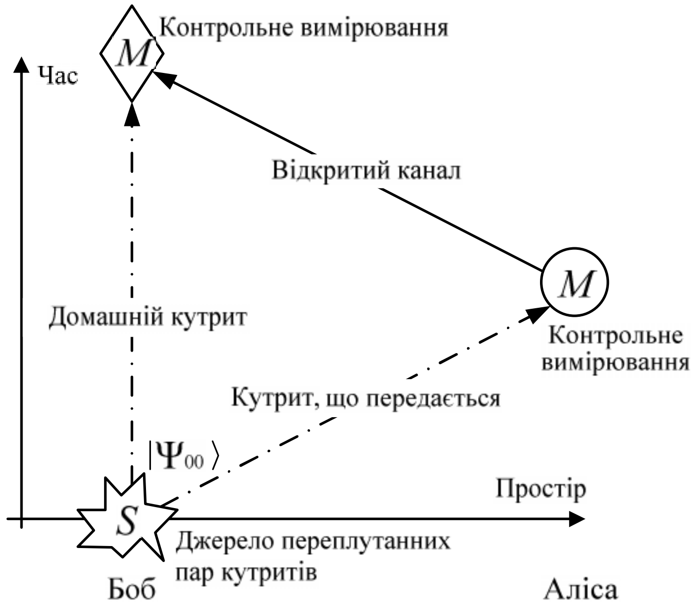

Рисунок 2 – Режим контролю підслуховування

Крок 5. У відповідності із своїм поточним дво-тритовим рядком, Аліса вибирає одну з дев'яти кодувальних операцій U_{ij} (див. табл. 1) і виконує цю операцію над отриманим нею від Боба кутритом. При цьому початковий стан пари кутритів $\left|\Psi_{00}\right\rangle$ перетвориться відповідно до операції, виконаної Алісою. Потім Аліса відправляє кутрит назад Бобу по квантовому каналу (див. мал. 1).

Крок 6. Отримавши кутрит, що передається, від Аліси, Боб виконує декодувальне вимірювання над парою кутритів в базисі Бела для кутритів, що дозволяє йому достовірно визначити стан, створений кодувальною операцією Аліси, і тим самим визначити дво-тритовий рядок, який вона послала. Набор проекційних операторів для вимірювань в базисі Бела для кутритів містить дев'ять операторів: $\left\{\left|\Psi_{ij}\right\rangle\left\langle\Psi_{ij}\right|\right\}$, де $i, j = 0\ldots2$.

Крок 7. Якщо повідомлення передано повністю, то протокол успішно закінчений, інакше перехід до кроку 1.

2. ПІНГ-ПОНГ ПРОТОКОЛ З ТРИПЛЕТАМИ ПОВНІСТЮ ПЕРЕПЛУТАНИХ КУТРИТІВ

Розглянемо тепер варіант пінг-понг протоколу з триплетами повністю переплутаних кутритів, інформаційна місткість якого на цикл протоколу майже в 1,5 рази вище за місткість протоколу з парами кутритів і в 1,58 рази вище за місткість протоколу з триплетами кубітів. Відзначимо, що коли ряд експериментів по переплутуванню пари кутритів виконаний до теперішнього часу [16, 17], то про експерименти по переплутуванню трійки кутритів автору нічого не відомо. Тому такий протокол поки, мабуть, є технічно не реалізовуваним. Проте прогрес в області створення устаткування для обробки квантової інформації дуже стрімкий, і робота з трійкою та більшою кількістю переплутаних три- і більш вимірних квантових систем стане реальністю, ймовірно, протягом найближчих декількох років.

Кроки протоколу з триплетами кутритів залишаються тими ж самими, що і для протоколу з парами кутритів. Зміни відбуваються в кодувальних операціях і процедурах вимірювань. Тому не будемо описувати протокол по кроках, а розглянемо тільки ті елементи протоколу, які відрізняються від протоколу з парами кутритів.

Існує двадцять сім повністю переплутаних ортонормованих станів триплету кутритів, які утворюють базис в гільбертовому просторі трьох тривимірних квантових систем. Ці стани можуть бути перетворені друг у друга локальними одночастковими операціями над будь-якими двома з трьох кутритів (квантове щільне кодування) [23]. Не будемо виписувати ці стани в явному вигляді, зважаючи на громіздкість, а приведемо тільки загальну формулу, з використанням якої можуть бути отримані явні вирази для всіх 27-ми станів [23]:

$$\left|\Psi_{k\,n\,m}\right\rangle = \frac{1}{\sqrt{3}}\sum_{j=0}^{2} e^{2\pi i\,jk/3}\left|\,j\right\rangle \otimes \left|\,j+n\,\mathrm{mod}3\right\rangle \left|\,j+m\,\mathrm{mod}3\right\rangle, \qquad (6)$$

де k, n, m = 0…2.

Боб готує стан $\left|\Psi_{000}\right\rangle = \left(\left|000\right\rangle + \left|111\right\rangle + \left|222\right\rangle\right)/\sqrt{3}$, потім залишає у себе перший кутрит і посилає Алісі інші два по квантовому каналу. В режимі передачі повідомлення Аліса виконує одну з 27-ми кодувальних операцій над двома кутритами і повертає обидва кутрити назад Бобу. Боб вимірює стан трьох кутритів в тричастковому базисі, де існує 27 проекційних операторів: $\left\{\left|\Psi_{knm}\right\rangle\left\langle\Psi_{knm}\right|\right\}$, k, n, m = 0…2. Таким чином, за один цикл протоколу можна передати три трити інформації. В табл. 2 приведений повний набір кодувальних операцій Аліси, (U_{ij} наведені в табл. 1). В дужках в заголовку таблиці вказаний номер кутриту, на який діє відповідний оператор.

Таблиця 2 – Набір унітарних операцій для перетворення $\left|\Psi_{000}\right\rangle$ в $\left|\Psi_{000}\right\rangle \ldots \left|\Psi_{222}\right\rangle$ – схема кодування інформації

$U_{n'm'}(3)$	$U_{nm}(2)$								
	U_{00}	U_{10}	U_{20}	U_{01}	U_{11}	U_{21}	U_{02}	U_{12}	U_{22}
U_{00}	$\left\|\Psi_{000}\right\rangle$	$\left\|\Psi_{100}\right\rangle$	$\left\|\Psi_{200}\right\rangle$	$\left\|\Psi_{010}\right\rangle$	$\left\|\Psi_{110}\right\rangle$	$\left\|\Psi_{210}\right\rangle$	$\left\|\Psi_{020}\right\rangle$	$\left\|\Psi_{120}\right\rangle$	$\left\|\Psi_{220}\right\rangle$
U_{01}	$\left\|\Psi_{001}\right\rangle$	$\left\|\Psi_{101}\right\rangle$	$\left\|\Psi_{201}\right\rangle$	$\left\|\Psi_{011}\right\rangle$	$\left\|\Psi_{111}\right\rangle$	$\left\|\Psi_{211}\right\rangle$	$\left\|\Psi_{021}\right\rangle$	$\left\|\Psi_{121}\right\rangle$	$\left\|\Psi_{221}\right\rangle$
U_{02}	$\left\|\Psi_{002}\right\rangle$	$\left\|\Psi_{102}\right\rangle$	$\left\|\Psi_{202}\right\rangle$	$\left\|\Psi_{012}\right\rangle$	$\left\|\Psi_{112}\right\rangle$	$\left\|\Psi_{212}\right\rangle$	$\left\|\Psi_{022}\right\rangle$	$\left\|\Psi_{122}\right\rangle$	$\left\|\Psi_{222}\right\rangle$

В режимі контролю підслуховування Аліса вимірює стани кутритів 2 і 3 окремо в одному з базисів (1) – (4), а потім повідомляє результати і вибрані базиси Бобу по класичному каналу. Боб проводить вимірювання стану 1-го кутриту у відповідному базисі і, як і для протоколу з парою кутритів, отримує визначений результат. В табл. 3 приведена розроблена схема вимірювань для випадку, коли Аліса вимірює окремо стани 2-го і 3-го кутритів в одному і тому ж базисі. Зрозуміло, можливі і інші схеми вимірювань, наприклад схема, в якій Аліса вимірює стани обох кутритів окремо, але в різних базисах, або схема, в якій Аліса вимірює обидва кутрити в базисі Бела для кутритів. Ми не розглядаємо всі ці схеми, оскільки для контролю підслуховування в протоколі достатньо тільки однієї схеми.

Відзначимо також, що схема для z-базису не наведена в табл. 3, тому що, на відміну від інших базисів, тут Аліса одержує результати "0", "1" або "2" з імовірністю $1/3$ тільки при вимірюванні стану 2-го кутриту. Після цього вимірювання стан $\left|\Psi_{000}\right\rangle$ колапсує в $\left|000\right\rangle$, $\left|111\right\rangle$ або $\left|222\right\rangle$ залежно від результату вимірювання Аліси, і результати вимірювань Алісою стану 3-го кутриту та Бобом стану 1-го кутриту визначені: вони повинні одержати "0", "0" у першому випадку, "1", "1" у другому і "2", "2" – у третьому.

Таблиця 3 - Схема вимірювань для контролю підслуховування в пінг-понг протоколі з триплетами кутритів

Результати Аліси, з імовірн.1/3 кожний		Результат Боба, з імовірн. 1 кожний	Результати Аліси, з імовірн. 1/3 кожний		Результат Боба, з імовірн. 1 кожний	Результати Аліси, з імовірн. 1/3 кожний		Результат Боба, з імовірн. 1 кожний
кутрит 2	кутрит 3	кутрит 1	кутрит 2	кутрит 3	кутрит 1	кутрит 2	кутрит 3	кутрит 1
вимірювальний базис *x*								
$\|x_0\rangle$	$\|x_0\rangle$	$\|x_0\rangle$	$\|x_1\rangle$	$\|x_0\rangle$	$\|x_2\rangle$	$\|x_2\rangle$	$\|x_0\rangle$	$\|x_1\rangle$
	$\|x_1\rangle$	$\|x_2\rangle$		$\|x_1\rangle$	$\|x_1\rangle$		$\|x_1\rangle$	$\|x_0\rangle$
	$\|x_2\rangle$	$\|x_1\rangle$		$\|x_2\rangle$	$\|x_0\rangle$		$\|x_2\rangle$	$\|x_2\rangle$
вимірювальний базис *v*								
$\|v_0\rangle$	$\|v_0\rangle$	$\|v_0\rangle$	$\|v_1\rangle$	$\|v_0\rangle$	$\|v_2\rangle$	$\|v_2\rangle$	$\|v_0\rangle$	$\|v_1\rangle$
	$\|v_1\rangle$	$\|v_2\rangle$		$\|v_1\rangle$	$\|v_1\rangle$		$\|v_1\rangle$	$\|v_0\rangle$
	$\|v_2\rangle$	$\|v_1\rangle$		$\|v_2\rangle$	$\|v_0\rangle$		$\|v_2\rangle$	$\|v_2\rangle$
вимірювальний базис *t*								
$\|t_0\rangle$	$\|t_0\rangle$	$\|t_0\rangle$	$\|t_1\rangle$	$\|t_0\rangle$	$\|t_2\rangle$	$\|t_2\rangle$	$\|t_0\rangle$	$\|t_1\rangle$
	$\|t_1\rangle$	$\|t_2\rangle$		$\|t_1\rangle$	$\|t_1\rangle$		$\|t_1\rangle$	$\|t_0\rangle$
	$\|t_2\rangle$	$\|t_1\rangle$		$\|t_2\rangle$	$\|t_0\rangle$		$\|t_2\rangle$	$\|t_2\rangle$

Таким чином, запропоновано два нових варіанти пінг-понг протоколу квантового безпечного зв'язку: з повністю переплутаними станами пар та триплетів кутритів. Ці варіанти пінг-понг протоколу дозволяють передати за один цикл два або три трити інформації відповідно, що значно більше інформаційної місткості протоколів з парами та триплетами кубітів. Розроблено схеми кодування інформації та схеми вимірювань для режиму контролю підслуховування. Дано детальні описи запропонованих протоколів.

Література

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

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

3. Deng F.-G., Long G.L., Liu X.-S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block // Physical Review A. – 2003. – V. 68, № 4. – 042317.

4. Man, Zh.-X, Zhang Zh.-J., Li Y. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations // Chinese Physics Letters. – 2005. – V. 22, №1. – P. 18 – 21.

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

6. Gao T., Yan F.-L., Wang Zh.-X. Quantum secure conditional direct communication via EPR pairs // International Journal of Modern Physics C. – 2005. – V. 16, № 8. – P. 1293 – 1301.

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

8. Gao T., Yan F.-L., Wang Zh.-X**.** Deterministic secure direct communication using GHZ states and swapping quantum entanglement// Journal of Physics A. – 2005. – V. 38, № 25. – P. 5761 – 5770.

9. Gao T., Yan F.-L., Wang Zh.-X. A Simultaneous quantum secure direct communication scheme between the central party and other *M* parties // Chinese Physics Letters. – 2005. – V. 22, № 10. – P. 2473 – 2476.

10. Deng F.-G., Li X.-H., Li Ch.-Y., Zhou P., Liang Y.-J., Zhou H.-Y. Multiparty quantum secret report // Chinese Physics Letters. – 2006. – V. 23, № 7. – P. 1676 – 1679.

11. Li X.-H., Li Ch.-Y., Deng F.-G., Zhou P., Liang Y.-J., Zhou H.-Y. Multiparty quantum remote secret conference // Chinese Physics Letters. – 2007. – V. 24, № 1. – P. 23 – 26.

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

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

14. Василиу Е.В., Василиу Л.Н. Пинг – понг протокол с трех– и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера // Труды Одесского политехнического университета. – 2008. – Вып. 1(29). – С. 171 – 176.

15. Experimental demonstration of a hyper – entangled ten – qubit Schrodinger cat state / Gao W.-B, Lu C.-Y., Yao X.-C. et al // [Електронний ресурс] http://arxiv.org/abs/0809.4277.

16. Thew T., Acin A., Zbinden H., Gisin N. Experimental realization of entangled qutrits for quantum communication // Quantum Information and Computation. – 2004. – V. 4, № 2. – P. 93 – 101.

17. Vaziri A., Pan J., Jennewein T., Weihs G., Zeilinger A. Concentration of higher dimensional entanglement: qutrits of photon orbital angular momentum // Physical Review Letters. – 2003. – V. 91, № 22. – 227902.

18. Cerf N.J., Bourennane M., Karlsson A., Gisin N. Security of quantum key distribution using d-level systems // Physical Review Letters. – 2002. – V. 88, № 12. – 127902.

19. Durt T., Kaszlikowski D., Chen J.-L., Kwek L. C. Security of quantum key distributions with entangled qudits // Physical Review A. – 2004. – V. 69, № 3. – 032313.

20. Wang Ch., Deng F.-G., Li Y.-S., Liu X.-S., Long G. L. Quantum secure direct communication with high dimension quantum superdense coding // Physical Review A. – 2005. – V. 71, № 4. – 044305.

21. Василиу Е.В., Василиу Л.Н. Оценка количества информации, попадающей к злоумышленнику, для трех вариантов пинг-понг протокола квантовой безопасной связи // Материали за IV международна научна практична конференция «Научно пространство на Европа – 2008», 15 – 30 апреля 2008 г. – София, «Бял ГРАД-БГ» ООД. – Т. 29. – С. 34 – 40.

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

23. Liu X.-S., Long G.L., Tong D.M., Li F. General scheme for superdense coding between multiparties // Physical Review A. – 2002. – V. 65, № 2. – 022304.