УДК 004.056.53+530.145 (045)

КВАНТОВИЙ ПРОТОКОЛ РОЗДІЛЕННЯ СЕКРЕТУ З ПАРАМИ ПЕРЕПЛУТАНИХ КУТРИТІВ НА ОСНОВІ ПІНГ-ПОНГ ПРОТОКОЛУ

ЛІМАРЬ І.В.

Одеська національна академія зв'язку ім. О.С. Попова,
вул. Кузнечна, 1, Одеса, 65029, Україна
quantum.biology@outlook.com

КВАНТОВЫЙ ПРОТОКОЛ РАЗДЕЛЕНИЯ СЕКРЕТА С ПАРАМИ ПЕРЕПУТАННЫХ КУТРИТОВ НА ОСНОВЕ ПИНГ-ПОНГ ПРОТОКОЛА

ЛИМАРЬ И.В.

Одесская национальная академия связи им. А.С. Попова,
ул. Кузнечная, 1, Одесса, 65029, Украина
quantum.biology@outlook.com

THE PING-PONG-BASED QUANTUM SECRET SHARING PROTOCOL WITH PAIRS OF ENTANGLED QUTRITS

LIMAR IGOR

O.S. Popov Odessa national academy of telecommunications
Kuznechna st., 1, Odessa, 65029, Ukraine
quantum.biology@outlook.com

Анотація. *Запропоновано новий квантовий протокол розділення секрету на основі пінг-понг протоколу квантового прямого безпечного зв'язку. У протоколі використовуються пари переплутаних кутритів, що дозволяє підвищити інформаційну місткість у порівнянні із протоколами на основі переплутаних кубітів. Застосовуваний у протоколі контроль прослуховування каналу, який виконується у випадкові моменти часу, дозволяє не прибігати до проблематичного, з урахуванням сучасних технологічних можливостей, використання квантової пам'яті. Коротко розглянуто стійкість запропонованого протоколу до атак.*

Ключові слова: *квантова криптографія, квантове розділення секрету, кутрити, квантова заплутаність, пінг-понг протокол.*

Аннотация. *Предложен новый квантовый протокол разделения секрета на основе пинг-понг протокола квантовой прямой безопасной связи. В протоколе используются пары перепутанных кутритов, что позволяет повысить информационную ёмкость по сравнению с протоколами на основе перепутанных кубитов. Примененный в протоколе контроль прослушивания канала, который выполняется в случайные моменты времени, позволяет не прибегать к проблематичному, с учетом современных технологических возможностей, использованию квантовой памяти. Кратко рассмотрена стойкость предложенного протокола к атакам.*

Ключевые слова: *квантовая криптография, квантовое разделение секрета, кутриты, квантовая запутанность, пинг-понг протокол.*

Abstract. *The new "ping-pong quantum secure direct communication"-based quantum secret sharing protocol is proposed. In the protocol the pairs of the entangled qutrits are used. It lets to increase the information capacity in comparison with "entangled qubits"-based protocols. The applied control of the channel eavesdropping, which is in progress in random instant of time, lets do not use the quantum memory, that is the problematical with taking into account the state-of-the-art technological possibilities. The ability of the protocol to resist by attacks is considered shortly.*

Key words: quantum cryptography, quantum secret sharing, qutrits, quantum entanglement, ping-pong protocol.

ПОСТАНОВКА ПРОБЛЕМИ

Відома в криптографії задача розділення секрету активно досліджується в останні 15 років на предмет її реалізації з використанням методів квантової криптографії [1]. Безумовною перевагою квантових протоколів розділення секрету (КПРС) над класичними є принци-

пова можливість завжди виявити прослуховування каналу зв'язку у випадку, якщо розділення секрету відбувається віддалено. Також КПРС завдяки використанню переплутаних квантових станів, як правило, більш захищені від нечесних дій учасників самого протоколу.

У той же час, однією із проблем квантових захищених комунікацій є необхідність підвищення пропускної здатності каналу. Вирішення цієї задачі можливо при використанні як можна більшої, наскільки це дозволяють сучасні технологічні можливості, розмірності квантових об'єктів-систем – кудитів [2-3]. Крім того, у квантовий криптографії взагалі та для схем розділення секрету, зокрема, актуальним є питання зберігання протягом певного часу в рамках циклу протоколу значного числа кудитів, що не є прийнятним при сьогоднішніх можливостях технічної реалізації. Альтернативою такому підходу є деякі прийоми, що реалізуються в рамках квантової комунікації, наприклад, контроль прослуховування каналу зв'язку, який виконується у випадкові моменти часу, чергуючись з передаванням корисної інформації. З врахуванням викладеного метою даної роботи є побудування ефективного протоколу розділення секрету з використанням тривимірних квантових систем і контролем прослуховування квантового каналу зв’язку.

1. РОЗДІЛЕННЯ СЕКРЕТУ НА ОСНОВІ СХЕМИ З ПАРАМИ ПОВНІСТЮ ПЕРЕПЛУТАНИХ КУТРИТІВ І МОЖЛИВІСТЮ КОНТРОЛЮ КАНАЛУ ЗВ'ЯЗКУ

Існує дев’ять повністю переплутаних ортогональних станів пари кутритів, які називають станами Белла для кутритів [4], вони наведені у таблиці 1. У запропонованій нами схемі (рис. 1) є три учасники процедури розділення секрету: Аліса, яка є дилером, Боб и Чарлі – це особи, які безпосередньо розділюють секрет.

Кодування інформації виконується за допомогою унітарних операторів. Список зазначених операторів, результати їх дії на другий кутрит у переплутаному стані $|\Psi_{00}\rangle$ та відповідний рядок з двох тритів наведені в таблиці 1. Відзначимо, що на перший кутрит діє одиничний оператор.

Таблиця 1 – Унітарні операції для перетворення стану $|\Psi_{00}\rangle$ в $|\Psi_{00}\rangle ... |\Psi_{22}\rangle$

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

Основною ідеєю протоколу є передавання даних по відкритому квантовому каналу, для забезпечення безпеки якого використовується випадкове перемикання в режим контролю прослуховування. Сама передача здійснюється за відомою схемою пінг-понг протоколу [5].

При реалізації запропонованого нами протоколу необхідно виконувати вимірювання як мінімум у двох так званих додаткових базисах [6]. Для таких базисів будь-які два базисні вектори, що належать двом різним базисам з даної множини базисів, задовольняють умові: $\langle e_i | e_j \rangle = 1/\sqrt{d}$, де d – розмірність гільбертова простору. Для кутритів розмірність гільбертова простору d=3 і існує чотири додаткові базиси. У роботах [7, 8] представлені наступні позначення та вирази для таких базисів:

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

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

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

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

Для здійснення контролю прослуховування каналу можна використовувати будь-які два із зазначених базисів. Збільшення кількості використовуваних базисів до трьох – чотирьох не приводить до збільшення ймовірності виявлення атаки [7]. У роботах [7, 8] представлений запис стану $|\Psi_{00}\rangle$ в базисах (1)-(4), який дозволяє визначити схему контролю підслуховування та відповідні результати вимірювань у легітимних користувачів при відсутності підслуховування:

$$|\Psi_{00}\rangle = \left(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|2\rangle\right)/\sqrt{3} = \left(|x_0\rangle|x_0\rangle + |x_1\rangle|x_2\rangle + |x_2\rangle|x_1\rangle\right)/\sqrt{3} =$$
$$= \left(|t_0\rangle|v_0\rangle + |t_1\rangle|v_1\rangle + |t_2\rangle|v_2\rangle\right)/\sqrt{3} = \left(|v_0\rangle|t_0\rangle + |v_1\rangle|t_1\rangle + |v_2\rangle|t_2\rangle\right)/\sqrt{3} \tag{5}$$

2. ПОКРОКОВИЙ ОПИС ПРОТОКОЛУ

1. Боб приготовляє пару кутритів у стані $|\Psi_{00}\rangle$. Один кутрит з пари Боб спрямовує Алісі, а другий залишає в себе.

2. Після одержання від Боба кутрита Аліса з певною ймовірністю може перейти в режим контролю прослуховування каналу зв'язку Боб-Аліса. У випадку, якщо Алісою обрано режим контролю, виконуються дії, описані в пункті 3. В іншому випадку Алісою вибираються альтернативи: контроль каналу Аліса-Чарлі, контроль каналу Боб-Чарлі або ж режим передачі повідомлення Відповідна послідовність операцій представлена в пунктах 4–8.

3. Для виконання контролю безпеки каналу Боб-Аліса обидва учасники – Аліса та Боб виконують квантові вимірювання стану відповідного кутрита, який має кожен з них. В ході перевірки обмін інформацією між Алісою та Бобом здійснюється по звичайному (не квантовому) відкритому каналу зв'язку. При цьому обов’язковою є процедура взаємної автентифікації для запобігання атаці «людина посередині», до якої вразливі усі квантові протоколи.

Як було зазначено вище, вимірювання станів кутритів Алісою та Бобом повинні виконуватись у взаємно незміщених базисах. Першою вибір базису та проведення вимірювання виконує Аліса. У режимі контролю, що розглядається, Аліса випадковим чином вибирає

один із двох взаємно незміщених базисів і в цьому базисі здійснює вимірювання стану кутріта, отриманого попередньо від Боба. Потім Аліса по класичному (не квантовому) відкритому каналу повідомляє Бобу, який базис нею був обраний для вимірювання, а також повідомляє сам результат вимірювання. При будь-якому варіанті вибору базисів Аліса з однаковою ймовірністю 1/3 одержить один із трьох можливих результатів вимірювання. Потім відповідний базис для проведення вимірювання вибирає Боб. Також, як і Аліса, Боб здійснює вибір одного із двох базисів. Однак Боб уже не може вибирати базис із наявної множини таким же довільним чином так, як це робила Аліса. Вибір Боба тепер певним чином обмежений з урахуванням попереднього вибору Аліси. А саме: якщо, наприклад, Аліса попередньо здійснила вибір *x*-базису, то Боб повинен також вибрати *x*-базис, якщо ж, наприклад, Алісою обраний *v*-базис, то відповідно до (5) Боб повинен вибрати *t*-базис. При цьому, якщо Алісою в зазначених випадках отримані результати «1» і «0» відповідно, то згідно (5) відповідні результати Боба повинні бути «2» і «0». З виразу (5) за аналогією можна отримати всі інші можливі варіанти вимірювань. Тобто, якщо, наприклад, Аліса вибрала *z*-базис, або *x*-базис, то Боб повинен вибрати також саме ці базиси. А якщо Аліса вибрала *x*-базис, або *v*-базис, то вибором Боба повинен бути *x*-базис і *t*-базис відповідно.

У випадку, коли несанкціоноване прослуховування квантового каналу відсутнє, мають місце наведені вище комбінації результатів вимірювань Аліси та Боба, що узгоджуються з (5). В іншому випадку має місце або прослуховування каналу, або наявність природних завад у каналі. Оскільки природні завади завжди присутні у реальних каналах зв’язку, то легітимні користувачі повинні виконати деяку кількість раундів контролю підслуховування, щоб оцінити рівень завад та зробити висновок, перевищує цей рівень граничний чи ні. У випадку перевищення вони роблять висновок про наявність несанкціонованого втручання та перериває протокол.

1. Боб випадковим чином вибирає одну з дев'яти кодувальних операцій, що наведені у табл. 1 і кодує кутрит, що знаходиться у нього. Потім Боб відправляє до Чарлі свій кутрит.

2. Випадковим чином з певною ймовірністю здійснюється перехід в один із трьох режимів: 6) режим контролю каналу Чарлі-Боб, 7) режим контролю каналу Чарлі-Аліса, 8)-9) режим формування секрету Алісою, спрямовування кутрита від Аліси до Чарлі та спільне відновлення секрету при кооперації Боба та Чарлі.

3. Перевірка прослуховування каналу Боб-Чарлі виконується в такий же спосіб, як і перевірка каналу Боб-Аліса – виконується вимірювання стану кутрита, отриманого Чарлі від Боба. Відмінність полягає лише в тому, що необхідно враховувати кодувальну операцію, яку попередньо над кутритом виконав Боб.

4. З метою перевірки прослуховування каналу Аліса-Чарлі користувач Аліса випадковим чином кодує наявний у неї кутрит однією з дев'яти кодувальних операцій, наведених у табл. 1. Потім Аліса передає цей кутрит Чарлі. Після цього Чарлі виконує вимірювання у базисі Белла для кутритів стану наявних у нього двох кутритів – одного попередньо отриманого від Боба, іншого – від Аліси. Потім Чарлі має повідомити Алісу про результат вимірювання, а Боб – про кодувальну операцію, яка була застосована ним до кутрита, спрямованого згодом Чарлі. Якщо після проходження каналу Аліса-Чарлі стан кутрита, який закодувала Аліса, не змінився, то це означає, що канал не прослуховується зловмисником. При контролі всіх каналів користувачі враховують вплив природнього шуму на виникнення невідповідностей результатів вимірювань у певній частині випадків.

5. Для безпосередньої реалізації режиму передачі повідомлення (секрету) Аліса вибирає необхідну кодувальну операцію з дев'яти можливих, представлених у табл. 1, і виконує кодування кутрита, який в неї знаходиться. У такий спосіб формується секрет. Після цього кутрит спрямовується Чарлі.

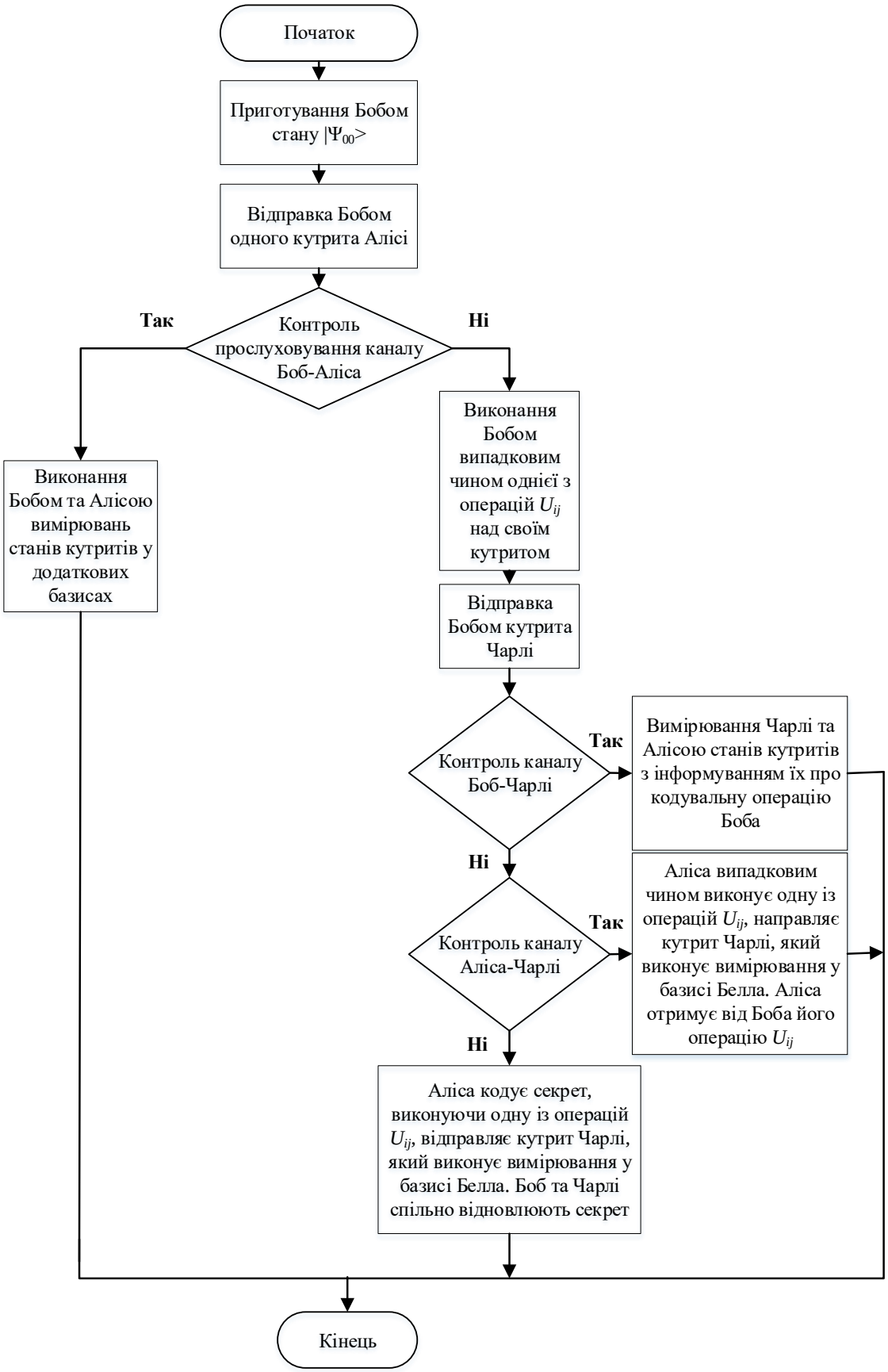

Рисунок 1 – Схема протоколу розділення секрету з перемиканням у режим контролю каналів

6. Після одержання обидвох кутритів – від Боба та від Аліси користувач Чарлі виконує вимірювання станів двох наявних у нього кутритів у базисі Белла для кутритів. Для відновлення кодувальної операції Аліси, тобто для відновлення секрету, необхідне співробітництво Боба та Чарлі. Боба повинен повідомити Чарлі про свою кодувальну операцію, а Чарлі повинен повідомити Боба про результат свого вимірювання. Боб і Чарлі окремо один від іншого не можуть відновити секрет, що забезпечує повноцінну процедуру розділення секрету та його відновлення при кооперації Боба й Чарлі.

Для визначення двох тритів Аліси, які і є секретом, Боб і Чарлі повинні використовувати кодувальну таблицю. Ця таблиця містить 81 варіант вимірювання у залежності від кодувальних операцій Боба та Аліси. Ми не наводимо кодувальну таблицю (табл. 2) повністю з огляду на її громіздкість, а показуємо тільки перші 18 варіантів, інші можуть бути отримані за аналогією.

Відзначимо, що Аліса повинна бути проінформована про те, якою випадковою кодувальною операцією користувався Боб на кроці 4). Крім того, перед початком процедури розділення секрету необхідна домовленість учасників про те, яким буде початковий стан, що готовить Боб, і яким буде відповідність квантових станів парам тритів (див. табл. 1).

3. СТІЙКІСТЬ ЗАПРОПОНОВАНОГО ПРОТОКОЛУ ДО АТАК

Як відомо, на пінг-понг протокол квантового прямого безпечного зв’язку можливі два основних види атак: активні, наприклад, "людина посередині", і атака пасивного перехоплення. Оскільки схема запропоновано у роботі квантового протоколу розділення секрету ґрунтується на пінг-понг протоколі, то протокол розділення секрету також буде вразливий до цих атак.

Добре відомим методом протидії атаці "людина посередині" є взаємна автентифікація суб’єктів протоколу. Автентифікація повідомлень, що передаються у класичному каналі зв'язку, необхідна як для квантових протоколів розподілення ключів, так і для квантових протоколів прямого безпечного зв'язку. У запропонованому в цій роботі квантовому протоколі розділення секрету з кутритами, який ґрунтується на пінг-понг протоколі, взаємна автентифікація користувачів як у класичному, так і у квантовому каналі також є обов'язковою.

Що стосується атаки пасивного перехоплення інформації, то методи контролю безпечності каналів між учасниками протоколу розділення секрету, що викладені вище, забезпечують початковий рівень захисту – коли легітимні користувачі виявили перехоплення, то вони переривають протокол. Але внаслідок наявності природнього шуму у квантовому каналі легітимні користувачі повинні виконати деяку кількість раундів контролю підслуховування. За цей час деяка кількість інформації може утекти до зловмисника і необхідний додатковий спосіб захисту.

Такий спосіб, що дозволяє звести практично до нуля тій невеликий обсяг інформації, який може отримати зловмисник, для пінг-понг протоколу з кутритами був запропонований раніше [9]. Цей же метод цілком придатний для підвищення захищеності запропонованого в даній роботі квантового протоколу розділення секрету з кутритами.

ВИСНОВКИ

У роботі запропоновано новий квантовий протокол розділення секрету між двома суб'єктами, який ґрунтується на пінг-понг протоколі квантового прямого безпечного зв'язку. Наведено детальний покроковий опис протоколу. Перевагою запропонованого протоколу над схемами з передаванням кубітів блоками є відсутність потреби в квантової пам'яті значного обсягу, що дозволяє реалізовувати протокол з використанням сучасних технологічних можливостей. Запропонований протокол має асимптотичну стійкість до атаки пасивного перехоплення зовнішнього зловмисника. Ця стійкість може бути значно підвищена, аж до зведення кількості інформації зловмисника до нескінченно малої величини, шляхом використання розробленого раніше метода підвищення стійкості пінг-понг протоколів.

Таблиця 2 – Кодувальна таблиця для протоколу розділення секрету з кутритами

№ з/п	Кодувальна операція Боба	Кодувальна операція Аліси	Результат вимірювання Чарлі у базисі Белла для кутритів	Рядок тритів, який відповідає секрету
1	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$\|\Psi_{0000}\rangle=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|/\sqrt{3}$	00
2	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$U_{10}=\|0\rangle\langle 0\|+e^{2\pi i/3}\|1\rangle\langle 1\|+e^{4\pi i/3}\|2\rangle\langle 2\|$	$\|\Psi_{0010}\rangle=\left(\|0\rangle\langle 0\|+e^{2\pi i/3}\|1\rangle\langle 1\|+e^{-2\pi i/3}\|2\rangle\langle 2\|\right)/\sqrt{3}$	10
3	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$U_{20}=\|0\rangle\langle 0\|+e^{4\pi i/3}\|1\rangle\langle 1\|+e^{2\pi i/3}\|2\rangle\langle 2\|$	$\|\Psi_{0020}\rangle=\left(\|00\rangle+e^{-2\pi i/3}\|11\rangle+e^{2\pi i/3}\|22\rangle\right)/\sqrt{3}$	20
4	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$\|\Psi_{0001}\rangle=\left(\|01\rangle+\|12\rangle+\|20\rangle\right)/\sqrt{3}$	01
5	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$U_{11}=\|1\rangle\langle 0\|+e^{2\pi i/3}\|2\rangle\langle 1\|+e^{4\pi i/3}\|0\rangle\langle 2\|$	$\|\Psi_{0011}\rangle=\left(\|01\rangle+e^{2\pi i/3}\|12\rangle+e^{-2\pi i/3}\|20\rangle\right)/\sqrt{3}$	11
6	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$U_{21}=\|1\rangle\langle 0\|+e^{4\pi i/3}\|2\rangle\langle 1\|+e^{2\pi i/3}\|0\rangle\langle 2\|$	$\|\Psi_{0021}\rangle=\left(\|01\rangle+e^{-2\pi i/3}\|12\rangle+e^{2\pi i/3}\|20\rangle\right)/\sqrt{3}$	21
7	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$U_{02}=\|2\rangle\langle 0\|+\|0\rangle\langle 1\|+\|1\rangle\langle 2\|$	$\|\Psi_{0002}\rangle=\left(\|02\rangle+\|10\rangle+\|21\rangle\right)/\sqrt{3}$	02
8	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$U_{12}=\|2\rangle\langle 0\|+e^{2\pi i/3}\|0\rangle\langle 1\|+e^{4\pi i/3}\|1\rangle\langle 2\|$	$\|\Psi_{0012}\rangle=\left(\|02\rangle+e^{2\pi i/3}\|10\rangle+e^{-2\pi i/3}\|21\rangle\right)/\sqrt{3}$	12
9	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$U_{22}=\|2\rangle\langle 0\|+e^{4\pi i/3}\|0\rangle\langle 1\|+e^{2\pi i/3}\|1\rangle\langle 2\|$	$\|\Psi_{0022}\rangle=\left(\|02\rangle+e^{-2\pi i/3}\|10\rangle+e^{2\pi i/3}\|21\rangle\right)/\sqrt{3}$	22
10	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$U_{00}=\|0\rangle\langle 0\|+\|1\rangle\langle 1\|+\|2\rangle\langle 2\|$	$\|\Psi_{0100}\rangle=\left(\|02\rangle+\|10\rangle+\|21\rangle\right)/\sqrt{3}$	00
11	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$U_{10}=\|0\rangle\langle 0\|+e^{2\pi i/3}\|1\rangle\langle 1\|+e^{4\pi i/3}\|2\rangle\langle 2\|$	$\|\Psi_{0110}\rangle=\left(e^{-2\pi i/3}\|02\rangle+\|10\rangle+e^{2\pi i/3}\|21\rangle\right)/\sqrt{3}$	10
12	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$U_{20}=\|0\rangle\langle 0\|+e^{4\pi i/3}\|1\rangle\langle 1\|+e^{2\pi i/3}\|2\rangle\langle 2\|$	$\|\Psi_{0120}\rangle=\left(e^{2\pi i/3}\|02\rangle+\|10\rangle+e^{-2\pi i/3}\|21\rangle\right)/\sqrt{3}$	20
13	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$\|\Psi_{0101}\rangle=\left(\|00\rangle+\|11\rangle+\|22\rangle\right)/\sqrt{3}$	01
14	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$U_{11}=\|1\rangle\langle 0\|+e^{2\pi i/3}\|2\rangle\langle 1\|+e^{4\pi i/3}\|0\rangle\langle 2\|$	$\|\Psi_{0111}\rangle=\left(e^{-2\pi i/3}\|00\rangle+\|11\rangle+e^{2\pi i/3}\|22\rangle\right)/\sqrt{3}$	11
15	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$U_{21}=\|1\rangle\langle 0\|+e^{4\pi i/3}\|2\rangle\langle 1\|+e^{2\pi i/3}\|0\rangle\langle 2\|$	$\|\Psi_{0121}\rangle=\left(e^{2\pi i/3}\|00\rangle+\|11\rangle+e^{-2\pi i/3}\|22\rangle\right)/\sqrt{3}$	21
16	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$U_{02}=\|2\rangle\langle 0\|+\|0\rangle\langle 1\|+\|1\rangle\langle 2\|$	$\|\Psi_{0102}\rangle=\left(\|01\rangle+\|12\rangle+\|20\rangle\right)/\sqrt{3}$	02
17	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$U_{12}=\|2\rangle\langle 0\|+e^{2\pi i/3}\|0\rangle\langle 1\|+e^{4\pi i/3}\|1\rangle\langle 2\|$	$\|\Psi_{0112}\rangle=\left(e^{-2\pi i/3}\|01\rangle+\|12\rangle+e^{2\pi i/3}\|20\rangle\right)/\sqrt{3}$	12
18	$U_{01}=\|1\rangle\langle 0\|+\|2\rangle\langle 1\|+\|0\rangle\langle 2\|$	$U_{22}=\|2\rangle\langle 0\|+e^{4\pi i/3}\|0\rangle\langle 1\|+e^{2\pi i/3}\|1\rangle\langle 2\|$	$\|\Psi_{0122}\rangle=\left(e^{2\pi i/3}\|01\rangle+\|12\rangle+e^{-2\pi i/3}\|20\rangle\right)/\sqrt{3}$	22

ЛИТЕРАТУРА

1. Xiao L. Efficient Multiparty Quantum-secret sharing Schemes / L. Xiao, G.L. Long, F.G. Deng, J.W. Pan // Physical Review A. – 2004. – V. 69, Issue 5. – 052307.

2. 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.

3. 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.

4. 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.

5. Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, Issue 18. – 187902.

6. 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.

7. Василіу Є.В. Пінг-понг протокол з повністю переплутаними станами пар та триплетів тривимірних квантових систем / Є.В. Василіу // Цифрові технології. – 2009. – № 5. – С. 18–26.

8. Василиу Е.В. Анализ атаки пассивного перехвата на пинг-понг протокол с полностью перепутанными парами кутритов / Е.В. Василиу, Р.С. Мамедов // Восточно-Европейский журнал передовых технологий. – 2009. – Т. 4, № 2 (40). – С. 4–11.

9. Василіу Є.В. Оцінки обчислювальної складності способу підсилення безпеки пінг-понг протоколу з переплутаними станами кубітів та кутритів / Є.В. Василіу, Р.С. Мамедов // Наукові праці ОНАЗ ім. О.С. Попова. – 2009, № 2. – С. 14–25.

REFERENCES:

1. Xiao L. Efficient Multiparty Quantum-secret sharing Schemes / L. Xiao, G.L. Long, F.G. Deng, J.W. Pan // Physical Review A. – 2004. – V. 69, Issue 5. – 052307.

2. 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.

3. 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.

4. 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.

5. Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, Issue 18. – 187902.

6. 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.

7. Vasiliu Ye.V. Ping-pong protokol z povnistyu pereplutany`my` stanamy` par ta try`pletiv try`vy`mirny`x kvantovy`x sy`stem / Ye.V. Vasiliu // Tzy`frovi texnologiyi. – 2009. - № 5. – S. 18–26.

8. Vasiliu E.V. Analiz ataki passivnogo perekhvata na ping – pong protokol s polnost'yu pereputannymi parami kutritov / E.V. Vasiliu, R.S. Mamedov // Vostochno-Evropejskij zhurnal peredovyh tekhnologij. – 2009. – T. 4, № 2 (40). – S. 4-11.

9. Vasiliu E.V. Otzinky obchislyuvalnoi skladnosti sposobu pidsylennya bezpeky ping-pong protokolu z pereplutanymi stanami kubitiv ta kutrytiv / E.V. Vasiliu, R.S. Mamedov // Naukovi pratzi ONAZ im. O.S. Popova. – 2009, № 2. – C. 14–25.