© Limar I., Vasiliu Ye. Quantum secret sharing protocol with communication channel checking // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 58-63.

ПРОТОКОЛ КВАНТОВОГО РОЗДІЛЕННЯ СЕКРЕТУ З КОНТРОЛЕМ КАНАЛУ ЗВ'ЯЗКУ

Ігор Лімарь, Євген Васіліу

Одеська національна академія зв'язку ім. О.С. Попова, Україна

ЛІМАРЬ Ігор Валерійович

Рік і місце народження: 1973, Одеса, Україна.
Освіта: Одеська державна академія холоду, 1995, Одеський національний університет імені І.І. Мечникова, 2010.
Посада: аспірант Одеської національної академії зв'язку ім. О.С. Попова.
Наукові інтереси: квантова криптографія, квантові протоколи розділення секрету, квантове бітове зобов'язання.
Публікації: 9 наукових публікацій, серед яких 5 наукових статей, 4 матеріали конференцій.
E-mail: quantum.biology@outlook.com

ВАСІЛІУ Євген Вікторович, д.т.н.

Рік і місце народження: 1966, Ялта, Крим, Україна.
Освіта: Одеський державний університет імені І.І. Мечникова, 1990.
Посада: директор Навчально-наукового інституту «Радіо, телебачення та інформаційної безпеки» з 2013 року.
Наукові інтереси: квантова криптографія, квантові протоколи розподілення ключів, квантові протоколи прямого безпечного зв'язку, квантові протоколи розділення секрету, квантова стеганографія.
Публікації: понад 100 наукових публікацій, серед яких 5 монографій, понад 60 наукових статей, матеріали конференцій, патенти.
E-mail: vasiliu@ua.fm

Анотація. *Запропоновано новий квантовий протокол розділення секрету між двома суб'єктами, який ґрунтується на пінг-понг протоколі квантового прямого безпечного зв'язку. Протокол базується також на відомій з літератури схемі з передаванням кубітів блоками. Але, на відміну від цієї схеми, у запропонованому протоколі передавання даних випадковим чином чергується із перевіркою каналу на наявність прослуховування. В силу цього відпадає необхідність в періодичному зберіганні значного числа кубітів, що дозволяє реалізовувати процедуру розділення секрету з використанням сучасних технологій квантової інформатики. Запропонований протокол розділення секрету, в якому також використовується розроблений раніше одним з авторів метод підвищення безпеки пінг-понг протоколів, забезпечує високий рівень стійкості до атаки пасивного перехоплення зовнішнього зловмисника, що є перевагою цього протоколу над відповідними класичними (неквантовими) схемами.*

Ключові слова: *квантова криптографія, квантове розділення секрету, переплутані кубіти, атака пасивного перехоплення, підвищення безпечності протоколу*

Вступ

Постановка задачі та огляд публікацій з даної проблематики. Одним з перспективних напрямків сучасної криптології є квантова криптографія. Основною перевагою криптосистем, які базуються на квантових технологіях, перед класичними (не квантовими) є можливість досить оперативного виявлення факту несанкціонованого підключення до каналів зв'язку. Окрім основного, такого, що промислово реалізований на даний час, напрямку квантової криптографії – квантового розподілення ключів, також існує ряд інших, поки ще таких, що реалізуються на експериментальному рівні в лабораторіях. До одного із таких напрямків відносяться схеми розділення секрету на основі квантових технологій [1-10]. Задача розділення секрету ставить за мету забезпечення спільного керування тими чи іншими системами та/або ресурсами рядом осіб із взаємним контролем. Існує багато класичних (неквантових) схем розділення секрету, які розв'язують вищеописану задачу, а також багато інших, в тому числі більш складних задач, які виникають у різних застосуваннях

розділення секрету [11–13]. Кожна з цих класичних схем має як певні переваги над іншими, так і певні недоліки, зокрема, деякі схеми мають недостатню крипостійкість або велику ресурсомісткість. Безумовною ж перевагою квантових протоколів розділення секрету (КПРС) над класичними є принципова можливість завжди виявити прослуховування каналу зв'язку у випадку, якщо розділення секрету відбувається віддалено (а не, скажемо, при особистої зустрічі). Також КПРС завдяки використанню переплутаних квантових станів, як правило, більш захищені від нечесних дій учасників самого протоколу.

Однією із проблем, з якою приходиться стикатися при створюванні протоколів квантового розділення секрету, є необхідність зберігання кубітів на певних етапах протоколу. Так, наприклад, в [5] був запропонований протокол з використанням переплутаних станів Белла пар кубітів та з передачею кубітів блоками. Цей протокол має високу стійкість як до атак зовнішніх зловмисників, так і до шахрайства самих учасників протоколу. Але, для зберігання досить великих блоків кубітів під час виконання протоколу необхідна квантова пам'ять великого обсягу. І хоча дослідження з розробки ефективних та прийнятних з позиції економічної доцільності систем квантової пам'яті ведуться досить давно [14], проблема належним чином на сьогоднішній день не вирішена. Одним із альтернативних рішень є побудування квантових криптосистем, що не мають потреби у зберіганні квантової інформації. Такі рішення, в основному, представлені схемами, в основу яких покладено принцип періодичного перемикання в режим контролю прослуховування каналу, зокрема, так званий пінг-понг протокол квантового прямого безпечного зв'язку [15]. **Метою цієї роботи** є розробка протоколу квантового розділення секрету, який, використовуючи базові принципи пінг-понг протоколу, не потребує квантової пам'яті й, в той же час, дозволяє контролювати безпеку використовуваних каналів зв'язку.

Розділення секрету на основі схеми із режимом контролю каналу. Розглянемо протокол розділення секрету з перемиканням у режим «контроль каналу» (рис. 1). В протоколі використовується пара переплутаних фотонів 1 и 2, яка може знаходитися тільки в одному із чотирьох ортогональних станів Белла:

$$\left|\psi^{\pm}\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|1\right\rangle_2 \pm \left|1\right\rangle_1\left|0\right\rangle_2\right), \qquad (1)$$

$$\left|\phi^{\pm}\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|0\right\rangle_2 \pm \left|1\right\rangle_1\left|1\right\rangle_2\right). \qquad (2)$$

Є три учасника процедури розділення секрету: Аліса, яка є дилером, а також Боб и Чарлі – особи, які безпосередньо розділюють секрет. Також відзначимо, що для кодування використовуються відомі унітарні операції:

$$U_0 \equiv I = \left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|, \qquad (3)$$

$$U_1 \equiv \sigma_z = \left|0\right\rangle\left\langle 0\right| - \left|1\right\rangle\left\langle 1\right|, \qquad (4)$$

$$U_2 \equiv \sigma_x = \left|0\right\rangle\left\langle 1\right| + \left|1\right\rangle\left\langle 0\right|, \qquad (5)$$

$$U_3 \equiv i\sigma_y = \left|0\right\rangle\left\langle 1\right| - \left|1\right\rangle\left\langle 0\right|, \qquad (6)$$

де I – тотожний оператор розмірності 2x2 та σ_i - матриці Паулі. Суть рішення полягає у тому, що при передачі фотонів по каналу зв'язку повинна виконуватись перевірка несанкціонованого підслуховування, аналогічна такій, що реалізується у пінг-понг протоколі [15, 16]. У якості вимірювальних базисів використовуються: $Z \equiv \left\{\left|0\right\rangle, \left|1\right\rangle\right\}$ та $X \equiv \left\{\left|+x\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right), \left|-x\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)\right\}$, які відповідають горизонтально-вертикальній та діагональній поляризації фотонів. Покроковий опис протоколу виглядає наступним чином:

1) Боб приготовляє один із 4-х станів Белла. Наприклад, $\left|\psi^{-}\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|1\right\rangle_2 - \left|1\right\rangle_1\left|0\right\rangle_2\right)$. Один із фотонів пари Боб на цьому етапі залишає у себе, а другий направляє Алісі. Слід відзначити, що первісний вибір Бобом одного конкретного із чотирьох можливих станів визначає всю наступну процедуру. В силу цього два інших учасника розділення секрету – Аліса и Чарлі мають бути в обов'язковому порядку проінформовані про те, який стан вибрано.

2) Після отримання Алісою фотона, який відправлений Бобом, вона із заданою ймовірністю здійснює перемикання у режим контролю безпечності каналу Аліса – Боб. У цьому випадку виконується пункт 3 протоколу. У противному випадку здійснюється перехід до виконання перевірки каналів Боб – Чарлі, Аліса – Чарлі, або передачі повідомлення (від Боба Чарлі та від Аліси Чарлі), що відповідає пунктам 4 - 8).

3) Контроль безпечності квантового каналу здійснюється шляхом послідовного вимірювання станів кубітів учасниками розділення секрету та наступного порівняння результатів вимірювань. Обмін інформацією про вимірювання виконується по звичайному відкритому каналу зв'язку. Слід відзначити, що цей канал, хоча і є відкритим, але необхідна взаємна аутентифікація всіх користувачів для запобігання атаці "людина посередині". Контроль безпечності виконується, наприклад, так. Аліса, отримавши фотон, виконує вимірювання в одному із зазначених вище базисів. Потім вона повідомляє Бобу базис, який був обраний нею для вимірювання, та сам результат вимірювання. Відповідні вимірювання над фотоном, що у нього залишився, також виконує і Боб. З урахуванням того, що фотони були спочатку приготовані як такі, що знаходяться у стані Белла $\left|\psi^{-}\right\rangle$, для випадку, коли канал не прослуховується, має мати місце точна антикореляція поляризації фотонів, тобто, якщо результат вимірювання Аліси "0", то у Боба повинно бути "1", і навпаки. Також необхідно враховувати процент помилок при аналізі результатів вимірювань, які можуть бути викликані не діями зловмисника, а природнім шумом у каналі.

4) Боб, випадковим чином вибираючи одну з унітарних операції (3) – (6), здійснює кодування кубіту, який знаходиться у нього. Після цього кубіт відправляється Чарлі.

5) Далі з певною ймовірністю випадковим чином виконується перемикання в один із трьох режимів: 6) контроль каналу Боб – Чарлі, 7) контроль каналу Аліса – Чарлі, 8) – 9) кодування Аліси, передача кубіта Чарлі та відновлення секрету Бобом та Чарлі.

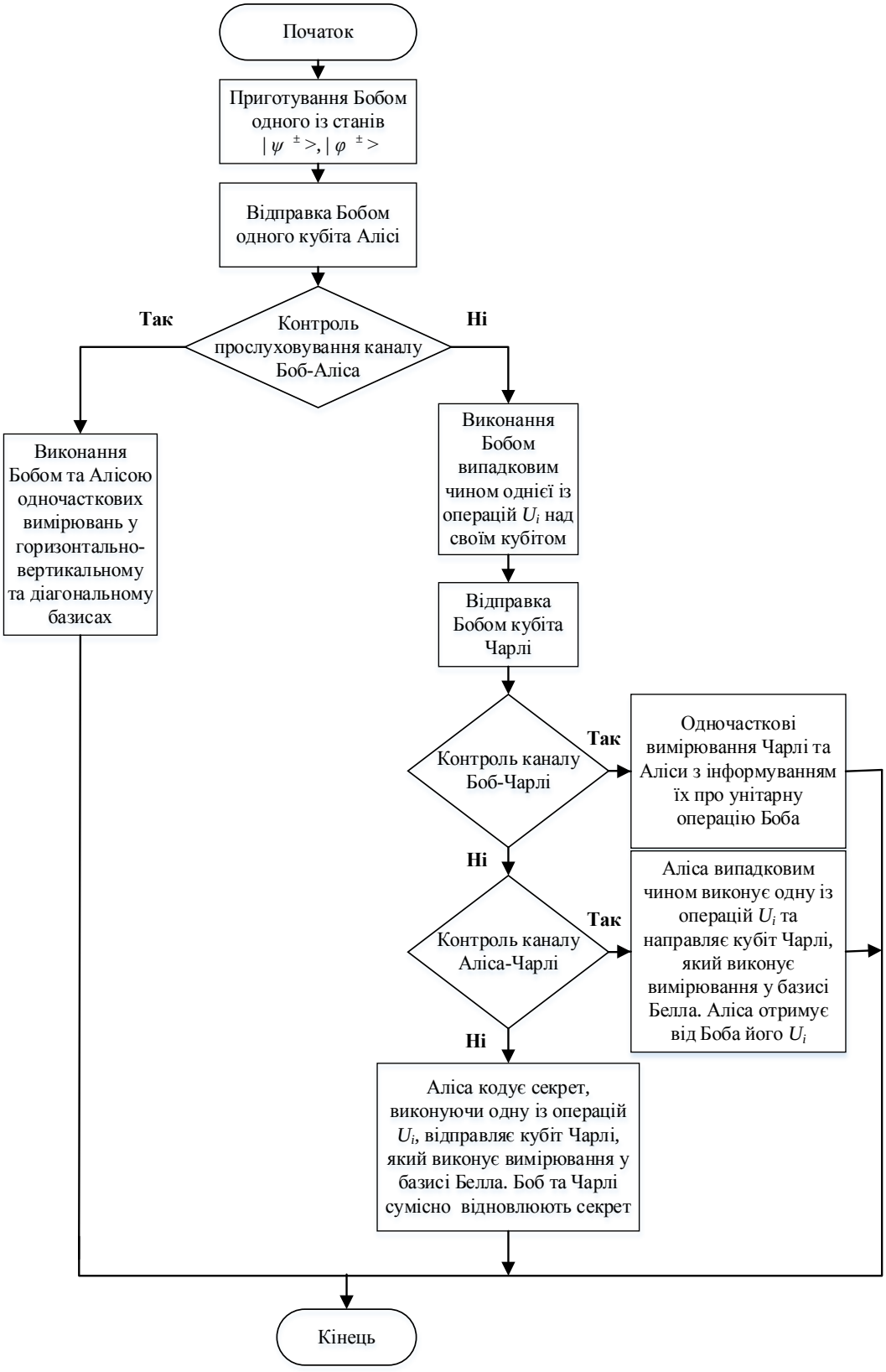

Рис. 1 – Схема протоколу розділення секрету з перемиканням у режим контролю каналів

6) Перевірка безпечності каналу Боб – Чарлі здійснюється шляхом одночасткових вимірювань, аналогічно перевірки каналу Боб – Аліса. При цьому зрозуміло, що необхідно враховувати кодувальну операцію Боба, яку він виконав на кроці 4, так як результат вимірювань Боба і Чарлі залежить від цієї операції.

7) Перевірка безпечності каналу між Алісою і Чарлі починається із випадкового кодування Алісою унітарним оператором кубіту, що знаходиться у неї, та передачі його Чарлі. Чарлі здійснює вимірювання у базисі Белла станів двох частинок, які тепер знаходяться у нього. Аліса потребує від Боба інформацію про те, яку кодувальну операцію він використовував для даного раунду, та від Чарлі – результат вимірювання. Якщо канал не прослуховується зловмисником, то стан кубіту, який був закодований Алісою перед перевіркою, потрапить до Чарлі без змін. Зрозуміло, що внаслідок природного шуму в квантовому каналі, результати всіх перевірок не завжди будуть такими, які вони повинні бути в ідеальному каналі. Тому користувачі протоколу при прийнятті рішення, чи є атака пасивного перехоплення, повинні враховувати цей природній шум, але його рівень, як правило, завжди значно менший, ніж той, що створює зловмисник своєю атакою.

8) Режим передачі секрету. Аліса вибирає ту чи іншу кодувальну операцію (3) – (6), виконує її над своїм кубітом та відправляє його Чарлі. Ця кодувальна операція Аліси і є секретом. Оскільки є чотири можливих кодувальних операцій, то секрет Аліси є двома бітами інформації.

Виконавши вимірювання у базисі Белла двох кубітів, які знаходяться у нього після завершення режиму передачі, Чарлі отримає результат $U_C = U_A \otimes U_B$. Кооперація Боба и Чарлі дозволяє у підсумку відновити кодувальну операцію Аліси. Для цього Боб повідомляє Чарлі, яку операцію він виконав на кроці 4, а Чарлі повідомляє Бобу результат вимірювання. Без обміну цією інформацією ні Боб, ні Чарлі ні в змозі визначити кодувальну операцію Аліси.

Результати виконання операцій при застосуванні Бобом и Алісою різних кодувальних операторів наведені у табл. 1. Відзначимо, що Аліса для кодування секрету повинна знати, яку випадкову кодувальну операцію виконав Боб на кроці 4. Якщо ж секрет є випадковим рядком бітів, наприклад, криптографічним ключем, то це не обов'язково – Аліса може випадковим чином виконувати будь-які операції. Але у будь-якому випадку учасники протоколу повинні спочатку домовитись про те, який початковий стан буде готувати Боб, та яка пара бітів якому стану відповідає.

Таблиця 1

Відповідність обраних кодувальних операцій результатам вимірювання та бінарному значенню секрету

№ з/п	Кодувальна операція Боба	Кодувальна операція Аліси	Результат вимірювання Чарлі у базисі Белла	Секрет у бінарному кодуванні
1.	I	I	$\|\psi^-\rangle$	00
2.	I	σ_z	$\|\psi^+\rangle$	01
3.	I	σ_x	$\|\phi^-\rangle$	10
4.	I	$i\sigma_y$	$\|\phi^+\rangle$	11
5.	σ_z	I	$\|\psi^+\rangle$	00
6.	σ_z	σ_z	$\|\psi^-\rangle$	01
7.	σ_z	σ_x	$\|\phi^+\rangle$	10
8.	σ_z	$i\sigma_y$	$\|\phi^-\rangle$	11
9.	σ_x	I	$\|\phi^-\rangle$	00
10.	σ_x	σ_z	$\|\phi^+\rangle$	01
11.	σ_x	σ_x	$\|\psi^-\rangle$	10
12.	σ_x	$i\sigma_y$	$\|\psi^+\rangle$	11
13.	$i\sigma_y$	I	$\|\phi^+\rangle$	00
14.	$i\sigma_y$	σ_z	$\|\phi^-\rangle$	01
15.	$i\sigma_y$	σ_x	$\|\psi^+\rangle$	10
16.	$i\sigma_y$	$i\sigma_y$	$\|\psi^-\rangle$	11

Оцінка ефективності протоколу дає наступні результати. Припустимо, що перевірка безпечності каналу Аліса – Боб потребує для свого проведення 50% приготовлених переплутаних пар кубітів, тобто перехід меж між цим режимом та іншими виконується з ймовірністю 0,5. З тих 50% фотонів, що залишилися, третину будемо витрачати на контроль безпечності каналу Боб – Чарлі і таку ж кількість – на перевірку каналу Аліса – Чарлі. Таким чином, безпосередньо для виконання розділення секрету буде використано менш ніж 17% частинок. Слід відзначити, що вказані показники щодо частоти перевірок можуть бути змінені у прийнятних з урахуванням критеріїв безпечності діапазонах. Наприклад, по 25% на перевірку безпечності трьох каналів, і тоді для розділення секрету залишиться також 25% переплутаних пар.

Стійкість запропонованого протоколу до атак. Як відомо, при квантової прямої передачі даних і, зокрема, в рамках пінг-понг протоколу можливі дві основні потенційні загрози: атаки активного характеру, наприклад, "людина посередині", і атаки пасивного перехоплення. Також можливі атаки обох цих видів, що використовують недосконаліть обладнання, але вони залежать від конкретного обладнання, і ці загрози розглядати не будемо.

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 [16]. У запропонованому в цій роботі квантовому протоколі розділення секрету, який ґрунтується на пінг-понг протоколі, взаємна автентифікація користувачів також є обов'язковою.

Що стосується атаки пасивного перехоплення інформації, то методи контролю безпечності каналів між учасниками протоколу розділення секрету, що викладені вище, в прийнятній мірі забезпечують захист від такого роду загрози. Детальний аналіз атаки пасивного перехоплення на різні види пінг-понг протоколу виконано раніше [17]. Тут ми коротко відзначимо основні моменти доказу стійкості запропоновано протоколу розділення секрету. На основі виразу для ентропії фон Неймана можна обчислити кількість інформації I_0, яка є доступною Єві за один раунд протоколу. Далі після розв'язання задачі на власні значення для конкретного варіанту пінг-понг протоколу можливо знайти ймовірність s того, що атака Єви не буде виявлена. Залежності s від I_0 демонструють, що атака успішно виявляється легітимними учасниками протоколу. Але при цьому зловмисник отримує деяку невелику кількість секретної інформації. В роботі [17] такий вид стійкості отримав назву «асимптотичної».

Підвищення захищеності запропонованого протоколу від атаки пасивного перехоплювання можливо тим же шляхом, що і для пінг-понг протоколу. Відповідний метод, що дозволяє звести практично до нуля тій невеликий обсяг інформації, який може отримати зловмисник, для пінг-понг протоколів запропонований у роботі [18]. Цей же метод придатний для підвищення захищеності запропонованого в даній роботі квантового протоколу розділення секрету.

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.

Література

[1] Hillery M. Quantum Secret Sharing / M. Hillery, V. Buzek, A. Berthiaume // Physical Review A. – 1999. – V. 59, Issue 3. – P.1829–1834.

[2] 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.

[3] Deng F.G. Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs / F.G. Deng , X.H. Li, C.Y. Li, P. Zhou, H.Y. Zhou // Physical Review A. – 2005. – V. 72, Issue 4. – 044301.

[4] Zhang Z. Multiparty quantum secret sharing of classical messages based on entanglement swapping / Z. Zhang, Z. Man // Physical Review A. – 2005. – V. 72, Issue 2. – 022303.

[5] Deng F.G. Multiparty quantum secret splitting and quantum state sharing / F.G. Deng, X.H. Li, C.Y. Li, P. Zhou, H.Y. Zhou // Physics Letters A. – 2006. – V. 354, issue 3. – P. 190–195.

[6] Gottesman D. Theory of quantum secret sharing // Physical Review A. – 2000. – V. 61, Issue 4. – 042311.

[7] Wang J. Multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state / J. Wang, Q. Zhang, C.-J. Tang // Optics Communication. – 2006. – V. 226. – P. 732–737.

[8] Liu F. Eavesdropping on Multiparty Quantum Secret Sharing Scheme Based on the Phase Shift Operations / F. Liu, Q. Su, Q.-Y Wen // International Journal of Theoretical Physics. – 2014. – V. 53, issue 5. – P. 1730–1737.

[9] Deng F.G. Bidirectional quantum secret sharing and secret splitting with polarized single photons / F.G. Deng, H.Y. Zhou, G.L. Long // Physics Letters A. – 2005. – V. 337, Issues 4–6. – P. 329–334.

[10] Tittel W. Experimental demonstration of quantum secret sharing / W. Tittel, H. Zbinden, N. Gisin // Physical Review A. – 2001. – V.63, Issue 4. – 042301.

[11] Смарт Н. Криптография / Смарт Н. – М.: Техносфера, 2005. – 528 с.

[12] Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник / Тилборг ван Х.К.А. – М.: Мир, 2006. – 471 с.

[13] Menezes A.J. Handbook of applied cryptography / Menezes A.J., Oorschot van P.C., Vanstone S.A. – CRC Press, 1996. – 816 p.

[14] Focus on Quantum Memory // New Journal of Physics [Електронний ресурс]. – Режим доступу: http://iopscience.iop.org/1367-2630/focus/Focus%20on%20Quantum%20Memory.

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

[16] Василиу Е.В. Стойкость пинг-понг протокола с триплетами Гринбергера – Хорна – Цайлингера к атаке с использованием вспомогательных квантовых систем / Е.В. Василиу // Информатика: Объединенный институт проблем информатики НАН Беларуси. – 2009, № 1 (21) – С. 117–128.

[17] Василіу Є.В. Синтез структури квантових систем прямого безпечного зв'язку / Є.В. Василіу // Цифрові технології. – 2011, № 9. – С. 20–30.

[18] 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.

УДК 004.056.53+530.145 (045)

Лимарь И.В., Василиу Е.В. Протокол квантового разделения секрета с контролем канала связи

Аннотация. *Предложен новый квантовый протокол разделения секрета между двумя субъектами, который основан на пинг-понг протоколе квантовой прямой безопасной связи. Протокол базируется также на известной из литературы схемы с передачей кубитов блоками. Однако, в отличие от этой схемы, в предложенном протоколе передача данных случайным образом чередуется с проверкой канала на наличие прослушивания. В силу этого отпадает необходимость в периодическом хранении значительного числа кубитов, что позволяет реализовывать процедуру разделения секрета с использованием современных технологий квантовой информатики. Предложенный протокол разделения секрета, в котором также используется разработанный раньше одним из авторов метод повышения безопасности пинг-понг протоколов, обеспечивает высокий уровень стойкости к атаке пассивного перехвата внешнего злоумышленника, что является преимуществом этого протокола над соответствующими классическими (неквантовыми) схемами.*

Ключевые слова: *квантовая криптография, квантовое разделение секрета, перепутанные кубиты, атака пассивного перехвата, повышение безопасности протокола.*

Limar I., Vasiliu Ye. Quantum secret sharing protocol with communication channel checking

Abstract. *The new quantum protocol of secret sharing between two subjects, which is based on the ping-pong protocol of quantum secure direct communication, is proposed. This protocol is based on scheme of transmission of the qubits by blocks, which is well known from publications. However, in contrast to this scheme in the proposed protocol the data transmission in a random way alternates with channel check on eavesdropping. Thereby the need for periodic storage of considerable number of qubits disappears. It will let to implement the procedure of secret sharing with assisting state-of-the-art technology of quantum information science. The proposed secret sharing protocol, which also uses the earlier developed by co-author the method of enhancement of the ping-pong protocols security, provides the high level of security to the outer malefactor's eavesdropping attack. It is the advantage of this protocol over the appropriate classical (non-quantum) schemes.*

Key words*: quantum cryptography, quantum secret sharing, entangled qubits, eavesdropping attack, protocol security enhancement.*

Отримано *1 лютого 2016 року*, затверджено редколегією *11 березня 2016 року*