Підсилення безпеки пінг – понг протоколу квантового безпечного зв'язку з *n*-кубітними ГХЦ – станами

Євген Василіу, Сергій Ніколаєнко

Кафедра інформатизації та управління, Одеська національна академія зв'язку ім. О.С. Попова, УКРАЇНА, м. Одеса, вул. Ковальська, 1, E-mail: vasiliu@ua.fm

Abstract – In this paper we suggested not a quantum method of security amplification of the ping – pong protocol with many-qubit entangled Greenberger – Horne – Zeilinger states. The necessary sizes of matrixes for hashing of message blocks are calculated at some values of parameters of the protocol.

Ключові слова – quantum secure direct communication, ping– pong protocol, many-qubit entangled Greenberger – Horne – Zeilinger states, security amplification, hashing.

I. Вступ

У сучасному інформаційному суспільстві все більше людей мають потребу в конфіденційному зв'язку. Квантові комунікації, які ґрунтуються на передачі інформації, закодованої у квантових станах мікрочастинок, пропонують ряд нових способів для безпечного обміну повідомленнями [1]. Один з напрямків квантових комунікацій – квантові протоколи безпечного зв'язку, у яких взагалі не використовується шифрування, а таємність передачі гарантується законами квантової фізики [2-8]. Відкритий текст секретного повідомлення кодується за допомогою квантових станів груп переплутаних кубітів – фотонів, і потім ці кубіти передаються по квантовому каналу зв'язку. При цьому закони квантової фізики гарантують виявлення підслуховування в каналі. Виявивши агента, що підслуховує (Єву), легітимні користувачі (Аліса та Боб) переривають протокол.

Одним із протоколів квантового безпечного зв'язку є так званий пінг – понг протокол. У першому варіанті цього протоколу [2] використовуються переплутані пари кубітів та дві кодувальні операції, що дозволяє передати один біт класичної інформації за один цикл протоколу. Використання квантового надщільного кодування для переплутаної пари кубітів [1] дозволяє передати два біти за цикл [3]. Подальше збільшення інформаційної місткості протоколу можливо шляхом використання замість переплутаних пар кубітів їх трійок, четвірок і т.д. [4], оскільки інформаційна місткість пінг – понг протоколу дорівнює n бітів на цикл, де n – кількість переплутаних кубитов.

Раніше були проаналізовані атаки з використанням допоміжних квантових систем (проб) на оригінальний пінг – понг протокол [2], а також на протокол з переплутаними парами та надщільним кодуванням [5] та на протокол з триплетами Грінбергера – Хорна – Цайлінгера (ГХЦ) [6]. Також було одержано загальний вираз для кількості інформації, яку може отримати Єва внаслідок своєї атаки, для пінг – понг протоколу з n-кубітними ГХЦ – станами [7]. Показано, що пінг – понг протокол з ГХЦ – станами є асимптотично безпечним, тобто атака Єви буде виявлена, але до виявлення атаки Єва зможе отримати деяку кількість інформації, що залежить від кількості n використовуваних у протоколі кубітів. В роботі [8] було запропоновано класичний (не квантовий) спосіб підсилення безпеки пінг – понг протоколу з парами кубітів та надщільним кодуванням. Метою цієї роботи є розробка способу підсилення безпеки пінг – понг протоколу з n-кубітними ГХЦ – станами при будь-яких n.

II. Інформація Єви при симетричній атаці на пінг – понг протокол з *n*-кубітними ГХЦ – станами

Інформація Єви при атаці з використанням квантових проб на пінг – понг протокол з переплутаними n-кубітними ГХЦ – станами визначається ентропією фон Неймана [2]:

$$I_0 = S(\rho) \equiv -Tr\{\rho \log_2 \rho\} = -\sum_i \lambda_i \log_2 \lambda_i \,, \qquad (1)$$

де λ_i – власні значення матриці щільності системи "кубіти, що передаються – проба Єви".

Для протоколу з n-кубітними ГХЦ – станами кількість власних значень матриці щільності дорівнює 2^n, а їх вид при симетричній атаці Єви [7]:

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\left[(p_1 + p_2)^2 - 16 p_1 p_2 \cdot \frac{2^{n-2}}{2^{n-1}-1} d \left(1 - \frac{2^{n-2}}{2^{n-1}-1} d\right)\right]^{1/2},$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\lambda_{2^n-1,\,2^n} = \frac{1}{2}\left(p_{2^n-1} + p_{2^n}\right) \pm \frac{1}{2}\left[\left(p_{2^n-1} + p_{2^n}\right)^2 - 16 p_{2^n-1} p_{2^n} \cdot \frac{2^{n-2}}{2^{n-1}-1} d \left(1 - \frac{2^{n-2}}{2^{n-1}-1} d\right)\right], \qquad (2)$$

де d – імовірність виявлення атаки легітимними користувачами при однократному переході в режим контролю підслуховування [2,5,6]; p_i – частоти n-грам у повідомленні, що передається.

Імовірність того, що Єва не буде виявлена після m успішних атак і отримає інформацію $I = m I_0$, визначається формулою [2]:

$$s(I,q,d) = \left(\frac{1-q}{1-q(1-d)}\right)^{\frac{I}{I_0}}. \qquad (3)$$

де q – імовірність переходу в режим контролю підслуховування [2,5,6], I_0 визначене в (1).

На рис. 1 показані залежності $s(I,q,d)$ для декількох n, однакових частот $p_i = 2^{-n}$, $q = 0.5$ і $d = d_{\max}$.

$$d_{\max} = 1 - \frac{1}{2^{n-1}} \qquad (4)$$

є максимальною імовірністю виявлення атаки при однократному переході в режим контролю підслуховування. При $d = d_{\max}$ Єва отримує повну інформацію про передані біти повідомлення [2,5,6].

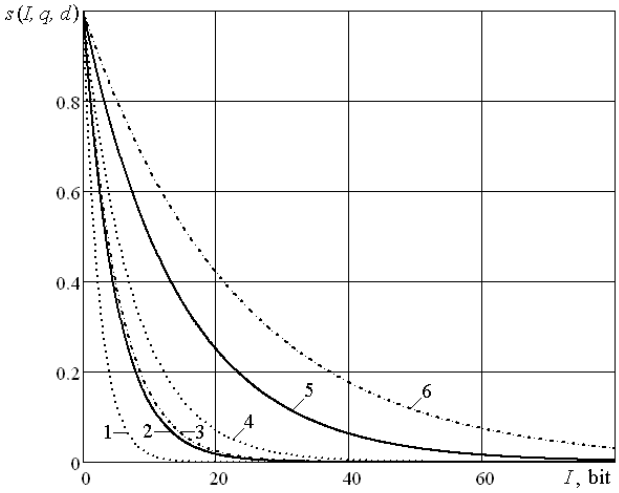

Рис. 1. Повна імовірність невиявлення атаки *s* для пінг - понг протоколу із багатокубітними ГХЦ - станами: *n* = 2, оригінальний протокол (1); *n* = 2, з надщільним кодуванням (2); *n* = 3 (3); *n* = 5 (4); *n* = 10 (5); *n* = 16 (6).

З рис. 1 видно, що повна імовірність невиявлення атаки зменшується експоненціально з ростом перехопленої Євою інформації при будь-якому *n*. Таким чином, пінг – понг протокол із багатокубітними ГХЦ – станами є асимптотично безпечним при будь-якій кількості *n* кубитов, що перебувають у переплутаних ГХЦ – станах.

III. Спосіб підсилення безпеки пінг-понг протоколу з *n*-кубітними ГХЦ – станами

Як випливає з результатів попереднього розділу, Єва може одержати деяку інформацію, перш ніж її атака буде виявлена, причому кількість цієї інформації зростає зі збільшенням кількості використовуваних у протоколі переплутаних кубітів. Отже, для практичного використання протоколу необхідний спосіб, який зробить отриману Євою інформацію даремною для неї. Такий спосіб може бути розроблений на основі методу підсилення таємності, що застосовується у квантових протоколах розподілу ключів [1]. У даному випадку цей спосіб буде деякою аналогію шифру Хіла.

Перед передачею Аліса розбиває своє двійкове повідомлення на *l* блоків деякої фіксованої довжини *r*, позначимо ці блоки через a_i $(i = 1,\ldots l)$, потім генерує для кожного блоку окремо випадкову оборотну двійкову матрицю K_i розміру $r \times r$ і множить отримані матриці на відповідні блоки повідомлення (множення виконується за модулем 2):

$$b_i = K_i a_i . \qquad (5)$$

Отримані в результаті блоки b_i передаються по квантовому каналу з використанням пінг – понг протоколу. Навіть якщо Єві вдасться перехопити один (або більше) із цих блоків, залишившись не виявленої, то, не знаючи використаних матриць K_i, Єва не може встановити вихідні блоки a_i. Для забезпечення достатнього рівня безпеки довжина блоку r і відповідно розмір матриць K_i повинні вибиратися так, щоб імовірність невиявлення Єви s (3) після передачі одного блоку була нехтовно малою величиною. Матриці K_i передаються Бобові по звичайному (не квантовому) відкритому каналу після завершення квантової передачі, але тільки в тому випадку, якщо Аліса і Боб переконалися у відсутності підслуховування. Потім Боб обертає отримані матриці та, помноживши їх на відповідні блоки b_i, одержує вихідне повідомлення.

Відзначимо, що описана процедура не є шифруванням повідомлення, а може бути названа оборотним гешуванням або гешуванням з використанням двосторонньої геш-функції, роль якої грає випадкова оборотна матриця двійкових чисел.

Для кожного блоку необхідно використовувати окрему матрицю K_i, що дозволить запобігти криптоаналітичним атакам, подібнім до атак на шифр Хіла, які можливі там при багаторазовому використанні однієї матриці для шифрування різних блоків (подібну атаку Єва могла б провести, якби їй удалося до виявлення її операцій у квантовому каналі перехопити кілька блоків, що гешуються з однією і тією ж матрицею). Оскільки матриці в цьому випадку не є ключем і їх можна передавати по відкритому класичному каналу, передавання потрібної кількості матриць не є проблемою.

Розглянемо тепер питання про вибір необхідної довжини блоку *r*. Як видно з рис. 1, ця величина буде залежати від кількості *n* використовуваних у протоколі переплутаних кубитов – чим більше *n*, тим більше повинна бути довжина *r* блоку для забезпечення того ж рівня безпеки. Конкретне значення *r* може бути обчислене з використанням (3) при заданому *n* і заданої імовірності невиявлення Єви *s*. Але сама величина *s* залежить від параметрів *q* і *d*.

Величину *q* – імовірність переходу в режим контролю підслуховування – вибирають легітимні користувачі. Чим більше *q*, тим швидше атака Єви буде виявлена, однак тем менше буде загальна ефективність протоколу, тому що чим частіше Аліса і Боб переходять в режим контролю підслуховування, тим рідше вони передають самі біти повідомлення.

Величину *d* – імовірність виявлення атаки при однократному виконанні контролю підслуховування – може регулювати Єва, вибираючи відповідним чином параметри своїх квантових проб, використовуваних для атаки [2,5,6]. Однак чим менше *d*, тим менше інформація Єви в будь-якому варіанті пінг – понг протоколу [2, 5, 6,7]. Таким чином, зменшуючи *d*, Єва зможе визначити правильно тільки деякі передані біти. Це значно утруднить їй визначення вихідних

блоків повідомлення a_i, навіть якщо вона залишиться невиявленої та отримує відповідні їм матриці K_i. Таким чином, при визначенні довжини r блоку будемо вважати, що Єва прагне одержати повну інформацію, це відповідає максимальній імовірності її виявлення $d_{\max}$ (4).

Необхідна довжина r блоку для гешування і відповідно необхідний розмір $r \times r$ гешувальних матриць повинні відповідати умові $r > I$, де I – інформація, що перехоплюється Євою. При цьому r повинно бути кратним кількості кубітів n, що використовуються для реалізації протоколу. Таким чином, для визначення r необхідно розрахувати I при заданих значеннях n, s, q і $d = d_{\max}$ (4).

Покладемо $s(I,q,d) = 10^{-k}$ і виразімо інформацію Єви I з (3):

$$I = -kI_0 \Big/ \lg\left(\frac{1-q}{1-q(1-d)}\right). \qquad (6)$$

Результати розрахунків I при $q = 0.5$ і $d = d_{\max}$ наведені у табл. 1.

ТАБЛ. 1. ІНФОРМАЦІЯ ЄВИ ПРИ АТАЦІ НА ПІНГ-ПОНГ ПРОТОКОЛ З N-КУБІТНИМИ ГХЦ – СТАНАМИ (БІТ)

n \ s	10^{-6}	10^{-4}	n \ s	10^{-6}	10^{-4}
2	69	46	11	220	147
3	74	50	12	240	160
4	88	59	13	260	173
5	105	70	14	279	186
6	123	82	15	299	200
7	142	94	16	319	213
8	161	107	17	339	226
9	180	120	18	359	240
10	200	133	19	379	253

Як видно з табл. 1, при невеликих n необхідний розмір матриць для гешування є невеликим, але досить швидко зростає із зростанням n. Тому стає питання про час, що потрібний для генерування та перевірки на оборотність випадкових двійкових матриць. Цей час буде суттєво залежати від імовірності того, що двійкова матриця, яка генерована випадковим чином, є оборотною. Така імовірність була обчислена в [9] і для матриць в GF(2) при $r \geq 16$ стає константою, яка дорівнює 0.289. Таким чином, у середньому майже кожна третя з двійкових матриць, що випадково генеровані, при $r \geq 16$ буде оборотною, що, на наш погляд, цілком прийнятно.

На закінчення зробимо наступне зауваження. Запропонований метод підсилення безпеки пінг – понг протоколу не вимагає наявності у легітимних користувачів ніяких передвстановлених ключів – на відміну від шифру Хіла матриці тут не є ключем і передаються відкрито, якщо Аліса і Боб переконалися у відсутності підслуховування у квантовому каналі, а останнє забезпечується методами квантової механіки. Таким чином, основна перевага квантових протоколів безпечного зв'язку, а саме відсутність необхідності розподіляти ключі (за винятком невеликого ключа для аутентифікації), зберігається при використанні запропонованого методу.

Висновок

Запропоновано не квантовий метод підсилення безпеки пінг – понг протоколу з багатокубітними переплутаними станами Грінбергера – Хорна – Цайлінгера. Розраховано необхідні розміри матриць для гешування блоків повідомлення при деяких значеннях параметрів протоколу.

Література

[1] М. Нильсен, И. Чанг, "Квантовые вычисления и квантовая информация", М.: Мир, 2006. – 824 с.

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

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

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

[5] Е.В. Василиу, "Анализ безопасности пинг – понг протокола с квантовым плотным кодированием", Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32 – 38.

[6] Е.В. Василиу, "Анализ атаки на пинг – понг протокол с триплетами Гринбергера – Хорна - Цайлингера", Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 1. – С. 15 – 24.

[7] С.В. Николаенко, "Утечка информации к злоумышленнику в пинг – понг протоколе с N перепутанными кубитами", Материалы 13-го международного молодежного форума "Радиоэлектроника и молодежь в XXI веке", часть 2, с. 59, Харьков, 2009.

[8] Е.В. Василиу, "Безопасность пинг – понг протокола квантовой связи для передачи текстовых сообщений", Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 2. – С. 36 – 44.

[9] J. Overbey, W. Traves, J. Wojdylo, "On the keyspace of the Hill cipher", Cryptologia. – 2005. – V. 29, № 1. – P. 59 – 72.