УДК 004.056.53+530.145

С.В. Ніколаєнко[1]

[1]*викладач Одеської національної академії зв'язку ім. О.С. Попова*

ГАМУВАННЯ ЯК МЕТОД ПІДСИЛЕННЯ СТІЙКОСТІ ПІНГ-ПОНГ ПРОТОКОЛУ З ПАРАМИ ПЕРЕПЛУТАНИХ КУБІТІВ

У статті розглядається класичний (не квантовий) спосіб посилення стійкості пінг-понг протоколу з парами переплутаних кубітів. Цей спосіб полягає в шифруванні методом гамування блоків повідомлень і дозволяє забезпечити достатньо високий рівень стійкості протоколу. При цьому самі гами не є секретною інформацією, і передаються відкритим каналом тільки після того, як легітимні користувачі переконалися у відсутності атаки в квантовому каналі. Розроблена імітаційна модель пінг-понг протоколу з парами переплутаних кубітів в квантовому каналі з використанням шифрування методом гамування. Виконаний розрахунок необхідних для забезпечення заданого рівня стійкості протоколу, довжин блоків повідомлення в залежності від параметрів протоколу і параметрів атакуючої операції зловмисника, а також відповідний розрахунок необхідних розмірів випадкових гам. Виконані оцінки обчислювальної складності генерації гам для даного методу посилення стійкості. Показано, що час генерації є прийнятним для гам розміром близько 2000 біт при використанні обчислювальної техніки з невисокою швидкодією.

Ключові слова: квантова криптографія, пінг-понг протокол, метод посилення стійкості протокола, шифрування методом гамування, імітаційне моделювання, тимчасові оцінки.

Вступ

У сучасному світі передача конфіденційних даних між декількома абонентами в різних мережах зв'язку може призвести як до втрати переданої інформації, так і до її компрометації, тобто розголошення інформації, що стала відомою якійсь особі, яка не має права доступу до неї. В останнє десятиліття активно розвивається новий напрямок захисту інформації – квантова криптографія. На відміну від криптографічних методів, безпека яких ґрунтується на недоведених математичних твердженнях, безпека квантової криптографії заснована на законах квантової фізики, де для переносу інформації використовується об'єкти квантової механіки. Такими об'єктами можуть бути фотони в лініях волоконно-оптичного зв'язку. Квантові явища, які використовуються з метою криптографічного захисту інформації, дозволяють створити таку систему захисту, за якої будь-яке підслуховування виявляється з високим ступенем точності і достовірності. Спроба підслуховування призводить дозбурення вихідного стану системи. Оскільки неможливо виміряти хоча однухарактеристику фотона, не порушивши і не спотворивши інші.

Одним із напрямків квантової криптографії є протоколи квантового прямого безпечного зв'язку (КПБЗ), які дозволяють передавати конфіденційні повідомлення безпосередньо квантовим каналом, тобто без використання шифрування. В даний час запропоновано велику кількість різних за призначенням протоколів КПБЗ [1-7]. Одним з таких протоколів, що не потребує квантової пам'яті великого об'єму, є пінг-понг протокол з парами переплутаних кубітів і без використання квантового надщільного кодуван-

ня, який дозволяє передати один біт класичної інформації за один цикл протоколу [1].

Пінг-понг протокол є одним із простих протоколів КПБЗ, який може бути реалізований з використанням сучасних технологій квантової інформатики [8]. На даний час існують різні варіації цього протоколу [1,2,6,7], але не до кінця досліджена їх стійкість до різних атак зловмисника. Оскільки пінг-понг протокол призначений для безпечного передавання класичної інформації квантовими каналами зв'язку, то є можливість використовувати класичні методи захисту інформації для підсилення стійкості пінг-понг протоколу та інших КПБЗ.

На цей час існує велика кількість класичних методів підсилення стійкості протоколів передачі даних [9-12], які надійно захищають дані від втручання і можуть бути застосовані для захисту від зловмисників інформації, переданої за допомогою квантових пінг-понг протоколів. Одним з таких актуальних і криптографічно гарантованих методів захисту інформації є метод гамування. Однак, якщо оцінки надійності та швидкості методу гамування для пінг-понг протоколу з парами переплутаними кутритів частково виконувалися раніше [13], то для пінг-понг протоколів з групами переплутаних кубітів таких оцінок раніше взагалі не проводилося.

Метою цієї роботи є збільшення стійкості до атаки пасивного перехоплення пінг-понг протоколу з парами переплутаних кубітів шляхом використання методу гамування.

Схема пінг-понг протоколу з парами переплутаних кубітів і без квантового надщільного кодування. Пінг-понг протокол є двостороннім протоколом квантового безпечного зв'язку – для передавання повідомлення від одного абонента (Аліси) до іншого абонента (Боба) кубіт пересилається спочатку від Боба до Аліси, а потім назад від Аліси до Боба. В пінг-понг протоколі застосовуються два режими – режим передавання самого повідомлення і режим контролю підслуховування, необхідний для виявлення атаки пасивного перехоплення. Аліса і Боб чергують ці режими випадковим чином. Атака виявляється з деякою імовірністю в режимі контролю підслуховування.

Схема режиму передавання повідомлення для оригінального пінг-понг протоколу, в якому використовуються два стани Бела і відповідно не використовується квантове надщільне кодування, показана на рис. 1 [1]. Боб готує повністю переплутаний стан пари кубітів $\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|1\right\rangle + \left|1\right\rangle\left|0\right\rangle\right)$. Він оставляє в себе один з кубітів ("домашній") і посилає другий ("передаваний") Алісі квантовим каналом зв'язку. Аліса виконує кодувальну операцію й повертає кубіт назад Бобові. Кодувальні операції, відповідні двійковим "0" і "1", мають вигляд:

$$U_0 = I;\ \ U_1 = \sigma_z, \tag{1}$$

де $I = \left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|$ – тотожний оператор, $\sigma_z = \left|0\right\rangle\left\langle 0\right| - \left|1\right\rangle\left\langle 1\right|$ – один з операторів Паулі.

Боб після отримання кубіту від Аліси виконує вимірювання в базисі Бела над обома кубітами і при відсутності атаки і природного шуму в каналі зв'язку отримує стан $\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|1\right\rangle + \left|1\right\rangle\left|0\right\rangle\right)$ або $\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|1\right\rangle - \left|1\right\rangle\left|0\right\rangle\right)$ в залежності від того, яка кодувальнаоперація виконана Алісою. Таким чином, цей варіант пінг-понг протоколу дозволяє передати один біт класичної інформації за один раунд режиму передавання повідомлень і є найпростішим з пінг-понг протоколів з найменшою інформаційною місткістю.

В режимі контролю підслуховування (рис. 2) Аліса і Боб виконують однокубітне вимірювання в одному з двох випадково обраних базисів: вертикально-горизонтальному

$B_z = \{|0\rangle, |1\rangle\}$ або діагональному $B_x = \{|+\rangle, |-\rangle\}$. Ці вимірювання дозволяють їм визначити, чи було втручання зловмисника (Єви) на лінії Боб $\rightarrow$ Аліса.

Для сповіщення один одного про зміну режимів у протоколі, для обміну результатами вимірювань в режимі контролю підслуховування, а також при необхідності для корекції помилок Аліса і Боб передають повідомлення звичайним (не квантовим) аутентифікованим каналом зв'язку.

Метод підсилення стійкості пінг-понг протоколу з парами переплутаних кубітів за допомогою гамування. Для підсилення стійкості пінг-понг протоколів можна застосовувати метод гамування [9]. Ідея цього методу полягає в наступному.

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 двійкову гамму γ_i розміром *r* та проводиться додавання отриманих гам з відповідними блоками повідомлення: $b_i = a_i + \gamma_i$.

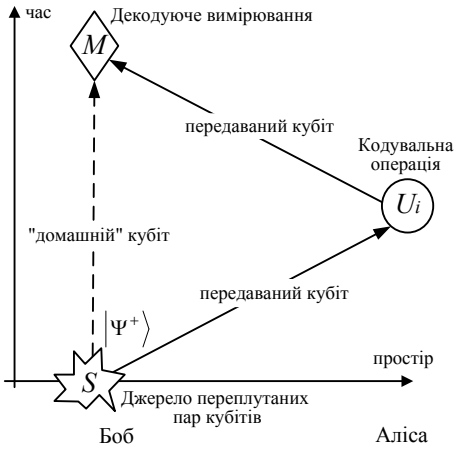

Рисунок 1 – Схема режиму передавання повідомлення

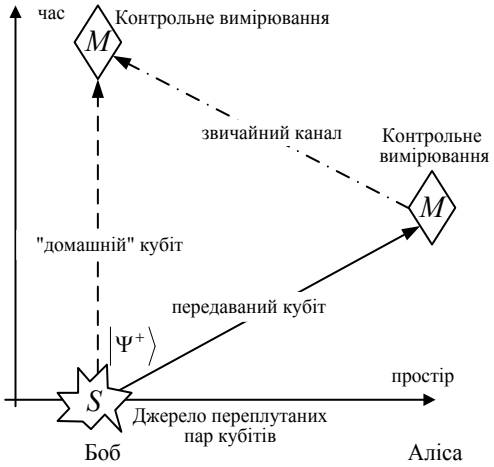

Рисунок 2 – Схема режиму контролю підслуховування

Отримані в результаті блоки b_i передаються квантовим каналом з використанням пінг-понг протоколу. Навіть якщо зловмиснику (Єві) вдасться перехопити один (або декілька) з цих блоків, залишившись не виявленої, то, не знаючи використаних гам γ_i, Єва не може відновити вихідні блоки a_i. Для забезпечення достатнього рівня безпеки довжина блоку *r* і відповідно розмір гам γ_i повинні вибиратися так, щоб ймовірність не виявленняатаки Єви після передачі *одного* блоку була нехтовно малою величиною.

Гами γ_i передаються Бобу звичайним відкритим каналом після завершення квантової передачі, але тільки в тому випадку, якщо Аліса і Боб переконалися у відсутності підслуховування. Потім Боб проводить додавання їх з відповідними блоками b_i, відновлює початкове повідомлення: $a_i = b_i + \gamma_i$.

Відповідно до вищевикладеного методу підсилення стійкості пінг-понг протоколів для імітаційного моделювання протоколу з парами переплутаних кубітів розроб-

лений алгоритм послідовності дій, який полягає в наступному.

Крок 1. Повідомлення розбивається на *l* блоків a_i заданої довжини *r*. Довжина блоку визначається за умови того, що ймовірність невиявлення атаки після передачі одного блоку не перевищує задану величину 10^{-k}[7]:

$$r \geq I = \frac{-kI_0}{\lg((1-q)/(1-q\cdot(1-d)))} \quad (2)$$

де *I*– кількість інформації, яку отримує Єва при передачі одного блоку;

I_0 – кількість інформації, яку отримує Єва за один раунд протоколу;

q– ймовірність переходу в режим контролю підслуховування;

d– рівень помилок, внесений атакою Єви.

Крок 2. Генерація випадкової двійковій гами γ_i розміром *r* та додавання цієї гами з відповідним блоком $b_i = a_i + \gamma_i$ (тобто виконання операції XOR або виключної диз'юнкції).

Крок 3. Виконання режиму передачі повідомлення пінг-понг протоколу з парами переплутаних кубітів (режим контролю підслуховування пінг-понг протоколу не моделювався).

Крок 4.У випадку, коли легітимні користувачі впевнилися у відсутності підслуховування, відбувається передача гам звичайним каналом зв'язку.

Крок 5. Відновлення початкового блоку даних a_i, тобто додавання отриманого блоку b_i з відповідною гаммою γ_i.

Імітаційне моделювання пінг-понг протоколуз парами переплутаних кубітів з використанням методу гамування для підсилення стійкості. Для моделювання роботи режиму передавання повідомлення пінг-понг протоколу з парами переплутаних кубітівз використанням методу гамування, згідно з вищевикладеним алгоритмом, в середовищі програмування C++ Builder [14] розроблено програмне забезпечення, інтерфейс якого показаний на рис. 3. В результаті моделювання отримані статистичні дані про данийметод підсилення стійкості пінг-понг протоколу. Приклад цих даних для рядка довжиною 340 біт також показаний на рис. 3.

Так, згідно з отриманими результатами (див. рис. 3) для передачі повідомлення довжиною 340 біт потрібно його розбити на 5 блоків по 68 біт і для кожного згенерувати свою гаму (ключ шифрування). Потім потрібно передати це закодоване повідомлення квантовим каналом,впевнитись в відсутності прослуховування та передати відкритим каналом відповідні гами для кожного блоку зашифрованого повідомлення, згідно з алгоритмом описаним вище. На приймаючій стороні потрібно зробити розшифрування отриманого повідомлення.

Оцінки обчислювальної складності генерації двійкових гам певного розміру. Для алгоритму, який був описаний вище, були розраховані середні оцінки обчислювальної складності генерації двійкових гам певного розміру *r*, які наведені у табл. 1. Обчислення проводилися на двоядерному процесорі Intel Pentium Dual-CoreT3200 з такими параметрами: тактова частота (MHz): 2000, частота шини (MHz): 667, кеш 2-го рівня (Kb): 1024, підтримується набір команд MMX, SSE, SSE2,SSE3, SSSE3, EM64T. Відповіднепрограмне забезпечення для генерації випадкових двійкових гам певного розміру було розроблене в середовищі програмування C++ Builder. З використанням генератора випадкових чисел виконувалася генерація 1000 випадкових двійкових гам заданого розміру*r* та обчислювався час, який потрібний для генерації однієї такої гами. Описана процедура виконувалася 1000 разів для кожного розміру гам, а потім були обчислені середні значення, які й наведені в табл. 1.

Рисунок 3 – Інтерфейс імітаційної моделі пінг-понг протоколу з парами переплутаних кубітів з використанням методу гамування

Для порівняльного аналізу даного методу підвищення стійкості пінг-понгпротоколу з методом стійкості, який базується на використані зворотного хешування (з використанням обернених матриць), запропонованим в [7], розроблено програмне забезпечення для обертання випадкових двійкових матриць в середовищі програмування C++ Builder, в якому використовується алгоритм LUP-розкладання [15]. За допомогою цього програмного забезпеченнябулозгенеровано1000 псевдовипадкових двійкових матриць заданого розміру r з застосуванням генератора випадкових чисел, з перевіркою їх на оберненість та розрахунком часу, необхідного для генерації однієї оберненої матриці. Для кожного розміру матриць описана процедура виконувалася 1000 разів з обчисленням середнього значення, результати наведені в табл. 1. Згідно з результатами роботи [16], частка обернених в двійковому полі Галуа GF(2) матриць становить 0,289 від повної кількості таких матриць (при $r \geq 16$).

Таблиця 1

Оцінки обчислювальної складності генерації двійкової гам розміру *r* та генерації випадкових обернених матриць розміру $r \times r$

r	Середній час генерації однієї випадкової оберненої матриці, с	Середній час генерації однієї випадкової двійкової гами, с	*r*	Середній час генерації однієї випадкової оберненої матриці, с	Середній час генерації однієї випадкової двійкової гами, с
50	0,0122	0,0009	650	14,610	0,1856
100	0,0728	0,0046	700	18,214	0,2145
150	0,2094	0,0095	750	22,385	0,2460
200	0,4429	0,0169	800	28,452	0,2788
250	0,9184	0,0254	850	31,597	0,3113
300	1,6102	0,0371	900	36,741	0,3557
350	2,5682	0,0502	950	44,027	0,3955
400	3,8923	0,0671	1000	55,075	0,4381
450	5,3113	0,0836	1250	99,148	0,6911
500	6,6605	0,1057	1500	186,75	0,9972
550	8,5056	0,1314	1750	323,18	1,3517
600	11,395	0,1578	2000	438,23	1,7635

Згідно з даними у табл. 1, час генерації однієї випадкової двійкової гами є незначним для невеликих гам навіть на такому порівняно слабкому процесорі. Так, для двійкових гам розміром 500 біт на генерацію однієї гами потрібно приблизно 0,106 секунд, для гам 2000 біт – 1,763 секунд. Генерація ж однієї випадкової оберненої двійкової матриці розміром 500×500 відбувається приблизно за 6,6 секунд, а для матриць 1000×1000 – приблизно за хвилину. Але цей час швидко зростає зі збільшенням розміру матриць.

Таким чином, новий запропонований спосіб підсилення безпеки пінг-понг протоколу потребує значно менше часу на підготовчу операцію – генерацію випадкових гам (ключа шифрування) у полі GF(2) заданого розміру, ніж спосіб, який використовує зворотне хешування [7]. На приймальній стороні процедура відновлення вихідних блоків повідомлення взагалі практично не впливає на ефективність протоколу.

Слід підкреслити, що запропонований метод підсилення стійкості пінг-понг протоколу, хоча і використовує гами для шифрування блоків повідомлення, але (як і запропонований раніше метод з використанням зворотного хешування) не є традиційним потоковим шифруванням. Нема необхідності зберігати гами в секреті, вони передаються відкритим каналом зв'язку *після* того, як користувачі пінг-понг протоколу впевнились, що під час квантового передавання не було атаки пасивного перехоплення, що забезпечується режимом контролю підслуховування самого протоколу. Таким чином, при використанні запропонованого методу підсилення стійкості пінг-понг протоколів не існує проблеми зберігання та передавання секретноїінформації, і основна перевага квантових протоколів безпечного зв'язку, в саме відсутність традиційного шифрування, зберігається при використанні цього методу.

При використанні методу підсилення стійкості, який базується на зворотному хешуванні [7], виконуються складні криптографічні операціїз використанням випадковихдвійкових обернених матриць (перемежування), а при гамуванні виконується тільки проста операція XOR. Але, метод гамування має дещо меншу стійкість, так як для відновлення вихідного блоку даних при зворотному хешуванні зловмиснику потрібно перехо-

пити весь блок повідомлення при його передаванні у квантовому каналі, а при гамуванні він має можливість відразу відновити ту частину блоку даних, яку він перехопив в квантовому каналі. Але, можливість цього може бути зроблена як завгодно малої, якщо легітимні користувачі виберуть достатню довжину блоку для гамування так, щоб імовірність невиявлення атаки в квантовому каналі була як завгодно малою. Якщо ж легітимні користувачі виявлять атаку, то вони не будуть передавати гаму відкритим каналом, і зловмисник не отримає ніякої інформації.

Висновки

Методи симетричного шифрування є одними з актуальних і криптографічно гарантованих методів захисту інформації, якіз відповідною модифікацією можуть застосовуватись і для підсилення стійкості протоколів квантового прямого безпечного зв'язку, зокрема, до пінг-понг протоколу з парами переплутаних кубітів. Запропонований в даній статті метод підсилення стійкості такого протоколу шляхом гамування блоків повідомлення має значно більшу швидкість, ніж метод підсилення стійкості, що ґрунтується на використанні випадкових обернених матриць [7]. При цьому новий метод також зберігає основу перевагу пінг-понг протоколу – відсутність необхідності шифрування повідомлень з розподіленням секретних ключів, – гами не є секретними ключами і передаються відкрито у випадку, якщо не було підслуховування під час передавання блоків повідомлення в квантовому каналі. Таким чином, запропонований в даній статті метод підсилення безпеки пінг-понг протоколу має переваги над відомим раніше і є цілком прийнятним для практичного застосування.

Література

1. Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.
2. Deng F.-G. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block / F.-G. Deng, G.L. Long, X.-S. Liu // Physical Review A. – 2003. – V. 68, № 4. –042317.
3. Wang Ch. Multi–step quantum secure direct communication using multi–particle Greenberger–Horne–Zeilinger state /Ch.Wang, F.G. Deng, G.L. Long // Optics Communications.– 2005. – V. 253, № 1. – P. 15–20.
4. Li X.-H. Multiparty Quantum Remote Secret Conference /X.-H.Li,C.-Y. Li,F.-G. Deng et al // Chinese Physics Letters. – 2007. – V. 24, № 1. – P. 23–26.
5. Jin X.-R. Three-party quantum secure direct communication based on GHZ states / X.-R. Jin, X.Ji, Y.-Q.Zhang et al // Physics Letters A. –2006. –V. 354, № 1-2.– P. 67–70.
6. Василиу Е.В. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием / Е.В. Василиу // Науковіпраці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32–38.
7. Василиу Е.В.Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Науковіпраці ОНАЗ ім. О.С. Попова. – 2009, № 1. – С. 83–91.
8. Ostermeyer, M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. – 2008. – V. 281, issue 17. – P. 4540–4544.
9. АграновскийА.В. Практическая криптография (серия «Аспекты защиты») / А.В. Аграновский, Р.А. Хади. – М.: Солон-Пресс, 2002.– 254 с.
10. Диффи У. Новые направления в криптографии / У.Диффи, М.Э.Хеллман. – М.: ИЛ, 1976. –654 с.
11. Шеннон К. Э. Работы по теории информации и кибернетике / К. Э. Шеннон . – М.: ИЛ, 1963. –832 с.
12. Партыка Т.Л. Информационная безопасность/ Т.Л. Партыка, И.И. Попов. –М.: Форум - Инфра, 2007. –368 с.
13. Кінзерявий В.М. Новий метод підсилення секретності пінг-понг протоколу з парами переплутаних кутритів / В.М. Кінзерявий, Є.В. Василіу, С.О. Гнатюк, Т.О. Жмурко// Захист

інформації. – 2012, №2 (55). – С. 5–13.
14. Архангельский А. Я. Программирование в C++ Builder / А. Я. Архангельский. – М.: Бином-Пресс, 2010.– 1304 с.
15. Кормен Т. Алгоритмы: построение и анализ = Introductionto Algorithms /Т.Кормен,Ч. Лейзерсон, Р. Ривест, К. Штайн.– М.:Вильямс, 2005. – 1296 с. – ISBN 5-8459-0857-4.
16. Overbey J. On the keyspace of the Hill cipher / J. Overbey, W. Traves, J. Wojdylo // Cryptologia. – 2005. – V. 29, № 1. – P. 59– 72.

Надійшла до редколегії 29.04.2013р.

Рецензент: д.т.н., проф. Петров А.С.

Николаенко С.В.

ГАММИРОВАНИЕ КАК МЕТОД УСИЛЕНИЯ СТОЙКОСТИ ПИНГ-ПОНГ ПРОТОКОЛА С ПАРАМИ ПЕРЕПУТАННЫХ КУБИТОВ

В статье рассматривается классический (не квантовый) способ усиления стойкости пинг-понг протокола с парами перепутанных кубитов. Этот способ заключается в шифровании методом гаммирования блоков сообщений и позволяет обеспечить достаточно высокий уровень стойкости протокола. При этом сами гаммы не является секретной информацией, и передаются открытым каналом только после того, как легитимные пользователи убедились в отсутствии атаки в квантовом канале. Разработана имитационная модель пинг-понг протокола с парами перепутанных кубитов в квантовом канале с использованием шифрования методом гаммирования. Выполнен расчет необходимых для обеспечения заданного уровня стойкости протокола, длин блоков сообщения в зависимости от параметров протокола и параметров атакующей операции злоумышленника, а также соответствующий расчет необходимых размеров случайных гам. Выполнены оценки вычислительной сложности генерации гамм для данного метода усиления стойкости. Показано, что время генерации является приемлемым для гамм размером около 2000 бит при использовании вычислительной техники с невысоким быстродействием.

Ключевые слова: квантовая криптография, пинг-понг протокол, метод усиления стойкости протокола, шифрования методом гаммирования, имитационное моделирование, временные оценки.

Nikolaenko S.V.

XOR ENCRYPTION FOR AMPLIFICATION SECURITY OF PING PONG PROTOCOL WITH PAIRS OF ENTANGLED QUBITS

In this paper the classical (not quantum) method of security amplification of the ping-pong protocol with pairs of entangled qubits is considered. This method uses XOR encryption blocks of messages and allows to provide rather high security level of the protocol. Keys are not classified information and transmitted by an open channel only when legitimate users are convinced of the absence of the attack in the quantum channel. The simulation model of ping-pong protocol with pairs of entangled qubits in quantum channel using XOR encryption is developed. Performed the calculation required for providing the given level of security of block lengths depending on the parameters of the protocol and parameters of eavesdropper's operations as well as corresponding calculation of the necessary size of the random keys. Estimated the computational complexity of the generation keys for the given method of amplification security. It is shown that time of generation is acceptable to the keys of about 2000 bits when using computers with a low performance.

Keywords: quantum cryptography, ping-pong protocol, method of amplification security protocol, XOR encryption, simulation, estimating time.