УДК 003.26:621.39+530.145

Василіу Є.В., Мамедов Р.С.
Василиу Е.В., Мамедов Р.С.
Vasiliu E.V., Mamedov R.S.

ОЦІНКИ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ СПОСОБУ ПІДСИЛЕННЯ БЕЗПЕКИ ПІНГ-ПОНГ ПРОТОКОЛУ З ПЕРЕПЛУТАНИМИ СТАНАМИ КУБІТІВ ТА КУТРИТІВ

ОЦЕНКИ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ СПОСОБА УСИЛЕНИЯ БЕЗОПАСНОСТИ ПИНГ-ПОНГ ПРОТОКОЛА С ПЕРЕПУТАННЫМИ СОСТОЯНИЯМИ КУБИТОВ И КУТРИТОВ

COMPUTING COMPLEXITY ESTIMATIONS OF WAY TO SECURITY AMPLIFICATION OF THE PING-PONG PROTOCOL WITH ENTANGLED STATES OF QUBITS AND QUTRITS

Анотація. У статті розглядається неквантовий спосіб підсилення безпеки пінг-понг протоколу з багатокубітними переплутаними станами Грінбергера-Хорна-Цайлінгера та зі станами Бела пар кутритів. Цей спосіб є оборотним гешуванням блоків повідомлень і дозволяє забезпечити високий рівень стійкості протоколу до загальної некогерентної атаки. Виконано розрахунок необхідних для забезпечення заданого рівня стійкості довжин блоків залежно від параметрів протоколу і параметрів атакуючої операції зловмисника, а також відповідний розрахунок необхідних розмірів випадкових оборотних двійкових та трійкових матриць, що виконують роль геш-функцій. Виконано оцінки обчислювальної складності генерації таких матриць. Показано, що час генерації прийнятний навіть для матриць розміром порядку 1000×1000 при використанні обчислювальної техніки з невисокою швидкодією. Запропонований неквантовий спосіб підсилення безпеки пінг-понг протоколу не сильно впливає на ефективність протоколу й, отже, цілком прийнятний для практичного застосування.

Аннотация. В статье рассматривается неквантовый способ усиления безопасности пинг-понг протокола с многокубитными перепутанными состояниями Гринбергера-Хорна-Цайлингера и с состояниями Белла пар кутритов. Этот способ состоит в обратимом хешировании блоков сообщений и позволяет обеспечить высокий уровень стойкости протокола к общей некогерентной атаке. Выполнен расчет необходимых для обеспечения заданного уровня стойкости длин блоков в зависимости от параметров протокола и параметров атакующей операции злоумышленника, а также соответствующий расчет необходимых размеров случайных обратимых двоичных и троичных матриц, выполняющих роль хеш-функций. Выполнены оценки вычислительной сложности генерации таких матриц. Показано, что время генерации приемлемо даже для матриц размером порядка 1000×1000 при использовании вычислительной техники с невысоким быстродействием. Предложенный неквантовый способ усиления безопасности пинг-понг протокола не сильно влияет на эффективность протокола и, следовательно, вполне приемлем для практического применения.

Summary. In this paper non-quantum method of security amplification of the ping-pong protocol with many-qubit entangled Greenberger-Horne-Zeilinger states and also with Bell states of qutrit pairs is considered. This method consists in reversible hashing of messages' blocks and allows ensuring high security level of the protocol against a general incoherent attack. Calculation of blocks lengths, which are necessary for guaranteeing of the given security level, depending on parameters of the protocol and parameters of eavesdropper's attacking operation, and also corresponding calculation of the necessary sizes of the random reversible binary and ternary matrixes which act as a hash-functions is fulfilled. Estimations of generation's computational complexity of such matrixes are carried out. It is shown that generation time is acceptable even for matrixes in the size of 1000×1000 at use of processor with low speed. The proposed non-quantum method of security amplification not strongly influences efficiency of the protocol and, hence, is fully acceptable to practical use.

Квантова криптографія є одним із найважливіших і найбільш розвинених застосувань квантової теорії інформації, що пропонує новий підхід до вирішення важливої проблеми передавання секретних повідомлень [1]. Одним з напрямків квантової криптографії є квантові протоколи безпечного зв'язку, в яких взагалі не використовується шифрування, а таємність передачі гарантується законами квантової механіки [2…4].

На даний час запропоновані різні види квантових протоколів безпечного зв'язку. Одним з таких протоколів є так званий пінг-понг протокол [2], який не потребує для своєї практичної

реалізації великої квантової пам'яті і може виконуватися з використанням існуючого технічного обладнання [5]. У початковому варіанті пінг-понг протоколу використовуються два стани Бела переплутаної пари кубітів, що дозволяє передати один біт класичної інформації за один цикл протоколу [2]. Використання всіх чотирьох белівських станів пари кубітів, тобто квантового надщільного кодування, дозволяє передати два біти за цикл [3]. Подальше збільшення інформаційної місткості можливе при використанні замість переплутаних пар кубітів їх трійок, четвірок і т.д. Так, у роботі [4] був розроблений пінг-понг протокол з переплутаними станами Грінбергера-Хорна-Цайлінгера (ГХЦ) трійок та четвірок кубітів. Інформаційна місткість пінг-понг протоколу з такими станами дорівнює n бітів на цикл, де n – кількість кубітів у використовуваних ГХЦ-станах.

Інший шлях підвищення інформаційної місткості пінг-понг протоколу – це використання переплутаних станів багаторівневих квантових систем. Так, відповідний протокол з використанням белівських станів пари трирівневих систем (кутритів) та квантового надщільного кодування для кутритів був розроблений у роботах [6, 7].

Різні атаки, як на оригінальний пінг-понг протокол, так і на його удосконалені варіанти, були розглянуті в ряді робіт [7…14]. Зокрема було з'ясовано, що всі варіанти пінг-понг протоколу мають тільки асимптотичну стійкість проти атаки з використанням допоміжних квантових систем (загальної некогерентної атаки). За такої атаки агент, що підслуховує (Єва), може одержати деяку кількість інформації, перш ніж її атака буде виявлена [14]. У роботі [15] запропонований неквантовий спосіб підсилення безпеки пінг-понг протоколу, який полягає в оборотному гешуванні бітових блоків повідомлення множенням їх на випадкові оборотні матриці. Цей спосіб може бути застосований також і при реалізації пінг-понг протоколу в квантовому каналі з шумом. Проте розрахунки необхідних довжин блоків у залежності від кількості кубітів у переплутаних станах і стратегії атаки Єви виконані не були. Метою цієї роботи є розрахунок необхідних довжин блоків для гешування й оцінка обчислювальної складності генерації випадкових оборотних матриць необхідного розміру, що дозволить оцінити швидкодію запропонованого способу підсилення безпеки пінг-понг протоколу й відповідно прийнятність цього способу для практики.

1. Кількість інформації Єви при симетричній атаці на пінг-понг протокол з *n*-кубітними ГХЦ-станами. Кількість інформація Єви при атаці з використанням допоміжних квантових систем (проб) на один цикл пінг-понг протоколу з n-кубітними ГХЦ-станами визначається ентропією фон Неймана:

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

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

Як показано у [15], кількість ненульових власних значень матриці щільності дорівнює 2^n, а їх вид при симетричній (див. [13]) атаці Єви:

$$\begin{gathered}\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16 p_1 p_2 \cdot \frac{2^{n-2}}{2^{n-1}-1} d \left(1 - \frac{2^{n-2}}{2^{n-1}-1} d\right)}; \\ - \\ \lambda_{2^n-1,\, 2^n} = \frac{1}{2}(p_{2^n-1} + p_{2^n}) \pm \frac{1}{2}\sqrt{(p_{2^n-1} + p_{2^n})^2 - 16 p_{2^n-1} p_{2^n} \cdot \frac{2^{n-2}}{2^{n-1}-1} d \left(1 - \frac{2^{n-2}}{2^{n-1}-1} d\right)}.\end{gathered} \tag{2}$$

Тут d – імовірність виявлення атаки при однократному переході в режим контролю підслуховування; p_1, p_2, …, p_{2^n} – частоти кодувальних операцій передавальної сторони (Аліси), які збігаються з частотами n-грам у передаваному двійковому повідомленні [15].

При однакових значеннях частот n-грам $p_1 = \ldots = p_{2^n} = 2^{-n}$, тобто коли повідомлення Аліси є випадковим бітовим рядком, формули (2) набувають такого виду [14, 15]:

$$\lambda_{1,2} = \ldots = \lambda_{2^n-1,2^n} = \frac{1}{2^n} \pm \frac{1}{2}\sqrt{\frac{1}{2^{2n-2}} - \frac{1}{2^{2n-4}} \cdot \frac{2^{n-2}}{2^{n-1}-1} d \left(1 - \frac{2^{n-2}}{2^{n-1}-1} d\right)}. \tag{3}$$

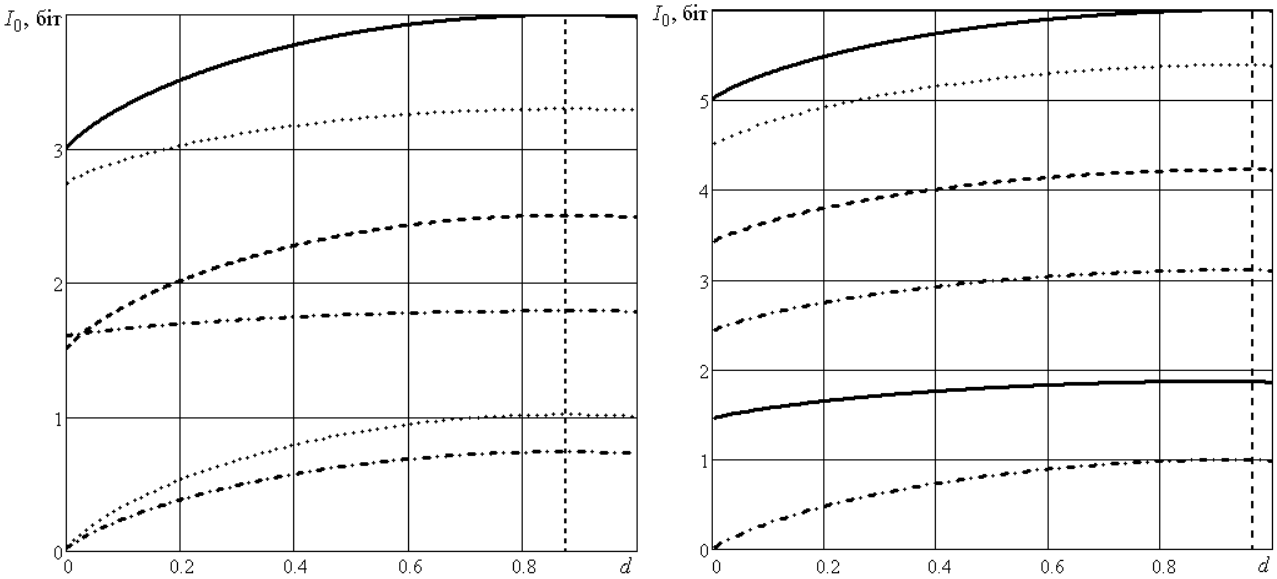
Як показують розрахунки, для більшості наборів частот n-грам p_1 , …, p_{2^n} кількість

інформації Єви I_0 (1) монотонно збільшується зі зростанням імовірності виявлення атаки *d*, поки не досягне максимального значення, яке дорівнює повній інформації, а потім починає зменшуватись (для деяких спеціальних наборів частот *n*-грам I_0 взагалі не залежить від d і є константою). Значення *d*, за якого Єва отримує повну інформацію, залежить від кількості *n* використовуваних у протоколі переплутаних кубітів і визначається формулою [14, 15]:

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

Це значення ймовірності виявлення атаки є максимальним, тому що при $d > d_{\max}$ кількість інформації Єви починає зменшуватись. Отже, Єва не буде вибирати параметри своїх квантових проб, від яких залежить *d*, так щоб *d* перевищувало $d_{\max}$ – для Єви немає сенсу збільшувати ймовірність виявлення атаки при зменшенні доступної їй інформації.

На рис. 1 показані залежності $I_0(d)$ для пінг-понг протоколу з чотири- та шестикубітними ГХЦ-станами для різних наборів частот *n*-грам p_1, …, p_{2^n}. Значення частот, взятих для побудови графіків, не наводяться через їх громіздкість. Так, для протоколу з шестикубітними ГХЦ-станами (рис. 1,б) для побудови кожної кривої бралося 64 різних значень p_i (за умови $p_1 + p_2 + \ldots + p_{64} = 1$). Найвищі криві на рис. 1 відповідають однаковим значенням частот *n*-грам, тобто $p_1 = \ldots = p_{16} = 1/16$ для рис. 1,а та $p_1 = \ldots = p_{64} = 1/64$ для рис. 1,б.



а) б)

Рисунок 1 – Залежність кількості інформації Єви I_0 від імовірності *d* виявлення атаки при симетричній атаці: *n* = 4 (а), *n* = 6 (б). Вертикальні штрихові лінії відповідають $d_{\max}$

Як видно з рис. 1, при $d = 0$ кількість інформації Єви не дорівнює нулю, проте вона нижче свого максимального значення при $d = d_{\max}$. Таким чином, Єва може отримати часткову інформацію, і при цьому її атака не буде виявлена. Проте, такий "невидимий режим" підслуховування існує тільки, якщо легітимні користувачі (Аліса й Боб) використовують для контролю підслуховування один вимірювальний базис. Використання другого вимірювального базису усуває можливість такої атаки, що не виявляється [13]. При цьому навіть коли Єва вибирає параметри своєї атакуючої операції так, щоб в одному з базисів *d* дорівнювало нулю, в іншому базисі *d* буде дорівнювати своєму максимальному значенню $d_{\max}$ (4). Розрахунки показують також, що коли Єва вибирає таку стратегію атаки, за якої в одному з вимірювальних базисів $d = 0$, а частоти

кодувальних операцій Аліси однакові, тоді кількість інформації Єви $I_0 = n-1$ біт (див. верхні криві на рис. 1 при $d = 0$). Таким чином, у цьому випадку кількість інформації, отримуваної Євою, на один біт менше тієї інформації, що передається за один цикл протоколу. При цьому Єва не може розрізнити дві можливі *n*-грами, однак вона може відрізнити цю пару від усіх інших можливих *n*-грам (це випливає зі схеми кодування бітових рядків у пінг-понг протоколі з кубітами). Так, наприклад, для протоколу з белівськими парами кубітів за такої атаки Єва отримає 1 біт інформації, тобто не зможе відрізнити, наприклад, "00" від "01", а також "10" від "11", але завжди зможе відрізнити ці дві альтернативи [10, 12]. У наведеному прикладі Єва точно знає перший біт біграми, але не знає другого; можлива й зворотна ситуація – це залежить від кодувальної схеми Аліси [10, 12].

2. Кількість інформації Єви при симетричній атаці на пінг-понг протокол з белівськими станами пар кутритів. Для цього варіанта пінг-понг протоколу кількість інформації Єви при атаці на один цикл протоколу [7]:

$$I_0 = S(\rho) \equiv -Tr\{\rho \log_3 \rho\} = -\sum_{i=1}^{9} \lambda_i \log_3 \lambda_i \quad \text{(трит)}, \tag{5}$$

де λ_i – власні значення матриці щільності ρ системи "кутрит, що передається – проба Єви". Як показано у [7], ці дев'ять власних значень є коренями трьох кубічних рівнянь:

$$\lambda^3 - (p_{00}+p_{10}+p_{20})\lambda^2 + 3\left(d-\frac{3}{4}d^2\right)(p_{00}p_{10}+p_{00}p_{20}+p_{10}p_{20})\lambda - \frac{27}{4}(d^2-d^3)p_{00}p_{10}p_{20} = 0,$$

$$\lambda^3 - (p_{01}+p_{11}+p_{21})\lambda^2 + 3\left(d-\frac{3}{4}d^2\right)(p_{01}p_{11}+p_{01}p_{21}+p_{11}p_{21})\lambda - \frac{27}{4}(d^2-d^3)p_{01}p_{11}p_{21} = 0,$$

$$\lambda^3 - (p_{02}+p_{12}+p_{22})\lambda^2 + 3\left(d-\frac{3}{4}d^2\right)(p_{02}p_{12}+p_{02}p_{22}+p_{12}p_{22})\lambda - \frac{27}{4}(d^2-d^3)p_{02}p_{12}p_{22} = 0, \tag{6}$$

де p_{ij} ($i,j = 0\ldots2$) є частотами трійкових біграм "00", "10", "20" і т.д. у трійковому рядку Аліси.

При однакових значеннях частот $p_{00} = p_{10} = \ldots = 1/9$, тобто коли повідомлення Аліси є випадковим рядком тритів, власні значення матриці щільності, які є розв'язками рівнянь (6), набувають виду:

$$\lambda_1 = \lambda_2 = \lambda_3 = \frac{1-d}{3}, \qquad \lambda_4 = \lambda_5 = \lambda_6 = \lambda_7 = \lambda_8 = \lambda_9 = \frac{d}{6}. \tag{7}$$

Аналогічно протоколу з *n*-кубітними ГХЦ-станами, для протоколу з белівськими станами пар переплутаних кутритів існує "невидимий режим" підслуховування, який усувається при використанні у режимі контролю підслуховування двох вимірювальних базисів [7]. Максимальне значення ймовірності виявлення атаки для протоколу з парами кутритів $d_{\max} = 2/3$ [7].

3. Кількість інформації Єви при заданій повній імовірності невиявлення атаки. Нехай Єва бажає перехопити інформацію, передану за один цикл пінг-понг протоколу, залишившись при цьому невиявленою. Імовірність такої успішної атаки [2]:

$$s(q,d) = (1-q) + q(1-d)(1-q) + q^2(1-d)^2(1-q) + \ldots = \frac{1-q}{1-q(1-d)}, \tag{8}$$

де q – ймовірність переходу легітимних користувачів у режим контролю підслуховування [2,4].

Доданки у формулі (8) відповідають тому, що атака Єви залишиться невиявленою 0, 1, 2, ... циклів контролю підслуховування до того, як легітимні користувачі перейдуть в режим передачі повідомлення і Єва отримає інформацію $I_0(d)$ (ці доданки є членами геометричної прогресії). Після m успішних атак Єва отримає інформацію $I = m\,I_0(d)$ біт (трит для протоколу з кутритами), і атаки залишаться невиявленими з імовірністю s^m. Тоді імовірність успішного перехоплення $I = m\,I_0(d)$ біт (трит), з урахуванням (8), визначається формулою:

$$s(I,q,d) = s(q,d)^{I/I_0} = \left(\frac{1-q}{1-q(1-d)}\right)^{I/I_0}. \tag{9}$$

Формула (9) була виведена в роботі [2] для пінг-понг протоколу з белівськими парами кубітів і без квантового надщільного кодування, коли в режимі контролю підслуховування досить використовувати один вимірювальний базис. Узагальнимо тепер цю формулу на пінг-понг протокол з *n*-кубітними ГХЦ-станами (для будь-яких *n*), а також на протокол з парами кутритів та надщільним кодуванням для кутритів, коли в режимі контролю підслуховування необхідно використовувати два базиси.

При використанні в режимі контролю підслуховування двох вимірювальних базисів, наприклад *z*- та *x*-базису, ймовірність виявити атаку Єви при однократному переході в режим контролю підслуховування [13]:

$$d = q_z d_z + q_x d_x , \tag{10}$$

де q_z та q_x – ймовірності використання легітимними сторонами *z*- та *x*-базисів відповідно ($q_z + q_x = 1$); d_z та d_x – ймовірності виявити атаку при вимірюваннях у цих базисах.

Найменші значення d_z та d_x дорівнюють нулю, але коли одна із цих величин дорівнює нулю, тоді інша дорівнює своєму максимальному значенню $d_{\max}$ [7, 13]. Оскільки Аліса й Боб не знають заздалегідь, яку стратегію атаки вибере Єва, тобто в якому з базисів вона буде прагнути створити менше значення ймовірності виявлення, то значення q_z та q_x розумно буде вибрати рівними один одному, тобто $q_z = q_x = 1/2$. Найменше значення *d* буде, коли або $d_z = 0$ и $d_x = d_{\max}$, або навпаки. Згідно з (10), за таких умов

$$d = \frac{d_{\max}}{2} . \tag{11}$$

Таким чином, формула (9) справедлива для пінг-понг протоколу з *n*-кубітними ГХЦ-станами, а також для протоколу з переплутаними парами кутритів при використанні в режимі контролю підслуховування двох вимірювальних базисів. У випадку, коли легітимні користувачі перемикаються між цими базисами з однаковою ймовірністю $1/2$, значення *d* в (9) будуть лежати в інтервалі $[d_{\max}/2; d_{\max}]$ залежно від стратегії атаки, яку вибере Єва. Відзначимо, що якщо Єва буде прагнути зменшити значення *d*, то вона буде отримувати лише часткову інформацію. Так для протоколу з *n*-кубітними ГХЦ-станами, якщо Єва вибере параметри своєї атакуючої операції так, щоб d_z дорівнювало нулю, то d_x буде дорівнювати $d_{\max}$ і $d = d_{\max}/2$, а кількість інформації Єви при однакових значеннях частот *n*-грам буде на 1 біт менше повної інформації (див. рис. 1). Аналогічно для протоколу з белівськими станами пар кутритів при $d_z = 0$ та $d_x = d_{\max}$ (або навпаки) кількість інформації Єви дорівнює одному триту, що на один трит менше інформації, яка передається за один цикл цього протоколу [7]. Якщо ж Єва захоче одержати повну інформацію, то вона повинна буде так вибрати параметри своєї атакуючої операції, щоб $d_z = d_x = d_{\max}$ і при цьому, згідно з (10), $d = d_{\max}$.

Для забезпечення високого рівня безпеки пінг-понг протоколу ймовірність успішної атаки Єви $s(I, q, d)$ (9) повинна бути нехтовно малою величиною. Припустимо $s(I, q, d) = 10^{-k}$ і виразимо з (9) кількість інформації Єви *I*, злогарифмував обидві частини цієї рівності:

$$I = \frac{-kI_0}{\lg\left(\dfrac{1-q}{1-q(1-d)}\right)} . \tag{12}$$

У табл. 1 та 2 наведені округлені (у більшу сторону) значення *I* при *k* = 6 та *k* = 4 відповідно для протоколу з *n*-кубітними ГХЦ-станами, а в табл. 3 – для протоколу з переплутаними парами кутритів. На рис. 2 показана залежність *I* від *n* та від *q* для *k* = 4 і $d = d_{\max}$. Видно, що при заданому *q* залежність *I* від *n* майже лінійна, а при заданому *n* залежність *I* від *q* експоненційна. На рис. 3,а точками показані значення *I* при *k* = 4, *q* = 0,5 та $d = d_{\max}$, також показана апроксимуюча пряма, отримана методом найменших квадратів. Аналогічно на рис. 3,б точками показані значення *I* при *k* = 4, *n* = 4 та $d = d_{\max}$, а також показаний графік апроксимуючої експоненційної функції. Як видно з рис. 3, лінійна функція з великою точністю апроксимує залежність *I* від *n*, а експоненційна функція також з великою точністю апроксимує залежність *I* від *q*.

Таблиця 1 – Кількість інформації Єви для протоколу з *n*-кубітними ГХЦ-станами при ймовірності невиявлення атаки $s = 10^{-6}$, біт

n	$q = 0{,}5;\ d = d_{\max}$	$q = 0{,}5;\ d = d_{\max}/2$	$q = 0{,}25;\ d = d_{\max}$	$q = 0{,}25;\ d = d_{\max}/2$
2	69	113	180	313
3	74	122	186	330
4	88	145	216	387
5	105	173	254	458
6	123	204	297	537
7	142	236	341	620
8	161	268	387	706
9	180	302	434	793
10	200	335	481	881
11	220	369	529	970
12	240	403	577	1059
13	260	437	625	1149
14	279	471	673	1238
15	299	505	721	1328
16	319	539	769	1417
17	339	573	817	1507
18	359	607	865	1597
19	379	641	913	1686
20	399	675	961	1776

Таблиця 2 – Кількість інформації Єви для протоколу з *n*-кубітними ГХЦ-станами при ймовірності невиявлення атаки $s = 10^{-4}$, біт

n	$q = 0{,}5,\ d = d_{\max}$	$q = 0{,}5,\ d = d_{\max}/2$	$q = 0{,}25,\ d = d_{\max}$	$q = 0{,}25,\ d = d_{\max}/2$
2	46	75	120	209
3	50	82	124	220
4	59	97	144	258
5	70	116	170	306
6	82	136	198	358
7	94	157	228	413
8	107	179	258	471
9	120	201	290	529
10	133	224	321	588
11	147	246	353	647
12	160	269	385	706
13	173	291	417	766
14	186	314	449	826
15	200	337	481	885
16	213	360	513	945
17	226	382	545	1005
18	240	405	577	1065
19	253	428	609	1124
20	266	450	641	1184

Таблиця 3 – Кількість інформації Єви для протоколу з белівськими станами пар кутритів, біт (трит)

s	$q = 0{,}5,\ d = d_{\max}$	$q = 0{,}5,\ d = d_{\max}/2$	$q = 0{,}25,\ d = d_{\max}$	$q = 0{,}25,\ d = d_{\max}/2$
10^{-4}	58 (36)	91 (58)	146 (92)	248 (157)
10^{-6}	86 (54)	137 (86)	219 (138)	372 (235)

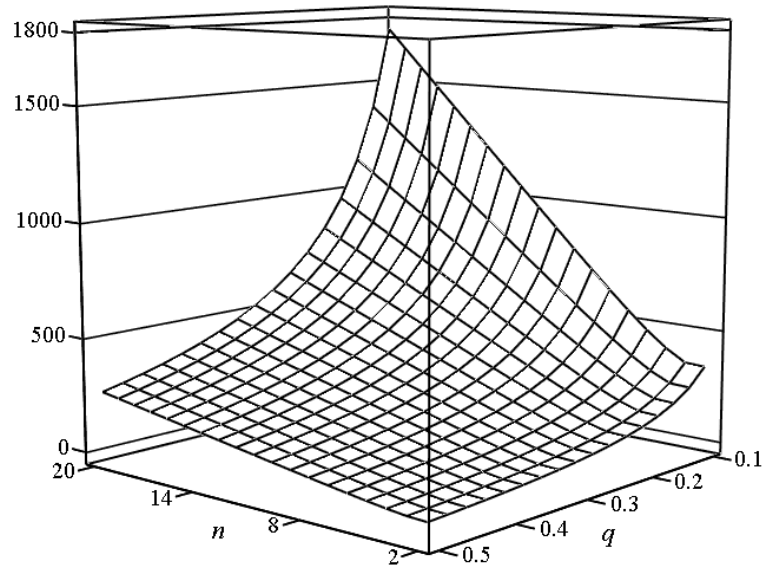
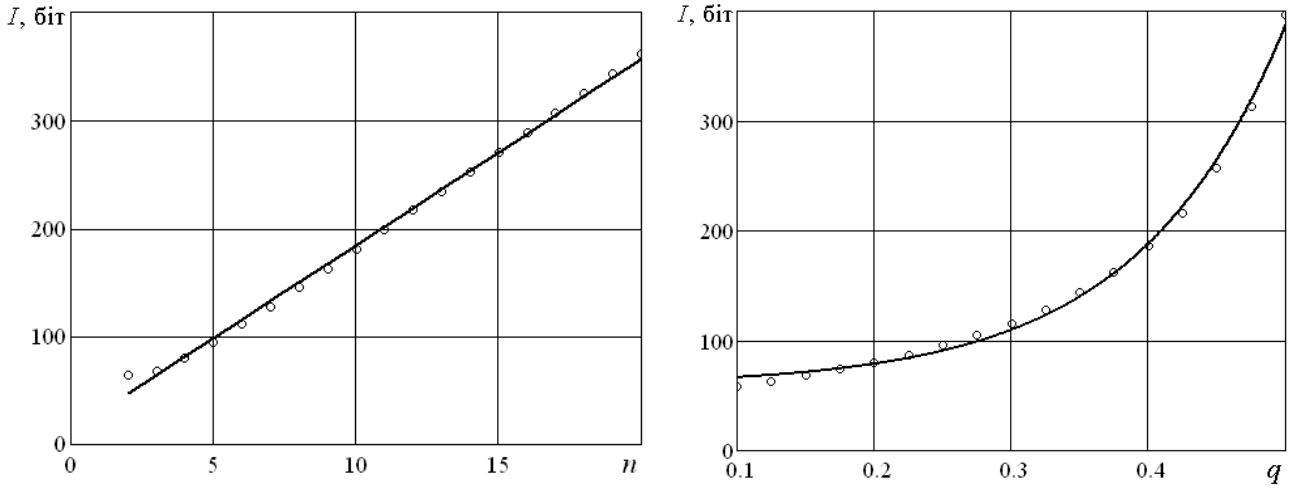


Рисунок 2 – Кількість інформації Єви для протоколу з *n*-кубітними ГХЦ-станами при $s = 10^{-4}$ і $d = d_{\max}$



а) б)

Рисунок 3 – Залежність кількості інформації Єви *I* від *n* (а) та від *q* (б)

Таким чином, при збільшенні кількості кубітів *n* у переплутаних ГХЦ-станах кількість інформації, яку може перехопити Єва за даного *s*, зростає лінійно. Це пояснюється лінійним зростанням кількості інформації, що передається за один цикл пінг-понг протоколу, при збільшенні *n*. У той самий час зі зменшенням *q* кількість інформації Єви зростає за експоненційним законом як для протоколу з *n*-кубітними ГХЦ-станами, так і для протоколу з белівськими станами пар кутритів. Оскільки ефективність пінг-понг протоколу з *n*-кубітними ГХЦ-станами дорівнює $n \cdot (1-q)$ біт/цикл, а протоколу з белівськими станами пар кутритів – $2 \cdot (1-q)$ трит/цикл, то зменшення *q* дозволяє збільшити ефективність протоколу, але при цьому кількість інформації, що перехоплюється, зростає експоненційно.

4. Спосіб підсилення безпеки пінг-понг протоколу та оцінки обчислювальної складності. Відповідно до схеми пінг-понг протоколу, легітимні користувачі чергують режими передачі повідомлення й контролю підслуховування, переходячи в останній з імовірністю *q* [2, 4, 15]. При

використанні ідеального квантового каналу зв'язку перший же невірний результат, отриманий при вимірюваннях у режимі контролю підслуховування, свідчить про операції Єви. Отже, отримавши першу ж помилку при контролі підслуховування, Аліса і Боб негайно переривають сеанс зв'язку. При цьому, тому що ймовірність виявити атаку при однократному контролі підслуховування досить велика, Аліса й Боб з високою ймовірністю виявлять атаку після декількох сеансів контролю підслуховування, і Єва не отримає тієї кількості інформації, що наведена в табл. 1…3 для дуже малих повних ймовірностей невиявлення атаки.

У випадку ж квантового каналу із шумом, очевидно, Аліса і Боб не можуть перервати сеанс зв'язку відразу ж після виникнення першої помилки в режимі контролю підслуховування, оскільки така помилка може бути викликана природним шумом у каналі, а не підслуховуванням, і не існує способу відрізнити помилки, зумовлені цими двома причинами. За наявності квантового каналу з незначним рівнем шумів *ma* можливості зневажити витоком одного-двох десятків початкових біт (або трит) повідомлення, Аліса і Боб можуть виконувати протокол, поки кількість невірних результатів у режимі контролю підслуховування не стане явно перевищувати очікуваний незначний рівень. Таким чином, за вищенаведених умов пінг-понг протокол може виконуватися без додаткових заходів з підсилення його безпеки.

Але для квантового каналу зі значним рівнем шумів легітимним користувачам уже складніше прийняти рішення, або слід перервати сеанс зв'язку. У цьому випадку потрібні додаткові заходи щодо підсилення безпеки пінг-понг протоколу. Такі заходи потрібні також і у випадку, коли неприпустимий навіть надто незначний витік інформації. Відзначимо, що виконані до цього часу численні експерименти з передавання кубітів оптоволоконними каналами показують, що передача з невеликим рівнем помилок (кілька відсотків) можлива на відстань у кілька десятків км [16]. Передача на відстань понад 100 км відбувається вже з більш значним рівнем помилок [17]. Оскільки на цей час ще не існує пристроїв, що виконують функції квантових повторювачів, то у випадку потреби передавати інформацію за допомогою квантових протоколів на відстані понад 100 км, користувачі зіштовхуються зі значним рівнем завад у квантовому каналі. Відзначимо, що в цьому випадку пінг-понг протокол має більшу перевагу порівняно з багатьма іншими квантовими протоколами розподілу ключів (а пінг-понг протокол, зрозуміло, може використовуватися і як квантовий протокол розподілу ключів) через те, що підслуховування в цьому протоколі створює значно більш високий рівень помилок. Так, наприклад, рівень помилок, зумовлених простою атакою "перехоплення – повторної посилки" кубітів у протоколі BB84 становить 25%, а більш складні атаки дозволяють суттєво знизити цей рівень [18]. У пінг-понг протоколі з переплутаними парами кубітів рівень спричинених атакою помилок становить 50% і швидко прямує до 100% зі збільшенням кількості переплутаних кубітів n (див. (4)), а у протоколі з переплутаними парами кутритів дорівнює 66,67%. Таким чином, пінг-понг протокол може використовуватись як для розподілу секретних ключів, так і для прямого передавання секретних повідомлень на великі відстані. Проте для цього необхідно доповнити протокол процедурою, що забезпечить високий рівень його стійкості до загальної некогерентної атаки.

Відповідна процедура була запропонована в роботі [15]. Наведемо тут її опис.

Перед початком передачі Аліса розбиває своє двійкове повідомлення (для протоколу з n-кубітними ГХЦ-станами) на l блоків деякої фіксованої довжини r, позначимо ці блоки через a_i ($i = 1,\ldots l$). Потім Аліса генерує для кожного блока окремо випадкову, оборотну над полем Галуа GF(2) (оборотну двійкову) матрицю M_i розміру $r \times r$ й множить отримані матриці на відповідні блоки повідомлення (множення виконується за модулем 2):

$$b_i = M_i a_i . \qquad (13)$$

Аналогічно для протоколу з белівськими парами кутритів Аліса розбиває своє трійкове повідомлення на l блоків, для кожного блока окремо генерує випадкову, оборотну над полем Галуа GF(3) (оборотну трійкову) матрицю M_i та множить отримані матриці на відповідні блоки повідомлення за модулем 3.

Отримані в результаті блоки передаються квантовим каналом з використанням пінг-понг протоколу. Навіть якщо Єві вдасться перехопити один (або декілька) із цих блоків, залишившись невиявленою, то, не знаючи використаних матриць M_i, Єва не зможе відновити вихідні блоки a_i. Очевидно, що атака прямого перебору матриць стає абсолютно нездійсненною (при поточному рівні

швидкодії обчислювальної техніки) уже при їхньому розмірі порядку 16×16, тому що кількість оборотних двійкових матриць такого розміру дорівнює $0{,}289 \cdot 2^{256}$, а кількість оборотних трійкових матриць ще значно вища: $0{,}56 \cdot 3^{256}$ [19].

Для забезпечення високого рівня стійкості довжина блока *r* і відповідний розмір матриць M_i ($r \times r$) повинні вибиратися так, щоб імовірність успішної атаки Єви *s* (9) після передачі *одного* блока була нехтовно малою величиною. Матриці M_i передаються Бобові по звичайному відкритому каналу після завершення квантового передавання, але тільки в тому випадку, якщо Аліса й Боб переконалися у відсутності підслуховування в квантовому каналі. Потім Боб обертає отримані матриці й, помноживши їх на відповідні блоки b_i, відновлює вихідні блоки повідомлення:

$$a_i = M_i^{-1} b_i . \qquad (14)$$

Для квантового каналу зі значним рівнем шумів Аліса повинна спочатку передати деяку кількість блоків b_i, достатню для того, щоб можна було зробити статистично значиму оцінку рівня помилок, які реєструються в режимі контролю підслуховування. Потім ця оцінка порівнюється з відомим заздалегідь граничним значенням природного рівня шумів у даному квантовому каналі. Якщо зроблена оцінка рівня помилок перевищує допустиме значення, то сеанс зв'язку переривається, тому що це перевищення приписується підслуховуванню Єви, а підслуховування в пінг-понг протоколі створює досить високий додатковий рівень помилок. Інакше передається наступна послідовність блоків і знову виконується оцінка рівня помилок. Матриці M_i передаються всі разом тільки після успішного завершення квантового передавання.

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 над полем Галуа матриця чисел. Також слід зазначити, що якщо ентропія вихідного блока даних a_i невелика, то множення на випадкову матрицю суттєво збільшує ентропію, так що передаваний блок b_i буде виглядати як випадковий рядок (якщо ентропія блоку a_i велика, наприклад, він є частиною файла, стиснутого ентропійними методами кодування, то множення на випадкову матрицю може незначно зменшити ентропію, але вона все одно залишиться близькою до максимальної). Таким чином, множення на випадкову матрицю виконує також функцію скремблювання.

Для кожного блока повинна використовуватись своя матриця M_i, що дозволить запобігти криптоаналітичним атакам, подібним до атак на шифр Хіла, які можливі там за багаторазового використання однієї матриці для шифрування різних блоків. Подібну атаку Єва могла б провести, якби їй вдалося до виявлення її операцій у квантовому каналі перехопити кілька блоків, що гешовані з однієї й тією ж матрицею. Оскільки матриці у даному випадку не є ключами і їх можна передавати по відкритому звичайному каналу, то передача потрібної кількості матриць не є проблемою.

Але виникає питання про час, який необхідний Алісі для генерації потрібної кількості оборотних матриць певного розміру. Аліса визначає розмір матриць, виходячи з бажаної ймовірності невиявлення атаки *s* (9). Для протоколу з *n*-кубітними ГХЦ-станами, при $s = 10^{-6}$ та $s = 10^{-4}$ кількість інформації *I*, яку може отримати Єва, наведена в табл. 1 і 2 відповідно. Для протоколу з белівськими станами пар кутритів *I* наведена в табл. 3. При цьому Єва може застосовувати різні стратегії атаки, зменшуючи величину *d* в інтервалі від $d_{\max}$ до $d_{\max}/2$ за рахунок зменшення доступної їй інформації, як встановлено в розд. 3 цієї статті. Звичайно, легітимні користувачі не знають, яку стратегію вибере Єва. Тому, якщо вони хочуть забезпечити найвищий рівень стійкості протоколу, то їм слід виходити з тієї кількості інформації, яку може отримати Єва при мінімально можливому *d*, а саме при $d = d_{\max}/2$.

Ще один параметр, який повинні вибрати Аліса й Боб, – це ймовірність переходу в режим контролю підслуховування *q*. Оскільки ефективність протоколу зростає зі зменшенням *q*, то вони зацікавлені у виборі як можна меншого *q*. Однак кількість інформації Єви залежить від *q* експоненційно (див. рис. 2 та рис. 3,б). Отже, і розмір необхідних матриць для гешування теж буде

зростати експоненційно, і також буде зростати час, який необхідний для їхньої генерації й перевірки на оборотність.

Таким чином, при заданому q розмір матриці необхідно вибирати з умови $r \geq I$ (при деякому d з інтервалу $[d_{\max}/2; d_{\max}]$), а також для протоколу з n-кубітними ГХЦ-станами з умови: r кратне n (тому що інформація в цьому протоколі передається блоками розміром n біт). Так, наприклад, для протоколу із чотирикубітними станами при $q = 0{,}25$, $s = 10^{-4}$ та $d = d_{\max}/2$ кількість інформації Єви I = 258 біт (див. табл. 2). Отже, Аліса повинна згенерувати необхідну кількість випадкових оборотних двійкових матриць розміром 260×260.

У табл. 4 наведені середні оцінки обчислювальної складності генерації випадкових двійкових та трійкових матриць певного розміру з перевіркою згенерованої матриці на оборотність. Обчислення проводилися на двоядерному процесорі Intel Celeron E1400 (тактова частота 2 ГГЦ, кеш другого рівня 512 Кб, підтримується набір команд SSE2) з використанням одного ядра. Відповідна програма була написана мовою програмування Matlab, оскільки там є вбудовані процедури модулярної арифметики. З використанням генератора псевдовипадкових чисел виконувалася генерація 1000 псевдовипадкових двійкових або трійкових матриць заданого розміру, перевірка їх на оборотність і обчислювався час, який потрібний для генерації однієї оборотної матриці. Описана процедура виконувалася 40 разів для кожного розміру матриць, а потім були обчислені середні значення, які й наведені в табл. 4. Відзначимо, що згідно з результатами роботи [19], частка оборотних над полем Галуа GF(2) матриць становить 0,289, а частка оборотних над полем Галуа GF(3) – 0,56 від повної кількості таких матриць (при $r \geq 16$).

Таблиця 4 – Оцінки обчислювальної складності генерації випадкових оборотних матриць розміру $r \times r$

r	Середнє число оборотних матриць із 1000 випадково згенерованих	Середній час генерації однієї випадкової оборотної матриці, с	Середній час зворотного гешування методом Гаусса, с
Матриці, які оборотні над полем GF(2)			
75	289	0,6	0,025
100	289	1,1	0,044
150	286	3,0	0,098
200	290	5,5	0,162
250	287	9,7	0,307
300	285	17,1	0,505
400	287	34,7	1,18
500	290	61,3	1,96
750	280	137,6	6,41
1000	297	388,1	15,7
Матриці, які оборотні над полем GF(3)			
50	563	0,3	0,026
100	563	1,4	0,080
150	557	2,9	0,138
200	557	6,1	0,240

Оскільки Боб одержує від Аліси матриці, які точно є оборотними, то він може відновлювати вихідні блоки повідомлення за формулою (14) без знаходження явного виду зворотних матриць M_i^{-1}, використовуючи метод Гаусса розв'язання систем лінійних рівнянь. Для цього потрібно значно менше процесорного часу. В табл. 4 наведено середній час такого зворотного гешування за формулою (14) з використанням методу Гаусса. Для обчислення цього середнього часу генерувалося по 10000 випадкових оборотних матриць заданого розміру.

Відзначимо, що використання двоядерного процесора дозволяє повністю завантажити описаними розрахунками одне ядро, інші програми, у тому числі системні, виконуються на другому

ядрі. Таким чином, наведені в табл. 4 оцінки обчислювальної складності відповідають стовідсотковому навантаженню на одне ядро процесора, характеристики якого наведені вище.

Як випливає з табл. 4, час генерації однієї випадкової оборотної матриці, як двійкової, так і трійкової, є незначним для невеликих матриць навіть на такому порівняно слабкому процесорі. Але цей час швидко зростає зі збільшенням розміру матриць. Так, для двійкових матриць розміром 500×500 на генерацію однієї оборотної матриці потрібно вже більше хвилини, а для матриць 1000×1000 – більше 6 хвилин. Підкреслимо, що використання більш продуктивної обчислювальної техніки – багатоядерних або багатопроцесорних систем – дозволить значно скоротити час генерації матриць. Так, наприклад, чотириядерний процесор Intel Core 2 Extreme QX9650 з тактовою частотою 3 ГГц продуктивніше використовуваного нами більше, ніж у два рази (на одне ядро). Отже, при використанні навіть одного такого процесора із завантаженням, допустимо, трьох його ядер, час генерації матриць зменшиться як мінімум у шість разів.

У той самий час, як показує табл. 4, Бобові для відновлення вихідних блоків повідомлення високопродуктивна обчислювальна техніка не потрібна.

Таким чином, запропонований спосіб підсилення безпеки пінг-понг протоколу не потребує значного часу на підготовчу операцію: генерацію випадкових, оборотних над полем GF(2) (або GF(3)) матриць заданого розміру, навіть при розмірі матриць порядку 1000×1000. На приймальній стороні процедура відновлення вихідних блоків повідомлення взагалі практично не впливає на ефективність протоколу.

Слід зазначити, що загальна ефективність пінг-понг протоколу залежить також від значної кількості факторів, пов'язаних з роботою устаткування, таких як складність маніпуляцій із багатокубітними та багатокутритними переплутаними квантовими станами, ефективність датчиків, рівень завад у квантовому каналі тощо. Так, ефективність протоколу з *n*-кубітними ГХЦ-станами зростає зі збільшенням кількості кубітів *n* у використовуваних ГХЦ-станах, але одночасно із цим може зростати й час, що потрібний для маніпуляцій із цими станами, і ймовірність помилок, зумовлених недосконалістю устаткування, що приведе до зниження ефективності протоколу. Як випливає з результатів цієї статті, для протоколу з *n*-кубітними ГХЦ-станами при збільшенні *n* зростає й час, потрібний для підготовчих операцій, тобто генерації необхідної кількості випадкових, оборотних над полем GF(2) матриць для гешування, що також приведе до зниження ефективності протоколу. З іншого боку, ефективність протоколу, як з кубітами, так і з кутритами, збільшується при зменшенні ймовірності переходу користувачів у режим контролю підслуховування, але при цьому знову зростає час, потрібний для генерації матриць. Таким чином, питання про знаходження таких параметрів пінг-понг протоколу, які б забезпечували найвищу його ефективність при врахуванні всіх необхідних факторів, може бути розв’язане тільки шляхом відповідних експериментальних досліджень та відповідного імітаційного моделювання.

На закінчення відзначимо наступне. У роботі виконано розрахунок необхідних довжин блоків для оборотного гешування блоків повідомлення, що передається за допомогою пінг-понг протоколу з *n*-кубітними ГХЦ-станами або зі станами Бела пар кутритів. Показано, що необхідна довжина блока зростає лінійно зі зростанням кількості кубітів у переплутаних ГХЦ-станах і екпоненційно – зі зменшенням ймовірності переходу легітимних користувачів у режим контролю підслуховування. Виконано оцінки обчислювальної складності генерації випадкових, оборотних над полями GF(2) та GF(3) матриць. Показано, що час генерації прийнятний навіть для матриць розміром порядку 1000×1000 при використанні обчислювальної техніки з невисокою швидкодією. Таким чином, запропонований спосіб підсилення безпеки пінг-понг протоколу не надто вплине на ефективність усього протоколу й є цілком прийнятним для практичного застосування.

Література

1. *Баумейстер Д.* Физика квантовой информации / Баумейстер Д., Экерт А., Цайлингер А. – М.: Постмаркет, 2002. – 376 с.
2. *Bostrom K*. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.
3. *Cai Q.-Y*. Improving the capacity of the Bostrom – Felbinger protocol / Q.– Y. Cai, B.– W. Li // Physical Review A. – 2004. – V. 69, № 5. – 054301.

4. *Василиу Е.В.* Пинг-понг протокол с трех– и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера / Е.В. Василиу, Л.Н. Василиу // Труды Одесского политехнического университета. – 2008. – Вып. 1(29). – С. 171–176.
5. *Ostermeyer M*. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. – 2008. – V. 281, № 17. – P. 4540–4544.
6. *Quantum* secure direct communication with high dimension quantum superdense coding / Ch. Wang, F.-G. Deng, Y.-S. Li [et al] // Physical Review A. – 2005. – V. 71, № 4. – 044305.
7. *Василиу Е.В.* Анализ атаки пассивного перехвата на пинг-понг протокол с полностью перепутанными парами кутритов / Е.В. Василиу, Р.С. Мамедов // Восточноевропейский журнал передовых технологий. – 2009, № 4/2 (40). – С. 4–11.
8. *Zhang Zh.-J*. Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss / Zh.-J. Zhang, Y. Li, Zh.-X. Man // Physics Letters A. – 2005. – Vol. 341, № 5–6. – P. 385–389.
9. *Cai Q.-Y*. The «Ping-pong» protocol can be attacked without eavesdropping / Q.-Y. Cai // Physical Review Letters. – 2003. – Vol. 91, № 10. – 109801.
10. *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.
11. *Cai Q.-Y*. Deterministic secure communication without using entanglement / Q.-Y. Cai, B.-W. Li // Chinese Physics Letters. – 2004. – Vol. 21, № 4. – P. 601– 603.
12. *Василиу Е.В*. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32–38.
13. *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.
14. *Николаенко С.В*. Утечка информации к злоумышленнику в пинг-понг протоколе с N перепутанными кубитами / С.В. Николаенко; науч. рук., доц., к. ф.-м. н. Василиу Е.В. // Радиоэлектроника и молодежь в XXI веке: Материалы 13-го международного молодежного форума. – Харьков, 2009. – Ч 2. – С. 59.
15. *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.
16. *Megabits* secure key rate quantum key distribution / Q. Zhang, H. Takesue, T. Honjo [et al] // New Journal of Physics. – 2009. – V. 11. – 045010.
17. *Practical* long-distance quantum key distribution system using decoy levels / D. Rosenberg, C.G. Peterson, J.W. Harrington [et al] // New Journal of Physics. – 2009. – V. 11. – 045009.
18. *Василиу Е.В.* Стойкость квантовых протоколов распределения ключей типа "приготовление–измерение" / Е.В. Василиу // Georgian Electronic Scientific Journal: Computer Science and Telecommunications. – 2007, № 2(13). – С. 50–62. – Режим доступа к журн.: http://gesj.internet–academy.org.ge
19. *Overbey J*. On the keyspace of the Hill cipher / J. Overbey, W. Traves, J. Wojdylo // Cryptologia. – 2005. – V. 29, № 1. – P. 59– 72.