

НОВИЙ МЕТОД ПІДСИЛЕННЯ СЕКРЕТНОСТІ ПІНГ-ПОНГ ПРОТОКОЛУ З ПАРАМИ ПЕРЕПЛУТАНИХ КУТРИТІВ

Запропоновано новий метод підсилення секретності пінг-понг протоколу з парами переплутаних кутритів, який дозволяє підвищити ефективність його роботи. Розроблено генератор тритових послідовностей, за допомогою якого формується тритова ключова послідовність, що використовується в методі підсилення секретності.

Ключові слова: квантова криптографія, пінг-понг протокол, стійкість протоколу, підсилення секретності, кутрит, генератор трійкових послідовностей.

Вступ. Внаслідок масової інформатизації збільшуються обсяги електронних інформаційних ресурсів, які потребують все більш досконалих методів захисту. Найбільш розповсюджені з них направлені на збереження конфіденційності та, здебільшого, забезпечуються криптографічними методами і засобами захисту. Проте, більшість традиційних криптографічних методів базується на складності вирішення певних математичних задач, які у зв'язку з швидким розвитком обчислювальних засобів (суперкомп'ютери, квантові комп'ютери, GRID-технології тощо) в майбутньому можуть бути розв'язані. Ймовірною альтернативою можуть бути методи квантової криптографії (КК), що є найбільш розвинутих напрямком квантової теорії інформації. Основна задача КК полягає у створенні каналу передачі інформації, абсолютна захищеність якого буде гарантуватись фундаментальними законами природи (квантової механіки), що дозволяють зафіксувати будь-яку спробу проникнення ззовні [1-3]. Однак, робота систем захисту інформації на базі квантових протоколів потребує не лише використання самих протоколів, а й паралельного використання засобів класичної криптографії та завадостійкого кодування, оскільки, не менш важливими є виправлення помилок та підсилення секретності [3].

Значний інтерес серед наукової спільноти викликають, зокрема, протоколи квантового прямого безпечного зв'язку (КПБЗ) [1, 2, 4, 5], характерною особливістю яких є відсутність будь-яких криптографічних перетворень (таким чином вирішена проблема розподілу ключів шифрування, що є дуже актуальною в традиційній криптографії). Одним із найпоширеніших методів КПБЗ є пінг-понг протокол [1, 6], який не потребує великого об'єму квантової пам'яті та може використовуватися в існуючих системах захисту інформації [7]. Однак, оригінальний варіант протоколу не зовсім придатний до практичного застосування в системах КК, так як не відповідає в повній мірі вимогам до сучасних систем зв'язку. З огляду на це, розроблено цілий ряд методів [2, 5, 6, 8] підвищення ефективності даного протоколу. Проте, їх не можна вважати досконалими, тому роботи, пов'язані з підвищенням ефективності пінг-понг протоколу, не втратили своєї актуальності.

Метою роботи є підвищення ефективності роботи пінг-понг протоколу з парами переплутаних кутритів. Під ефективністю, у даному випадку, будемо мати на увазі підвищення стійкості та швидкодії протоколу.

1. Метод підсилення безпеки пінг-понг протоколу з парами повністю переплутаних кутритів

Пінг-понг протокол має два режими роботи, а саме, режим передачі повідомлення та режим контролю підслуховування [1, 9, 10]. У якості кубітів у оригінальному варіанті пінг-понг протоколу використовуються фотони, максимально переплутані за їх поляризаційними ступенями свободи (стани Белла). Інформація кодується фазою переплутаних кубітів. Оскільки тільки один кубіт передається від відправника – Боба до приймача – Аліси (пінг), а потім назад від Аліси до Боба (понг), закодована інформація не може бути вилучена зміною стану цього одного кубіту. Декодування стає можливим лише при виконанні вимірювання в базисі Белла обох кубітів, що дозволяє визначити їх кореляцію один з одним. У режимі

контролю підслуховування легітимні користувачі аналізують рівень помилок, якщо цей рівень перевищує допустимий, то користувачі переривають сеанс зв'язку.

У початковому варіанті протоколу кожний кубіт, що передається (один з переплутаної пари), використовується для кодування одного класичного біту. На сьогодні, існують різні модифікації протоколу [2, 5, 6, 8], які, використовуючи квантове надщільне кодування та багатовимірні квантові системи – кудити (кутрити, кукварти і т.д.), дозволяють підвищити інформаційну місткість протоколу. Різні атаки, як на оригінальний пінг-понг протокол, так і на його вдосконалені варіанти, були розглянуті в ряді робіт [11-15]. Зокрема, була проаналізована атака з використанням допоміжних квантових систем (загальна некогерентна атака) на різні варіанти пінг-понг протоколу, в тому числі на протокол з парами кутритів [11]. За такої атаки Єва може одержати деяку кількість інформації, перш ніж її атака буде виявлена [11, 14, 15] – так звана асимптотична стійкість (недолік у порівнянні з абсолютно стійкими системами квантового розподілу ключів [4]).

У роботі [9] запропоновано неквантовий метод підсилення асимптотичної стійкості пінг-понг протоколу з парами повністю переплутаних кутритів, який полягає в наступному:

1) Перед передачею Аліса розбиває своє трійкове повідомлення розміром m на l блоків деякої фіксованої довжини r , які позначає як a_i ($i = \overline{1, l}$).

2) Потім Аліса генерує для кожного a_i випадкову оборотну трійкову матрицю M_i розміру $r \times r$.

3) Після чого множенням матриці на блок даних утворює нове повідомлення: $b_i = M_i a_i$.

4) Отримані в результаті блоки b_i Аліса передає квантовим каналом з використанням пінг-понг протоколу, при цьому легітимні користувачі аналізують рівень помилок у режимі контролю підслуховування протоколу [9, 10, 16].

5) Якщо рівень помилок, проаналізований в п.4, не перевищує допустимий, то після завершення квантової передачі матриці M_i передаються Бобові звичайним (не квантовим) каналом.

6) Боб обертає отримані матриці.

7) Після чого Боб одержує вихідне повідомлення множенням оберненої матриці на отримане від Аліси квантовим каналом повідомлення: $a_i = M_i^{-1} b_i$.

Навіть якщо Єві вдалося би перехопити один (або більше) із блоків a_i , залишившись не виявленою, то, не знаючи використаних матриць M_i , вона не може встановити вихідні блоки a_i . Для забезпечення високого рівня стійкості, довжина блока r і відповідний розмір матриць M_i ($r \times r$) повинен обиратися так, щоб імовірність успішної атаки Єви s після передачі одного блока a_i була нехтовно малою величиною. Значення параметрів r та s розраховуються згідно роботи [9].

Недоліком описаного методу підсилення секретності є те, що для передачі всього повідомлення генерується та використовується дуже велика кількість випадкових, оборотних над полем Галуа, тритових матриць, що потребує великих часових та ресурсних затрат. Для наглядного розуміння в табл. 1 наведено розмір тритових матриць в залежності від загального розміру повідомлення m та параметру r . З таблиці видно, що для передачі повідомлення розміром m квантовим каналом потрібно використовувати матриці загальним розміром $r \cdot m$ тритів. Крім того, в роботі [9] взагалі не описано як саме генеруються тритові матриці, тому не можливо оцінити їх псевдовипадковість.

Для розуміння загальних розмірів даних в бітах переведемо загальний розмір з трійкової системи числення в двійкову: 100000000 тритів приблизно дорівнюють 20 МБ (якщо переводити кожні 20 тритів у 32 біти). Тому, загальний розмір матриць M_i при $r = 28$

становитиме 560 МБ, які спочатку потрібно згенерувати, виконати множення M_i на a_i , потім передати класичним каналом, а наприкінці обернути та виділити з $b_i - a_i$, що займе занадто багато часу.

Загальний розмір матриць M_i

Таблиця 1

	Загальний розмір повідомлення m в тритах						
	100	1000	10000	100000	1000000	10000000	100000000
$r=4$	400	4000	40000	400000	4000000	40000000	400000000
$r=8$	832	8000	80000	800000	8000000	80000000	800000000
$r=12$	1296	12096	120096	1200096	12000096	120000096	1200000096
$r=16$	1792	16128	160000	1600000	16000000	160000000	1600000000
$r=20$	2000	20000	200000	2000000	20000000	200000000	2000000000
$r=24$	2880	24192	240192	2400192	24000192	240000192	2400000192
$r=28$	3136	28224	280672	2800448	28000560	280000112	2800000336

Пропонується використовувати замість матриць M_i розміром $r \times r$ ключову трійкову послідовність k_i розміром r . Повідомлення b_i буде вираховуватись за формулою $b_i = k_i + a_i$, а a_i – за формулою $a_i = b_i - k_i$, де операції "+" та "-" – означають відповідно операції потритового додавання та віднімання за модулем 3. Ключова трійкова послідовність k_i буде вироблятися за допомогою генератора псевдовипадкових трійкових послідовностей, та 96-тритового ключа K . Після завершення квантової передачі, у випадку відсутності атаки, замість передачі матриць M_i буде передаватись ключ K звичайним каналом зв'язку.

У п.2 даної роботи описано принцип роботи розробленого генератора тритових послідовностей, який пропонується використовувати у цьому методі підсилення секретності для генерування ключової послідовності k_i . При необхідності він може бути змінений на інший.

Загальна схема запропонованого неквантового методу підсилення безпеки пінг-понг протоколу з парами повністю переплутаних кутритів наведена на рис. 1.

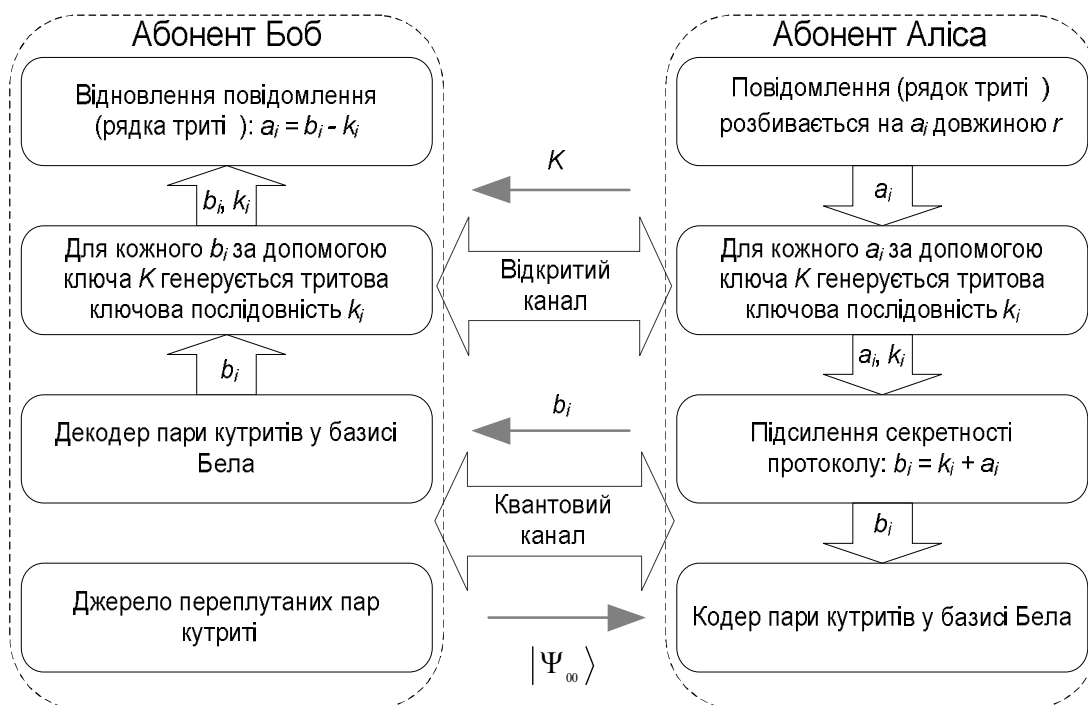


Рис.1. Загальна схема запропонованого методу підсилення безпеки пінг-понг протоколу з парами повністю переплутаних кутритів

Проаналізуємо швидкість роботи існуючого [9] та запропонованого методу підсилення секретності пінг-понг протоколу. Нехай необхідно передати за допомогою пінг-понг протоколу повідомлення довжиною $m = r \cdot l$ – трит, де r – розмір блоку даних, а l – кількість таких блоків. Позначимо як t_1 – час генерування ключових даних. Для існуючого методу підсилення секретності – час генерування оборотних матриць M_i ($i = \overline{1, l}$) розміром $r \times r$, а для запропонованого – час генерування ключової послідовності k_i розміром r . Тоді t_2 – час утворення повідомлення b_i , а t_3 – час передачі повідомлень b_i по квантовому каналі за пінг-понг протоколом. Позначимо як t_4 – час передачі оборотних матриць M_i по класичному каналі для існуючого методу підсилення секретності, а для запропонованого – час передачі 96 тритового ключа K . Час утворення оборотних матриць M_i^{-1} для існуючого методу підсилення або час генерування ключової послідовності k_i розміром r для запропонованого методу підсилення секретності позначимо як t_5 . Тоді t_6 – час відновлення повідомлення a_i . У табл. 2. розраховано t_j ($j = \overline{1, 6}$) в залежності від швидкості генерування тритових послідовностей V_{gen} , швидкостей передачі повідомлень квантовим V_{kv} і класичним каналом V_{kl} та швидкості виконання операцій множення та додавання в полі $GF(3)$ V_x .

Загальний час роботи системи

Таблиця 2

Методи підсилення безпеки пінг-понг протоколу	t_1 , сек	t_2 , сек	t_3 , сек	t_4 , сек	t_5 , сек	t_6 , сек
Існуючий	$\frac{l \cdot r^2}{V_{gen}}$	$\frac{l \cdot (2r^2 - r)}{V_x}$	$\frac{l \cdot r}{V_{kv}}$	$\frac{l \cdot r^2}{V_{kl}}$	$\frac{l \cdot (4r^3 - 4r^2)}{V_x}$	$\frac{l \cdot (2r^2 - r)}{V_x}$
Запропонований	$\frac{l \cdot r}{V_{gen}}$	$\frac{l \cdot r}{V_x}$	$\frac{l \cdot r}{V_{kv}}$	$\frac{96}{V_{kl}}$	$\frac{l \cdot r}{V_{gen}}$	$\frac{l \cdot r}{V_x}$

Швидкість роботи кожного з методів буде визначатися за такою формулою:

$$V = \frac{r \cdot l}{t_1 + t_2 + t_3 + t_4 + t_5 + t_6} \text{ трит/сек.}$$

Оскільки швидкість роботи протоколу залежить від V_{gen} , V_{kv} , V_{kl} , V_x , r та l , то для більш конкретної оцінки швидкостей обох методів підсилення було вирішено провести моделювання роботи протоколу з різними показниками V_{gen} , V_{kv} , V_{kl} , V_x , r та l . Для цього була запропонована модель, яка складається таких етапів:

1. На початку фіксуються базові параметри протоколу: V_{kv} , V_{kv} , V_x , V_{gen} .
2. Обирається не квантовий спосіб підсилення безпеки пінг-понг протоколу.
3. Обирається довжина повідомлення m (10^4 , 10^5 , 10^6) у тритах.
4. Обирається параметр r (4, 12, 20) та розраховується параметр l .
5. Після чого для обраних параметрів V_{gen} , V_{kv} , V_{kl} , V_x , r та l розраховується

загальна швидкість роботи пінг-понг протоколу, яку заносять у таблицю для подальшої обробки.

Результати моделювання наведені в табл. 3, причому для моделювання роботи протоколу обрано 5 різних комбінацій параметрів V_{gen} , V_{kv} , V_{kl} , V_x :

1. $V_{gen} = 10^8$ трит/сек, $V_{kl} = V_x = V_{kv} = 10^6$ трит/сек.
2. $V_x = 10^8$ трит/сек, $V_{kl} = V_{gen} = V_{kv} = 10^6$ трит/сек.
3. $V_{kv} = 10^8$ трит/сек, $V_{kl} = V_x = V_{gen} = 10^6$ трит/сек.
4. $V_{kl} = 10^8$ трит/сек, $V_{gen} = V_x = V_{kv} = 10^6$ трит/сек.
5. $V_{gen} = V_{kl} = V_x = V_{kv} = 10^6$ трит/сек.

Швидкість роботи методів підсилення секретності в трит/сек

Таблиця 3

Комбінація параметрів	Методи підсилення	$m = 10000$ трит			$m = 100000$ трит			$m = 1000000$ трит		
		$r = 4, l = 2500$	$r = 12, l = 834$	$r = 20, l = 500$	$r = 4, l = 25000$	$r = 12, l = 8334$	$r = 20, l = 5000$	$r = 4, l = 250000$	$r = 12, l = 83334$	$r = 20, l = 50000$
1	Існ.	14916	1703	617	14916	1703	617	14916	1703	617
	Запроп.	330076	33076	33076	331020	331020	331020	331115	331115	331115
2	Існ.	103950	32530	17550	103950	32530	17550	103950	32530	17550
	Запроп.	330076	330076	330076	331020	331020	331020	331115	331115	331115
3	Існ.	14263	1672	610	14263	1672	610	14263	1672	610
	Запроп.	248780	248781	248781	249316	249316	249316	249370	249370	249370
4	Існ.	14916	1703	617	14916	1703	617	14916	1703	617
	Запроп.	199996	199996	199996	199999	199999	199999	199999	199999	199999
5	Існ.	14084	1669	610	14084	1669	610	14084	1669	610
	Запроп.	199616	199617	199616	199961	199961	199961	199996	199996	199996

Як видно з табл. 3 при збільшенні параметра r швидкість запропонованого методу підсилення секретності не змінюється, а швидкість методу [9] зменшується у 6-24 рази (в залежності від параметрів $V_{gen}, V_{kv}, V_{kl}, V_x$). При збільшенні параметру l швидкості методів практично не змінюються. Швидкість роботи запропонованого методу у порівнянні з існуючим збільшується у 3 – 536 разів і залежить від параметрів $V_{gen}, V_{kv}, V_{kl}, V_x, r$ та l . З огляду на це, можна зробити висновок, що використання запропонованого методу підсилення секретності, дозволить підвищити швидкість пінг-понг протоколу.

2. Генератор трійкових послідовностей

Принцип роботи розробленого генератора полягає у наступному:

1. На вхід розробленого генератора подається 96 тритовий ключ K , загальний розмір повідомлення m та розмір блоку даних r .
2. Далі розраховується параметр $n \in Z$, який означає, яку кількість разів необхідно використовувати циклову функцію для генерування послідовності розміром $m : n = m/48 + 1$.
3. Ключ K розбивається на 4 частини K_1, K_2, K_3, K_4 по 24 трита.

4. За допомогою циклової функції, формується трійкова послідовність y_i ($i = 1, \dots, n$). На вхід циклової функції подаються 24-тритні допоміжні змінні $A, B, C, D, E, F, Y_1, Y_2$ (початкові значення яких наведені в табл. 4, вагові коефіцієнти тритів зростають зліва на право) та частини ключа K_1, K_2, K_3, K_4 , за допомогою яких формується вихідна тритова послідовність. У цикловій функції для кожного $i = 1, \dots, n$, виконуються такі операції:

4.1. Розраховується нове значення A : 4.1.1. $A = Sbox(A \langle + \rangle K_1) + D$;
4.1.2. $A = Left_{24}(MatrixMult(A), K_4)$.

4.2. Розраховується нове значення B : 4.2.1. $B = Sbox(B + K_2) \langle + \rangle E$;
4.2.2. $B = Right_{24}(MatrixMult(B), K_3)$.

4.3. Розраховується нове значення C : 4.3.1. $C = Sbox((C \langle + \rangle F) + Y_2)$;
4.3.2. $C = Left_{24}(MatrixMult(C), D)$.

4.4. Розраховується нове значення K_1 : 4.4.1. $K_1 = Sbox(K_1 + A) \langle + \rangle E$;
4.4.2. $K_1 = Sbox(MatrixMult(K_1) + Y_1)$.

4.5. Розраховується нове значення K_2 : 4.5.1. $K_2 = Sbox(K_2 \langle + \rangle B) \langle + \rangle F$;
4.5.2. $K_2 = Sbox(MatrixMult(K_2) + Y_2)$.

4.6. Розраховується нове значення Y_1 : 4.6.1. $Y_1 = Sbox(Y_1 \langle + \rangle K_1)$;
4.6.2. $Y_1 = MatrixMult(Left_{24}(Y_1, B))$; 4.6.3. $Y_1 = Sbox(Y_1 + K_2)$.

4.7. Розраховується нове значення D : 4.7.1. $D = Sbox(D \langle + \rangle K_3) + A$;
4.7.2. $D = Left_{24}(MatrixMult(D), K_2)$.

4.8. Розраховується нове значення E : 4.8.1. $E = Sbox(E + K_4) \langle + \rangle B$;
4.8.2. $E = Right_{24}(MatrixMult(E), K_1)$.

4.9. Розраховується нове значення F : 4.9.1. $F = Sbox((F \langle + \rangle C) + Y_1)$;
4.9.2. $F = Left_{24}(MatrixMult(F), A)$.

4.10. Розраховується нове значення K_3 : 4.10.1. $K_3 = Sbox(K_3 + D) \langle + \rangle B$;
4.10.2. $K_3 = Sbox(MatrixMult(K_3) + Y_2)$.

4.11. Розраховується нове значення K_4 : 4.11.1. $K_4 = Sbox(K_4 \langle + \rangle E) \langle + \rangle C$;
4.11.2. $K_4 = Sbox(MatrixMult(K_4) + Y_1)$.

4.12. Розраховується нове значення Y_2 : 4.12.1. $Y_2 = Sbox(Y_2 \langle + \rangle K_3)$;
4.12.2. $Y_2 = MatrixMult(Left_{24}(Y_2, E))$; 4.12.3. $Y_2 = Sbox(Y_2 + K_4)$.

4.13. Розраховується 48-тритне значення y_i за допомогою конкатенації Y_1 та Y_2 :
 $y_i = Y_1 | Y_2$.

5. З утвореної послідовності y_i ($i = 1, \dots, n$) формується послідовність довжиною m .

Отримана послідовність розділяється на l блоків довжиною r , які і утворюють вихідну ключову послідовність тритів k_j ($j=1, \dots, l$).

Початкові значення змінних $A, B, C, D, E, F, Y_1, Y_2$

Таблиця 4

A	012012012012012012021	D	211020112200201220101012
B	122010120022012112021010	E	020211221022101021012100
C	221102101201120100210202	F	100120201101122112002022
Y_1	022102012010211212100102	Y_2	212001020110212021001212

Опишемо операції, які використовуються в запропонованому генераторі:

1. Операція "+" – потритове додавання за модулем 3.
2. Операція "<+" – додавання за модулем 3^{24} .
3. $Right_{24}(X, Y)$ – циклічний зсув вправо числа X на Y разів.
4. $Left_{24}(X, Y)$ – циклічний зсув вліво числа X на Y разів.

5. $Sbox(X)$ – нелінійна заміна кожних шести тритів числа X на відповідне їм значення таблиці підстановок. Для виконання операції число X розбивається на чотири частин по 6 тритів x_i ($i=0, \dots, 3$). Виконання заміни через таблицю підстановок полягає в тому, що значення x_i задає адресу в таблиці підстановки, по якій необхідно взяти нове значення x_i . Запропонований S -блок побудований за допомогою обрахунку зворотного елемента поля $(X)^{-1} \in GF(3^6)$ з подальшим виконанням афінного перетворення над полем $GF(3)$: $S(X) = M \cdot (X)^{-1} + V$, де $X, V \in GF(3^6)$, а M – квадратна не вироджена матриця над полем $GF(3)$ розміром 6×6 (вагові коефіцієнти тритів зростають зверху до низу і зліва на право, тобто елемент $M[0][0]$, який знаходиться в верхньому лівому куті, відповідає молодшому розряду):

$$M = \begin{pmatrix} 1 & 2 & 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 0 & 1 & 1 \\ 1 & 2 & 1 & 2 & 0 & 1 \\ 1 & 0 & 2 & 1 & 2 & 0 \\ 0 & 1 & 0 & 2 & 1 & 2 \\ 2 & 0 & 1 & 1 & 2 & 1 \end{pmatrix}, V = \begin{pmatrix} 0 \\ 2 \\ 2 \\ 1 \\ 0 \\ 2 \end{pmatrix}.$$

Кінцеве поле $GF(3^6)$ фіксується кільцем многочленів з операціями за модулем незвідного многочлена $m(x) = x^6 + x + 2$.

6. $MatrixMult(X)$ – множення трійкової матриці Mat розміром 24×24 трита на X (представлений у вигляді стовпчика) над полем $GF(3)$, дана матриця побудована на основі такого закону: $Mat[i][j] = U[(j + 24 - i) \bmod 24]$, де $i, j = 0, \dots, 23$, а масив $U = \{ 1, 0, 2, 2, 1, 0, 2, 0, 1, 1, 1, 2, 0, 1, 2, 1, 0, 2, 0, 0, 1, 2, 0, 2 \}$.

2. Cai Q.-Y. Improving the capacity of the Bostrom-Felbinger protocol / Q.-Y. Cai, B.-W. Li // *Physical Review A*. — 2004. — V. 69, issue 5. — 054301.
3. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг // — М. : Мир, 2006. — 824 с.
4. Quantum Secure Telecommunication Systems / [Oleksandr Korchenko, Petro Vorobiyenko, Maksym Lutskiy, Yevhen Vasiliu, Sergiy Gnatyuk] // *Telecommunications Networks : Current Status and Future Trends* / edited by Jesus Hamilton Ortiz. — Rijeka, Croatia : InTech, 2012. — P. 211-236.
5. Василю Е.В. Пинг-понг протокол с трех- и четырехкубитными состояниями Гринбергера-Хорна-Цайлингера / Е.В. Василю, Л.Н. Василю // *Труды Одесского политехнического университета*. — 2008. — Вып. 1(29). — С. 171-176.
6. Васіліу С.В. Пінг–понг протокол з повністю переплутаними станами пар та триплетів тривимірних квантових систем / С.В. Васіліу // *Цифрові технології*. — 2009, № 5. — С. 18-26.
7. 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.
8. Wang Ch. 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, issue 4. — 044305.
9. Василю Е.В. Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василю, С.В. Николаенко // *Наукові праці ОНАЗ ім. О.С. Попова*. — 2009, № 1. — С. 83-91.
10. Корченко О.Г. Імітаційна модель пінг-понг протоколу з парами переплутаних кутритів у квантовому каналі з шумом / О.Г. Корченко, С.В. Васіліу, С.О. Гнатюк, В.М. Кінзерявий // *Захист інформації*. — 2010. — №3. — С. 46-56.
11. Василю Е.В. Анализ атаки пассивного перехвата на пинг-понг протокол с полностью перепутанными парами кутритов / Е.В. Василю, Р.С. Мамедов // *Восточноевропейский журнал передовых технологий*. — 2009, № 4/2 (40). — С. 4-11.
12. 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. — V. 341, issue 5-6. — P. 385-389.
13. Cai Q.-Y. The «Ping-pong» protocol can be attacked without eavesdropping / Q.-Y. Cai // *Physical Review Letters*. — 2003. — V. 91, issue 10. — 109801.
14. 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, issue 4. — 042317.
15. Василю Е.В. Стойкость пинг-понг протокола с триплетами Гринбергера-Хорна-Цайлингера к атаке с использованием вспомогательных квантовых систем / Е.В. Василю // *Информатика: Объединенный институт проблем информатики НАН Беларуси*. — 2009, № 1 (21) — С. 117-128.
16. Корченко О.Г. Імітаційне моделювання роботи системи квантового прямого безпечного зв'язку із застосуванням завадостійких кодів для кутритів / О.Г. Корченко, С.В. Васіліу, С.О. Гнатюк, В.М. Кінзерявий // *Захист інформації*. — 2011. — №2 (51). — С. 61-69.

Надійшла: 12.05.2012

Рецензент: д.т.н., проф. Корченко О.Г.