© Vasiliu Ye. Photon number splitting attack on the quantum key distribution protocol with six states // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 148-152.

АТАКА РОЗДІЛЕННЯ ЧИСЛА ФОТОНІВ НА КВАНТОВИЙ ПРОТОКОЛ РОЗПОДІЛЕННЯ КЛЮЧІВ ІЗ ШІСТЬОМА СТАНАМИ

Євген Васіліу

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

ВАСІЛІУ Євген Вікторович, д.т.н.

Рік і місце народження: 1966, Ялта, Крим, Україна.
Освіта: Одеський державний університет імені І.І. Мечникова, 1990.
Посада: директор Навчально-наукового інституту «Радіо, телебачення та інформаційної безпеки» з 2013 року.
Наукові інтереси: квантова криптографія, квантові протоколи розподілення ключів, квантові протоколи прямого безпечного зв'язку, квантові протоколи розділення секрету, квантова стеганографія.
Публікації: понад 100 наукових публікацій, серед яких 4 монографії, понад 60 наукових статей, матеріали конференцій, патенти.
E-mail: vasiliu@ua.fm

Анотація. *У статті на основі методів квантової теорії інформації проаналізовано найбільш потужну атаку розділення числа фотонів – атаку із заміною квантового каналу зі втратами на ідеальний – на протокол квантового розподілення ключів із шістьома станами, який є узагальненням протоколу BB84 на максимально можливе для кубітів число взаємно незміщених базисів – три базиси. Показано, що стійкість протоколу із шістьома станами до атаки розділення числа фотонів вище на декілька процентів, ніж стійкість протоколу BB84, при будь-яких значеннях середнього числа фотонів в імпульсі та коефіцієнту передачі каналу. Також показано, що як і для протоколу BB84, стійкість зменшується як при збільшенні середнього числа фотонів в імпульсі, так і при зменшенні коефіцієнту передачі каналу.*

Ключові слова: *квантова криптографія, квантові протоколи розподілення ключів, протокол BB84, протокол із шістьома станами, атака розділення числа фотонів.*

Вступ

Одними із найважливіших завдань симетричної криптографії із секретним ключем є розроблення та удосконалення процедур розподілення ключа між користувачами (суб'єктами *A* и *B*). На сьогодні для розподілення секретного ключа широко використовують схеми з відкритим ключем, наприклад, схему цифрового конверта або алгоритм Діфі-Хелмана [1], які мають тільки обчислювальну стійкість, тобто використовують обмеженість обчислювальних потужностей зловмисника (суб'єкта *E*). Альтернативою таким схемам розподілення ключів на основі асиметричної криптографії є системи квантового розподілення ключів, стійкість яких ґрунтується на законах квантової фізики й за певних умов досягає теоретико-інформаційної [2]. Основна ідея квантового розподілення ключів полягає в наступному: проводячи маніпуляції над носіями квантової інформації – окремими фотонами, зловмисник з високою ймовірністю вносить збурення в їхні стани, що може бути виявлено легітимними користувачами. Таким чином, зловмисник не може здійснити ефективне перехоплення, залишившись непоміченим.

Для досягнення теоретико-інформаційної стійкості квантових протоколів розподілення ключів (КПРК) необхідні оцінки кількості інформації, що могла потрапити до зловмисника при реалізації протоколу [2]. Як наближену оцінку, як правило, розглядають інформацію, що могла утекти до суб'єкта *E* при виконанні протоколу квантової передачі [2,3]. Відповідна кількісна характеристика - це найбільша із двох величин: взаємна інформація Шеннона між суб'єктами *A* и *E* $I_{AE}(D)$ або між суб'єктами *B* и *E* $I_{BE}(D)$, які є функціями рівня помилок *D*, що вносяться атакою пасивного перехоплення суб'єкта *E*. Для так званих симетричних атак, до якої відноситься й розглянута в цій статті атака розділення числа фотонів, $I_{AE}(D)=I_{BE}(D)$, тому надалі будемо використовувати $I_{AE}(D)$.

Відомо, що для практичної реалізації КПРК з одиночними фотонами потрібні джерела, які випромінюють суворо одиночні фотони [2]. Але такі джерела поки не створені й на практиці використовують слабкі когерентні імпульси, випромінювані лазерними світлодіодами. Ці імпульси можуть містити більше одного фотону. Тоді зловмисник має можливість відвести один фотон з імпульсу, зберегти його до оголошення

легітимними користувачами базисів та виконати вимірювання в правильному базисі. Тим самим після завершення передавання фотонів зловмисник отримує повну інформацію про ключ, не впливаючи при цьому на фотони, що передавались від суб'єкта *A* до суб'єкта *B*, і тим самим атака не буде виявлена. Така атака є простішим варіантом атаки розділення числа фотонів (РЧФ) [2,4,5].

На сьогодні атака РЧФ детально досліджена для відомого протоколу BB84, який використовується в більшості систем квантового розподілення ключів, що пропонуються на ринку рядом компаній. Розроблені також удосконалення BB84 – так звані протоколи зі станами приманки, які більш стійкі до атаки РЧФ [6,7]. Але для протоколу із шістьома станами, якій є узагальненням BB84 на максимально можливе для кубітів число взаємно незміщених базисів (три базиси), атака РЧФ раніше не досліджувалась. Протокол з шістьома станами має меншу інформаційну місткість, ніж BB84, але більшу стійкість до некогерентної атаки. Тому дослідження його стійкості до атаки РЧФ є актуальним завданням, що й є **метою даної роботи**.

Атака розділення числа фотонів на протокол BB84

Розглянемо спочатку атаку РЧФ на протокол BB84, слідуючи роботі [5], з метою подальшого порівняння стійкості до цієї атаки протоколів BB84 і з шістьома станами.

Ймовірність того, що когерентний імпульс лазерного світлодіода містить n фотонів, визначається розподілом Пуассона:

$$p_n = e^{-\mu}\frac{\mu^n}{n!}, \qquad (1)$$

де μ – середнє число фотонів в імпульсі.

У випадку квантового каналу із втратами, імовірність того, що суб'єкт *B* зареєструє в отриманому імпульсі n фотонів визначається формулою:

$$p_{n,\,loss} = e^{-\eta\mu}\frac{(\eta\mu)^n}{n!}, \qquad (2)$$

де η – коефіцієнт передачі каналу.

Ймовірність зареєструвати в імпульсі більше одного фотона дається формулою:

$$p_{n>1,\,loss} = 1 - e^{-\eta\mu}(1+\eta\mu). \qquad (3)$$

Для реалізації атаки РЧФ суб'єкт *E* для кожного імпульсу повинен виконати квантове неруйнівне вимірювання числа фотонів в імпульсі, не впливаючи при цьому на їхню поляризацію. Відзначимо, що таке вимірювання дуже складно виконати, але на даний час це технічно можливо [8]. Якщо суб'єкт *E* виявляє в імпульсі більше одного фотона, він відводить один, дозволяючи іншим безперешкодно пройти до суб'єкта *B*. Потім суб'єкт *E* виконує переплутування перехопленого фотона зі своєю допоміжною квантовою системою (пробою) й очікує оголошення базисів. Виконуючи потім вимірювання стану проби, суб'єкт *E* одержить точне значення переданого біта, не вносячи при цьому ніяких помилок у просіяний ключ.

Якщо ж імпульс несе один фотон, то стратегії суб'єкта *E* можуть бути різними. Наприклад, він може просто пропускати всі однофотонні імпульси, що дозволить йому залишитися невиявленим. Однак при малому середньому числу μ фотонів в імпульсі число багатофотонних імпульсів буде невеликим, і це не дозволить суб'єкту *E* одержати скільки-небудь значну інформацію про ключ. Інша стратегія полягає в тому, що суб'єкт *E* виконує один з варіантів некогерентної атаки [2,9,10] на однофотонні імпульси. У цьому випадку, вочевидь, він вносить помилки в просіяний ключ, кількість яких буде залежати як від типу некогерентної атаки, так і від частки однофотонних імпульсів при передачі.

Ще одна стратегія суб'єкта *E* полягає в блокуванні частини однофотонних імпульсів, у результаті суб'єкт *B* одержує порожній імпульс, тобто його датчик не реєструє фотон. Тим самим суб'єкта *E* збільшує частку багатофотонних імпульсів, що дозволяє йому збільшити інформацію про ключ при тому же рівні внесених у просіяний ключ помилок. Але при цьому атака суб'єкта *E* може бути виявлена іншим способом, тому що суб'єкт *B*, знаючи ймовірність одержати порожній імпульс $p_0 = e^{-\eta\mu}$, може виявити значне перевищення їхньої кількості над очікуваним. Відзначимо, що суб'єкт *B* може також не тільки визначати кількість порожніх імпульсів, але й контролювати всю статистику одержуваних ним сигналів, виконуючи неруйнівне вимірювання числа фотонів в імпульсі. У цьому випадку суб'єкт *E* змушений буде відводити фотон тільки з невеликої частини багатофотонних імпульсів, а інші пропускати, не одержуючи ніякої інформації.

У роботах [4,5,8] розглядається ще одна теоретично можлива атака, яка дозволяє підвищити потужність атаки поділу числа фотонів, – заміна квантового каналу із втратами, який використовують суб'єкти *A* і *B*, на канал без втрат (природно, що вони не знають про заміну). У цьому випадку суб'єкт *E* отримує можливість блокувати деяку частину однофотонних імпульсів так, щоб суб'єкт *B* у результаті одержав приблизно очікуване ним число порожніх імпульсів. Для вихідного каналу з дуже великими втратами така стратегія дозволяє суб'єктові *E* одержати майже повне знання ключа, не вносячи ніяких помилок. Крім того, існує деяка область параметрів η та μ, де атака РЧФ дозволяє суб'єктові *E* зберегти не тільки очікувану суб'єктом *B* частку порожніх імпульсів, але також і всю статистику числа фотонів в імпульсах [4]. Відзначимо, що на практиці для передачі ключа за протоколом BB84 за допомогою слабких когерентних імпульсів використовують джерела фотонів з μ порядку 0,1. Цьому значенню μ відповідає область $\eta < 0{,}176$ [4], тобто суб'єкт *E* може залишитися невиявленим і одержати при цьому повну інформацію про ключ, тільки якщо втрати у вихідному каналі дуже великі. Звідси зокрема випливає, що легітимні користувачі на практиці повинні використовувати квантовий канал обмеженої довжини так, щоб його коефіцієнт передачі залишався досить високим.

Для обчислення взаємної інформації $I_{AE}(D)$, приймемо наступну *стратегію перехоплення інформації*. Суб'єкт *E* блокує деяку частку *k* однофотонних імпульсів, а до інших застосовує оптимальну некогерентну атаку [2,10]. У свою чергу, від кожного багатофотонного імпульсу суб'єкт *E* відводить один фотон і одержує точне значення біта, вимірюючи стан проби після оголошення базисів, як описано вище. Помилки в суб'єкта *B* виникають тільки при атаці на неблоковані однофотонні імпульси, частка яких дорівнює 1–*k*.

Величина *k* вибирається так, щоб число непустих імпульсів, яке очікує суб'єкт *B* для каналу із втратами, дорівнювало числу непустих імпульсів після того, як суб'єкт *E* заміняє канал на ідеальний ($\eta = 1$) і блокує частку однофотонних імпульсів, тобто

$$1 - e^{-\eta\mu} = (1-k)\,p_1 + p_{n>1}, \qquad (4)$$

звідки з використанням (1) одержуємо:

$$k = \frac{1}{\mu}\left(e^{\mu(1-\eta)} - 1\right). \qquad (5)$$

Величина *k*, що визначається виразом (5), дозволяє атакуючому зберегти число непустих імпульсів, яке очікують легітимні користувачі, знаючи заздалегідь коефіцієнт передачі каналу, якій вони використовують. Підкреслимо, що для цього атакуючий повинний замінiть канал із втратами на ідеальний канал без втрат, що технічно може буде дуже складно або взагалі неможливо. Але, як це взагалі прийнято в квантовому криптоаналізі, ми розглядаємо саму сильну атаку, що допускається законами фізики, незважаючи на технічні складності її реалізації.

Відомо, що взаємна інформація між суб'єктами *A* і *B* для всіх квантових протоколів розподілення ключів з кубітами дається виразом [8]:

$$I_{AB}(D) = \frac{1}{2}\phi(1-2D), \qquad (6)$$

де *D* – рівень помилок, а функція ϕ визначається виразом:

$$\phi(x) = (1-x)\log_2(1-x) + (1+x)\log_2(1+x). \qquad (7)$$

У роботі [8] було показано також, що при оптимальній некогерентній атаці на протокол BB84 ймовірність для суб'єкта *E* правильно вгадати стан, що був переданий суб'єктом *A*, а відповідно й правильно вгадати переданий біт, дорівнює

$$P_{correct}^{nc} = 1/2 + \sqrt{D(1-D)}. \qquad (8)$$

При атаці РЧФ ця ймовірність дається виразом [8]:

$$P_{correct}^{pns} = \frac{1 - e^{-\mu}(1+\mu) + (1-k)\mu e^{-\mu}\cdot P_{correct}^{nc}}{1 - e^{-\mu}(1+\mu k)}. \qquad (9)$$

Остаточно, оскільки ймовірність для суб'єкта *E* невірно вгадати стан, переданий суб'єктом *A*, дорівнює $\left(1 - P_{correct}^{pns}\right)$, то $I_{AE}(D)$ для описаної вище РЧФ атаки, за аналогією з (6) для $I_{AB}(D)$, просто дорівнює

$$I_{AE}(D) = \frac{1}{2}\phi\left[1 - 2\left(1 - P_{correct}^{pns}\right)\right], \qquad (10)$$

де $\phi(x)$ означено в (7).

3. Атака розділення числа фотонів на протокол з шістьома станами

Одержимо тепер вираз для взаємної інформації між легітимним користувачем і зловмисником при атаці РЧФ на протокол із шістьома станами. Будемо вважати, що зловмисник при атаці на цей протокол використовує ту ж, описану вище стратегію атаки РЧФ, що і на протокол BB84. Тоді ймовірність для зловмисника правильно вгадати переданий стан буде визначатись тим же виразом (9), в який необхідно підставити ймовірність правильно вгадати переданий стан при некогерентній атаці на протокол із шістьома станами.

Відповідна ймовірність була виведена в роботі [9]:

$$P_{correct}^{nc\,(6st)} = \frac{1}{2}\left(1 + D + \sqrt{D(2-3D)}\right). \qquad (11)$$

Тоді взаємна інформація $I_{AE}(D)$ між суб'єктами *A* и *E* при атаці РЧФ на протокол із шістьома станами буде описуватися тим же виразом (10), де $P_{correct}^{pns\,(6st)}$ визначається наступною формулою:

$$P_{correct}^{pns(6st)} = \frac{1 - e^{-\mu}(1+\mu) + (1-k)\mu e^{-\mu}\left(1/2\left(1 + D + \sqrt{D(2-3D)}\right)\right)}{1 - e^{-\mu}(1+\mu k)}. \qquad (12)$$

На рис. 1 показані криві $I_{AE}(D)$ при атаці РЧФ на протоколи BB84 та з шістьома станами для каналу з невеликими втратами η = 0,9 і при різних значеннях середнього числа μ фотонів в імпульсі. На рис. 2 показані відповідні криві для каналу з набагато більшими втратами η = 0,5 і для тих же значень μ. Як видно з рис. 1, 2, протокол із шістьома станами є більш стійким до РЧФ атаки, ніж протокол BB84, але перевага в стійкості протоколу з шістьома станами невелика. Також видно, що при малих значеннях середнього числа фотонів в імпульсі стійкість обох протоколів мало залежить від кількості втрат в каналі (порівн. криві 2, 3 на рис. 1 і 2). Але при μ = 1 при збільшенні втрат в каналі стійкість обох протоколів суттєво зменшується (порівн. криві 4, 5 на рис. 1 і 2).

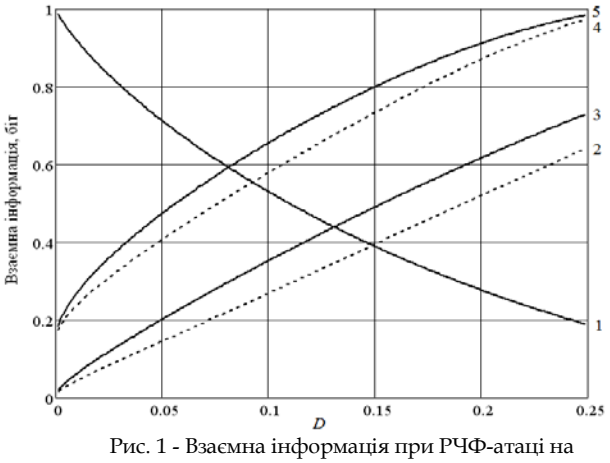

Рис. 1 - Взаємна інформація при РЧФ-атаці на протоколи BB84 і з 6-ма станами при η = 0,9:
1 – взаємна інформація між легітимними користувачами $I_{AB}(D)$;

2 – взаємна інформація $I_{AE}(D)$ при РЧФ-атаці на протокол з 6-ма станами при μ = 0,2;
3 – взаємна інформація $I_{AE}(D)$ при РЧФ-атаці на протокол BB84 при μ = 0,2;
4 – взаємна інформація $I_{AE}(D)$ при РЧФ-атаці на протокол з 6-ма станами при μ = 1;
5 – взаємна інформація $I_{AE}(D)$ при РЧФ-атаці на протокол BB84 при μ = 1.

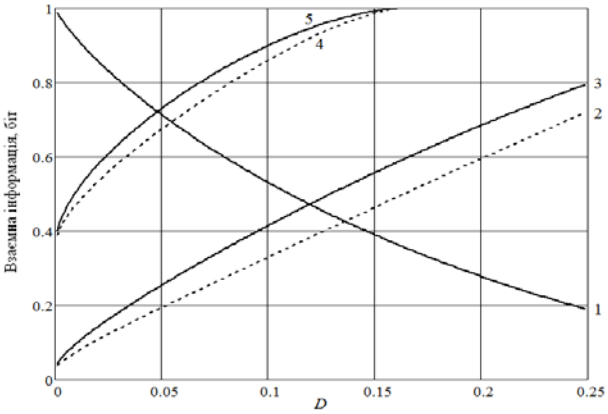

Рис. 2 - Взаємна інформація при РЧФ-атаці на протоколи BB84 і з 6-ма станами при η = 0,5.
Позначення кривих ті ж самі, що на рис. 1.

Згідно з теоремою Цізара – Кернера [12], легітимні користувачі можуть одержати повністю секретний ключ (тобто ключ, інформація зловмисника про який менше заданої, як завгодно малої величини), виконавши так звану процедуру підсилення секретності, якщо взаємна інформація між ними більше за взаємну інформації між легітимним користувачем та зловмисником $I_{AB}(D) > I_{AE}(D)$. Таким чином, величина рівня помилок $D_{\max}$, яка відповідає точці перетину кривих $I_{AB}(D)$ і $I_{AE}(D)$, є гранично допустимим рівнем помилок, при якому легітимні користувачі можуть встановити секретний ключ. Отже максимально допустимий рівень помилок $D_{\max}$ є одним з основних параметрів стійкості будь-якого протоколу квантового розподілення ключів.

У табл. 1 наведені одержані чисельним розв'язуванням рівняння $I_{AB}(D_{\max}) = I_{AE}(D_{\max})$ значення $D_{\max}$ для оптимальної некогерентної та когерентної атак на однофотонні імпульси та для атаки РЧФ при тих же значеннях μ і η, що на рис. 1, 2. Результати, наведені в табл. 1, підтверджують висновки, що зроблено вище у зв'язку з рис. 1, 2.

Таблиця 1

Максимальні рівні помилок $D_{\max}$ для протоколів BB84 та з шістьома станами, при яких легітимні користувачі можуть встановити секретний ключ, при різних атаках на ці протоколи

Вид атаки	Параметри		Максимальний рівень помилок для протоколу BB84, %	Максимальний рівень помилок для протоколу із шістьома станами, %
	μ	η		
Оптимальна некогерентна	–	–	14,6	15,6
Розділення числа фотонів	0,2	0,9	13,1	14,9
	1	0,9	8,1	9,2
	0,2	0,5	12,0	13,6
	1	0,5	4,8	5,5
Когерентна	–	–	11,0	11,8

Таким чином, протокол із шістьома станами є дещо більш стійким – на декілька відсотків, як до атак на однофотонні імпульси (некогерентної та когерентної), що було відомо раніше, так і до атаки РЧФ, що є головним результатом цієї роботи. Але платою за цю невелику додаткову стійкість є більш низька інформаційна місткість протоколу із шістьома станами (1/3 для цього протоколу і 1/2 для BB84), і відповідно більш низька швидкість передавання ключа.

Висновки

У роботі на основі методів квантової теорії інформації проаналізовано найбільш потужну атаку розділення числа фотонів (атаку із заміною квантового каналу із втратами на ідеальний) на відомий протокол квантового розподілення ключів – протокол із шістьома станами, який є узагальненням протоколу BB84 на максимально можливе для кубітів число взаємно незміщених базисів – три базиси. Показано, що стійкість протоколу з шістьома станами до атаки розділення числа фотонів вище на декілька процентів, ніж стійкість протоколу BB84, при будь-яких значеннях параметрів μ і η. Також показано, що як і для протоколу BB84 стійкість зменшується як при збільшенні середнього числа фотонів в імпульсі, так і при зменшенні коефіцієнту передачі каналу.

Протокол із шістьома станами має меншу інформаційну місткість порівняно з протоколом BB84, його невелика перевага в стійкості до декількох атак, на наш погляд, не компенсує зменшення швидкості генерування ключа. Тому з цих двох протоколів для практичного використання ми рекомендуємо протокол BB84, або деякі його модифікації, що стосуються або схеми самого протоколу (протокол SARG04), або його технічної реалізації (протоколи зі станами приманки), і які є більш стійкими до атаки розділення числа фотонів.

Література

[1] Бернет С. Криптография. Официальное руководство RSA Security / С. Бернет, С. Пэйн. – М.: ООО «Бином-Пресс», 2007. – 384 с.

[2] Gisin, N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Reviews of Modern Physics. – 2002. – V. 74, №1. – P. 145-195.

[3] Lutkenhaus, N. Estimates for practical quantum cryptography / N. Lutkenhaus // Physical Review A. – 1999. – V. 59, №5. – P. 3301-3319.

[4] Lutkenhaus, N. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack / N. Lutkenhaus, M. Jahma // New Journal of Physics. – 2002. – V. 4. – P. 44.1-44.9.

[5] Niederberger, A. Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography / A. Niederberger, V. Scarani, N. Gisin // Physical Review A. – 2005. – V. 71, №4. – 042316.

[6] Hwang, W. Y. Quantum key distribution with high loss: Toward global secure communication / W.-Y. Hwang Phys. Rev. Lett. — 2003. — Vol. 91. — 057901.

[7] Liu, Y. Decoy-state quantum key distribution with polarized photons over 200 km / Y. Liu, T.-Y. Chen, J. Wang [та ін.] // Optical Express. – 2010. – V. 18. – P. 8587-8594.

[8] Williamson, M. Eavesdropping on practical quantum cryptography / M. Williamson, V. Vedral // Journal of Modern Optics. – 2003. – V. 50, issue 13. – P. 1989–2011.

[9] Bruss, D. Optimal Eavesdropping in Quantum Cryptography with Six States / D. Bruss // Physical Review Letters. – 1998. – V. 81, issue 14. – P. 3018-3021.

[10] Василиу, Е.В. Сравнительный анализ эффективности и стойкости к некогерентным атакам квантовых протоколов распределения ключей с передачей многомерных квантовых систем / Е.В. Василиу, Р.С. Мамедов // Наукові праці ОНАЗ ім. О.С. Попова. – 2008, № 2. – С. 20-27.

[11] Fuchs, C. Optimal Eavesdropping in Quantum Cryptography. I. Information Bound and Optimal Strategy / Fuchs C., Gisin N., Griffits R. B. [et al.] // Physical Review A. – 1997. – V. 56, issue 2. – P. 1163-1172.

[12] Csiszar I. Broadcast channels with confidential messages / I. Csiszar, J. Korner // IEEE Trans. on Inform. Theory. –1978. – V. IT-24, № 3. – P. 339-348.

УДК 004.056.53+530.145 (045)

Василиу Е.В. Атака разделения числа фотонов на квантовый протокол распределения ключей с шестью состояниями

Аннотация. *В статье на основе методов квантовой теории информации проанализирована наиболее мощная атака разделения числа фотонов – атака с заменой квантового канала с потерями на идеальный – на протокол квантового распределения ключей с шестью состояниями, который является обобщением протокола BB84 на максимально возможное для кубитов число взаимно несмещенных базисов – три базиса. Показано, что стойкость протокола с шестью состояниями к атаке разделения числа фотонов выше на несколько процентов, чем стойкость протокола BB84, при любых значениях среднего числа фотонов в импульсе и коэффициента передачи канала. Также показано, что, как и для протокола BB84, стойкость уменьшается как при увеличении среднего числа фотонов в импульсе, так и при уменьшении коэффициента передачи канала.*

Ключевые слова: *квантовая криптография, квантовые протоколы распределения ключей, протокол BB84, протокол с шестью состояниями, атака разделения числа фотонов.*

Vasiliu Ye. Photon number splitting attack on the quantum key distribution protocol with six states

Abstract. *In the paper on the basis of methods of the quantum information theory the most powerful photon number splitting attack (the attack with replacement of the quantum channel with losses on ideal channel) on the protocol of quantum key distribution with six states is analyzed. It is shown that security of the protocol with six states to photon number splitting attack is higher for some percent, than security of the BB84 protocol, at any values of mean photon number in an impulse and transmission efficiency of the channel. It is also shown that, as well as for the BB84 protocol, security decreases both at increase in mean photon number, and at decrease in transmission efficiency.*

Key words: *quantum cryptography, quantum key distribution protocols, BB84 protocol, protocol with six states, photon number splitting attack.*

Отримано *12 травня 2014 року*, затверджено редколегією *30 травня 2014 року*