© Limar I., Vasiliu Ye., Riabukha O., Zhmurko T. Classification of the attacks on quantum systems for the transfer of confidential data // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 3, p.181-189.

DOI: 10.18372/2225-5036.23.12096

КЛАСИФІКАЦІЯ АТАК НА КВАНТОВІ СИСТЕМИ ПЕРЕДАВАННЯ КОНФІДЕНЦІЙНИХ ДАНИХ

Ігор Лімарь[1], Євген Васіліу[1], Олександр Рябуха[1] , Тетяна Жмурко[2]

[1]Одеська національна академія зв'язку ім. О.С. Попова, Україна
[2]Національний авіаційний університет, Україна

ЛІМАРЬ Ігор Валерійович

Рік і місце народження: 1973, Одеса, Україна.
Освіта: Одеська державна академія холоду, 1995, Одеський національний університет імені І.І. Мечникова, 2010.
Посада: науковий співробітник Одеської національної академії зв'язку ім. О.С. Попова.
Наукові інтереси: квантова теорія інформації, квантова криптографія, квантові протоколи розділення секрету, квантове бітове зобов'язання, квантові явища у біології.
Публікації: 24 наукових публікації, серед яких 12 наукових статей, 12 матеріалів наукових конференцій.
E-mail: quantum.biology@outlook.com

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» Одеської національної академії зв'язку ім. О.С. Попова.
Наукові інтереси: квантова криптографія, квантові протоколи розподілення ключів, квантові протоколи прямого безпечного зв'язку, квантові протоколи. розділення секрету, квантова стеганографія, постквантова криптографія.
Публікації: понад 100 наукових публікацій, серед яких 6 монографій, понад 60 наукових статей, матеріали наукових конференцій, патенти.
E-mail: vasiliu@ua.fm

РЯБУХА Олександр Миколайович, к.т.н.

Рік і місце народження: 1979, с. Берізки-Бершадські, Бершадський район, Вінницька область, Україна.
Освіта: Одеський національна академія зв'язку імені О.С. Попова, 2002.
Посада: викладач кафедри інформаційної безпеки та передачі даних Одеської національної академії зв'язку ім. О.С. Попова.
Наукові інтереси: криптографія, квантова криптографія, випадкові процеси, завадостійке кодування, стеганографія.
Публікації: 16 наукових публікації, серед яких 9 наукових статей, 7 матеріалів наукових конференцій.
E-mail: ryabukha@gmail.com

ЖМУРКО Тетяна Олександрівна, к.т.н.

Рік і місце народження: 1990 рік, м. Вінниця, Україна.
Освіта: Національний авіаційний університет, 2012 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2016 року.
Наукові інтереси: інформаційна безпека, програмний захист інформації, квантова криптографія.
Публікації: більше 50 наукових публікацій, серед яких монографії, наукові статті, тези та матеріали доповідей на конференціях, авторські свідоцтва.
E-mail: t.zhmurko@nau.edu.ua

Анотація. *У даній статті запропоновано розширену класифікацію атак на протоколи та практично реалізовані системи квантової криптографії з урахуванням основних відомих на сьогодні видів нападів. Класифікація поділяє атаки на три класи: пасивні атаки, які можливі при використанні легітимними користувачами однофотонних джерел; пасивні та активні атаки, зумовлені недосконалістю обладнання систем квантового зв'язку (квантовий хакінг); пасивні та активні атаки, зумовлені недосконалістю самих протоколів. Наявність такої класифікації дозволяє виконувати необхідну оцінку стійкості протоколів квантової криптографії та приймати рішення щодо вибору доступних на ринку квантових криптосистем за критерієм їх здатності протистояти існуючим та перспективним засобам квантового криптоаналізу. Детально описано атака Троянського коня та атака віддаленого управління детекторами одиночних фотонів з використанням адаптованого яскравого освітлення. В рамках опису атаки управління детекторами викладено принцип використання фальшивих станів, а також розглянуто різновиди цієї атаки, що залежать від типу використовуваних у детекторах лавинних фотодіодів: з пасивним та активним способами гасіння лавини, із стробіюванням.*

Ключові слова: *квантова криптографія, квантовий розподіл ключів, перехоплення інформації, квантовий канал, квантовий хакінг, детектори одиночних фотонів.*

Вступ

Методи та протоколі квантової криптографії забезпечують високий рівень безпеки, в деяких випадках аж до теоретико-інформаційного. Але вони все ж є уразливими до багатьох атак, як пасивних, так і активних, що обумовлені різними причинами. Ці причини полягають перш за все у деяких вадах окремих протоколів, серед яких є такі, що можуть бути усунені удосконаленням (що часто призводить до ускладнення) протоколів, а є і таки, що усунені бути не можуть, оскільки обумовлені самою фізикою процесів, що відбуваються. Значна кількість атак на різні протоколи квантової криптографії також обумовлена недосконалістю конкретного обладнання, що використовується на сьогодні.

Аналіз існуючих досліджень

Починаючи з ранніх етапів становлення квантової криптографії (початок 90-х років) дослідники проводили моделювання потенційно можливих атак на розроблювальні протоколи й виконували кількісну оцінку витоку інформації із квантових криптосистем. Але більшість таких робіт присвячені доказам стійкості до деяких можливих атак конкретних протоколів та методам захисту від конкретних атак. Як таких класифікацій атак на протоколи квантової криптографії й реальні квантові криптосистеми в науковій літературі небагато. Слід відзначити роботи [1-3], в яких побудовані деякі схеми класифікацій атак на протоколи квантової криптографії, але цей матеріал дещо застарів та практично не враховує атаки на обладнання, яке використовується на даний час у квантових криптосистемах, що випускаються промислово. У недавній роботі [4] зроблено спробу класифікувати виявлені уразливості обладнання сучасних систем квантової криптографії, що можуть привести як до витоку інформації до несанкціонованого користувача (пасивні атаки), так і до зміни інформації несанкціонованим користувачем (активна атака типу «людина посередині»). У роботі [4] такий клас атак названо «квантовим хакінгом».

Динамічний розвиток ринку систем квантового розподілу ключів, що випускають промислово, на протязі останніх 10-ти років і виявлення в цей же період істотних проблем відносно безпеки комерційно доступних криптосистем цього класу, з одного боку, привело до опису значного числа зовсім нових видів атак, а з іншого, змусило переглянути роль раніше проаналізованих загроз. Усвідомлення цього положення висунуло вимогу структуризації всього наявного набору методів несанкціонованого проникнення в системи квантової криптографії, що виникли як у ході їхнього цілеспрямованого пошуку розроблювачами квантових криптографічних протоколів і виробниками комерційно доступного обладнання, так і, якоюсь мірою «стихійно», тобто у результаті виявлення слабких місць уже сконструйованих установок, що серійно випускаються.

З урахуванням викладеного вище, ***метою даної роботи*** є побудування загальної класифікації відомих на теперішній час видів атак на протоколи та практично реалізовані системи квантової криптографії.

Основна частина дослідження

Одними з нових видів атак на квантові криптосистеми є атаки типу «Троянський кінь» та атаки, метою яких є віддалене управління детекторами легітимного користувача, яке здійснює несанкціонований користувач. Ці атаки можна віднести до класу «зумовлені недосконалістю обладнання».

Основні принципи атаки за допомогою «троянських фотонів». Хронологічно як одна з найперших стратегій нападів на системи квантового розподілу ключів з'явився метод несанкціонованого випускання агентом, що підслуховує (Єва), фотонів в шифрувальний пристрій передавальної сторони (Аліса) з подальшим отриманням Євою цих фотонів з уже закодованої в них секретною інформацією. Вперше детально ця атака була описана в роботі [5]. В ході більш пізнього узагальнення атак такого класу [6] вони отримали назву «атак Троянського коня». Незважаючи на те, що такого роду напади відомі протягом значного періоду, в ході якого істотно еволюціонували методи забезпечення безпеки протоколів квантової криптографії, на сьогоднішній день проблема атаки «Троянського коня» є досить актуальною, а сама атака є однією з найефективніших методик несанкціонованого проникнення в системи квантової криптографії. Так, деякі автори констатують, що в силу недооцінки серйозності даної загрози внаслідок, на перший погляд, простого характеру троянської атаки, склалася ілюзія легкості контролю такого нападу в реальних криптосистемах [7]. У той

же час, на думку авторів роботи [7], до теперішнього часу не проведений належним чином кількісний аналіз загроз розглянутого класу. Навпаки, як констатують автори зазначеної роботи, все більше число опублікованих результатів експериментів демонструють несприятливу ситуацію в плані вразливості систем квантового розподілу ключів до атаки «Троянського коня».

Концептуально атака «Троянського коня» на систему квантового розподілу ключів виглядає наступним чином. Єва вводить імпульс яскравого світла в оптичний канал, що з'єднує легітимних користувачів – Алісу і Боба. Цей світловий імпульс, який містить троянські фотони, спрямований в бік легітимного користувача, який здійснює початкову відправку фотонів для розподілу ключів шифрування, тобто – в сторону Аліси. При цьому передбачається, що пристрій Аліси, яке здійснює відправку фотонів все ж певною мірою захищено. Однак цей захист недосконалий і світловий імпульс, досягнувши пристрою розподілу ключів шифрування кодується тією ж інформацією φ (фаза), як і фотон, підготовлений Алісою для запланованої передачі Бобу. Частина троянських фотонів, відбившись від оптичних елементів кодувального пристрою Аліси, повертається через оптоволоконну лінію зв'язку тим самим шляхом, яким спочатку світловий імпульс, сформований Євою, досяг легітимного користувача. На цій ділянці Єва має можливість зареєструвати свої троянські фотони, які вже закодовані Алісою. Таким чином, незважаючи на те, що інформація φ призначалася для секретного розподілу ключів, внаслідок описаних вище дій несанкціонованого користувача безпека системи поставлена під загрозу.

Розглянемо атаку «Троянський кінь» детальніше. Модуль передавача є частиною установки квантового розподілу ключів з модуляцією фази. Єва вводить світло в апаратуру Аліси через те ж оптоволокно, яке служить квантовим каналом між користувачами. Мета зловмисника полягає в тому, щоб досягти фазового модулятора, який кодує секретну інформацію ϕ_A. Для цього лазер Єви випускає імпульси зі середнім числом фотонів μ_{in}, які перебувають у когерентному стані $\left|\sqrt{\mu_{in}}\right\rangle$. Імпульси отримують інформацію про фазову модуляцію ϕ_A і повертаються до Єви як $e^{i\phi_A}\left|\sqrt{\mu_{out}}\right\rangle$, де $\mu_{out} = \gamma\mu_{in}$ зі значенням оптичної ізоляції передавального модуля $\gamma << 1$. Світловий імпульс, отриманий Євою, корелює з фазою φ_A і це ставить під загрозу безпеку системи.

При здійсненні атаки «Троянський кінь» Єва спочатку готує *M* груп фотонів, а потім використовує кожну групу для різних величин фазового модулятора Аліси. Передбачається [7], що кожна група фотонів відповідає одному імпульсу джерела світла Єви і що кожен імпульс приготовлений в чистому когерентному стані. У результаті система характеризується тензорним добутком когерентних станів: $\left|\sqrt{\mu_1}\right\rangle \otimes \left|\sqrt{\mu_2}\right\rangle \otimes ... \oplus \left|\sqrt{\mu_M}\right\rangle$, де μ_i (i=1,…,M) – середнє число фотонів i-го когерентного стану.

Кожен з троянських імпульсів Єви відправляється в модуль передачі, щоб зондувати різні величини фази φ_A фазового модулятора Аліси. Після цього імпульси отримує Єва, для них середнє число фотонів становить $\mu_{out} = \gamma\mu_{in}$.

Саме та обставина, що більшість схем квантового розподілу ключів ґрунтуються на передачі інформації через оптоволоконні лінії зв'язку, робить проблему досить значимою. Дійсно, ідеальні компоненти оптичної системи дозволили б передати всі світлові імпульси в кінцеву точку без втрат, але реальні канали не дозволяють цього зробити. В процесі передачі по каналу, а також через оптичні компоненти системи, певна частина світла буде відбита або розсіяна. Більш конкретно, зміна показника заломлення під час поширення світла викликає відбиття Френеля, в той час як коливання щільності матеріалу оптоволокну викликає релеєвське розсіювання або розсіювання Мандельштама-Брілюена. Обсяг відбиття і розсіювання може залежати від довжини хвилі і інтенсивності вхідного світла. Яскравий імпульс, запущений з квантового каналу несанкціонованим користувачем в підсистему квантового розподілу ключів, в конкретному випадку, в передавальний модуль Аліси, зустрічається з багаторазовим різноманітним відбиттям і розсіюванням. Очевидно, що потік відбитих імпульсів поширюється з пристрою Аліси в квантовий канал. Ретельно аналізуючи це відбите світло, Єва може отримати інформацію про властивості і функціонуванні компонентів передавального пристрою Аліси. Такий аналіз може бути здійснений, наприклад, шляхом використання методів так званого розрізнення станів [8]. В роботі [7] зазначено, що використовуючи рефлектометрію оптичної частотної області, з шифратора, що включає в себе компоненти на основі $LiNbO_3$, принципово можливо отримати інформацію про фазу φ. Більш того, у роботі [9] вказано, що значення фази, що задається шифратором легітимної сторони, може бути визначено зловмисником з 90% ймовірністю успіху шляхом використання всього лише 3-х троянських фотонів.

Недавні успішні атаки на системи квантового розподілу ключів, що випускає промисловість, привернули значну увагу [10]. У лабораторних умовах вдалося отримати інформацію при роботі таких системам, як Clavis2 (виробництво ID Quantique) і Cygnus (виробництво SeQureNet).

Атака віддаленого управління детекторами одиночних фотонів з використанням адаптованого яскравого освітлення. Поряд з атакою «Троянський кінь» іншої значущої загрозою системам квантового розподілу ключів, в тому числі тим, що випускаються промислово, є виділені в окремий клас атаки, що отримали назву «віддалене управління детекторами одиночних фотонів з використанням адаптованого яскравого освітлення». В силу характерної стратегії, використовуваної при здійсненні атак такого типу, ми вважаємо, що цей вид атак слід також відносити до вже існуючого і добре відомого класу атак «людина посередині». Для стислості ми також далі будемо називати такий напад «атака засліплення», ґрунтуючись на основному способі передачі

легітимній стороні неправдивої інформації – управлінні зловмисником приймальними детекторами шляхом направлення через комунікаційний канал інтенсивних імпульсів світла.

Суть атаки «людина посередині» в оптоволоконному каналі полягає у врізанні в оптоволоконний канал між легітимними користувачами та установці там обладнання зловмисника Єви. Таке обладнання призначено для перехоплення інформації, що надсилається відправником Алісою, і, по можливості, криптоанализу цих даних. Крім того, далі зловмисник може сформувати підроблений, потрібний йому набір даних і відправити його легітимному одержувачу Бобу. Таким чином Єва здійснює перехоплення з подальшим криптоаналізом і/або маніпулюванням інформацією, якою обмінюються легітимні користувачі, з перекручуванням її потрібним їй чином.

Атаки з використанням «фальшивих станів». Аналогічний підхід був запропонований для атаки на системи квантового розподілу ключів [11]. У літературі він отримав назву «атаки з використанням фальшивих станів».

Спочатку атака на квантову криптосистему з використанням фальшивих станів позиціонувалася як різновид атаки «людина посередині», в ході якої Єва не намагається відновити вихідні стани, але генерує натомість світлові імпульси, які одержуються легітимними сторонами, не підвищуючи в комунікаційному каналі рівня помилок, що вказувало б легітимним сторонам на атаку.

Відомо, що атака типу «людина посередині» на квантові протоколи розподілу ключів, яку називають ще непрозорою атакою або атакою «перехоплення – повторної посилки фотонів» [1,2, 12, 13], приречена на невдачу, якщо Єва буде просто, без будь-яких додаткових заходів, направляти Бобу такі ж квантові стани, які виявлені нею при перехопленні та вимірюванні станів, відправлених Алісою. Так, для протоколу BB84 така стратегія приводить до виникнення 25% помилок при вимірюванні станів Бобом, а для протоколу з 6-ма станами - 33% помилок. Однак можна було б спробувати ввести в оману легітимні сторони, використовуючи недоліки їх обладнання. Завдання атакуючого полягає в тому, щоб легітимні користувачі вважали, що вони вимірюють початкові квантові стани, в той час як насправді вони б виявляли світлові імпульси, що згенеровані Євою. Ці світлові імпульси називають «фальшивими станами».

У всіх розроблених атаках типу «засліплення» атака Єви успішна тоді, коли вона змушує Боба вимірювати фотони не у випадковим чином обраних базисах, а у базисах, що обрані й диктуються Євою. Єва здійснює підключення до ділянки оптоволокну, що з'єднує апаратуру Аліси і Боба. Потім Єва, фіксуючи свої вимірювальні базиси, накопичує значення для кожного квантового стану, який вона виявляє. Після цього вона відправляє фальшивий стан Бобу для кожного виявленого стану, забезпечуючи вибір Бобом базису вимірювання. Боб завжди виявляє стан у базисі, обраному Євою. Присутність Єви залишається прихованою, оскільки після кроку просіювання ключа всі біти в сирому ключі були виміряні нею в належному базисі, і подальша перевірка Алісою і Бобом не призводить до збільшення квантового рівня бітових помилок.

Питанням залишалося, як саме змусити Боба вважати, що він виконав вимірювання в тому чи іншому базисі. Технічне рішення було знайдено шляхом використання деяких особливостей детекторів систем квантового розподілу ключів. У значної частини квантових криптосистем, що промислово випускаються на даний час, для реєстрації фотонів використовуються лавинні фотодіоди – твердотільні аналоги фотоелектронних помножувачів.

Нижче розглянуті основні методи віддаленого управління трьома видами детекторів одиночних фотонів, що дозволяють здійснити атаку «фальшивих станів».

Атака віддаленого управління детекторами одиночних фотонів, що використовують лавинні фотодіоди з пасивним заглушенням. Розглянемо метод впливу зловмисника на детектори одиночних фотонів, що використовують такий вид лавинних фотодіодів, які ґрунтуються на пасивному заглушенні [14]. Так як пасивне заглушення найбільше підходить для кремнієвих фотодіодів, квантові криптосистеми, що мають їх в своїй конструкції, здійснюють оптичну передачу в діапазоні хвиль 500–900 нм. Промислові квантові криптосистеми, що працюють на більш довгих хвилях, використовують інший тип детекторів одиночних фотонів, які називаються детекторами із стробіюванням.

Пасивним заглушенням називають процес заглушення лавинного струму, що виникає в фотодіоді при реєстрації фотона. Після заглушення лавинного струму стан приладу відновлюється і детектор готовий до реєстрації наступного фотона.

Детектори одиночних фотонів на основі лавинних фотодіодів з пасивним заглушенням можуть бути тимчасово засліплені відносно яскравим світлом інтенсивності менше ніж 1 нВт. Режим яскравого світла дуже добре підходить для атаки на систему квантового розподілу ключів, що містить такі детектори. У цьому режимі всі детектори в приймальнику Боба однаково засліплені безперервним освітленням, що приходить від зловмисника Єви. Коли Єві потрібен певний детектор Боба, щоб зробити «клацання» (реєстрацію фотона), вона змінює поляризацію світла (або інші параметри, які використовуються, щоб закодувати квантові стани) таким чином, що цільовий детектор припиняє отримувати світло, в той час як інший детектор (детектори) продовжує освітлюватися. Єва повертає цільовому детектору здатність реєструвати одиничні фотони і, коли Єва змінює поляризацію знову, відбувається одне (окреме) «клацання». Таким чином Єва має повний контроль над Бобом і може успішно виконати атаку «людина посередині».

Розглянемо тепер механізм засліплення. Кремнієвий лавинний фотодіод зміщений на 6–10. В вище його напруги пробою джерелом високої напруги через резистор. Схема працює завдяки присутності двох паразитних ємкостей близько 1 пФ кожна. Коли немає ніякого струму, що тече через фотодіод, обидві ємності заряджені напругою зміщення.

Під час лавини вони швидко розряджаються через фотодіод, виробляючи короткий імпульс струму. Розрядний струм однієї ємності перетворений в напругу на резисторах, і ця напруга виявляється. Короткий вихідний імпульс компаратора розширено приблизно до 10 мкс моностабільним мультивібратором. Імпульс струму, вироблений під час лавини, має ширину близько 1 нс. Коли напруга в фотодіоді знижується досить близько до напруги пробою, лавина заглушується. Ємності згодом повільно перезаряджаються через резистор зміщення з постійним часом перезарядки близько 1 мкс.

Поки ємності не перезаряджені до певної порогової напруги, що в даному випадку займає приблизно 1 мкс, у детектора немає можливості виявляти одиничні фотони. Після того, як закінчується 1 мкс, детектор буде поступово збільшувати свою квантову ефективність, в той час як напруга продовжує підвищуватися. Однак фотон, який прибуває протягом першої мікросекунди, може все ще викликати лавину з меншим піковим струмом, не досягнувши порога компаратора. Такі маленькі лавини скидають напругу і можуть зберегти детектор засліпленим невизначено довго, якщо вони відбуваються досить часто. Це – основний механізм засліплення в детекторах з пасивним заглушенням.

Тепер розглянемо, як Єва може управляти детектором одиночних фотонів. Коли вхідне освітлення залишається в необхідному для цілей Єви діапазоні, детектор знаходиться у засліпленому стані. Однак, після того, як світло вимкнене, у ємності в детекторі є час, щоб перезарядитись, і детектор знову набуває здатності реєструвати одиничні фотони. Коли світло переключене 2 мкс по тому, детектор здійснює єдину реєстрацію фотона з ймовірністю, більше ніж 0,8 (або ніякого «клацання» в іншій частині випадків), і після цього стає засліпленим знову.

Використовуючи метод управління детектором, описаний вище, Єва може виконати атаку на систему квантового розподілу ключів. У квантовій криптосистемі Боб має кілька детекторів і / або робить вибір вимірювального базису. Єві потрібен спосіб викликати «клацання» в певному детекторі в певному обраному нею базисі, не викликаючи «клацання» в іншому детекторі (детекторах) або в іншому базисі. В роботі [14] описаний приклад атаки на систему з поляризаційним кодуванням і активним вибором базису Бобом, який використовує протокол BB84. У такій системі вхідне світло в установці Боба спочатку проходить через модулятор, який, за випадковим вибором Боба, або нічого не робить, або повертає вхідний стан поляризації на 45° за годинниковою стрілкою, таким чином встановлюючи один з двох можливих вимірювальних базисів. Після модулятора світло розділяється в поляризаційному роздільнику променю (PBS). Вертикальна складова поляризації йде в детектор D0, а горизонтальна складова йде в детектор D1.

Єва виконує атаку «людина посередині» з направленням фальшивих станів проти цієї системи. У нападі фальшивих станів вона повністю блокує світло між Алісою і Бобом. Потім Єва використовує копію установки Боба (Bob'), щоб виміряти квантовий стан Аліси, випадково вибираючи вимірювальний базис. Після цього Єва змушує Боба зробити «клацання» саме в тому базисі, який вибрала вона і, з отриманням того ж результату вимірювання, який вона щойно отримала.

Підкреслимо, що в цьому полягає кардинальна відмінність простий атаки «людина посередині» (непрозорої атаки) від атаки з використання фальшивих станів: в останньому випадку базис і результат вимірювання Боба завжди такі ж, як і у Єви. Таким чином атака не викликає помилки в просіяному ключі і підслуховування не виявляється.

Конкретно розглянемо ситуацію, коли Єва виявила квантовий стан Аліси в базисі 0° і зареєструвала «клацання» в своєму детекторі D0. Вона тепер повинна сформувати і відправити Бобу фальшивий стан. Фальшивий стан має викликати клацання в детекторі Боба D0 у випадку, коли Боб вибирає базис 0°, і не повинен викликати клацання ні в одному з детекторів Боба у випадку, якщо Боб вибирає базис 45° (базис, відмінний від того, який використовувала Єва). Фальшивий стан, який досягає цієї мети, складається з некогерентної суміші вертикальних і горизонтальних компонент поляризації з певною схемою інтенсивності для кожного компонента поляризації.

Розглянемо, що відбувається з фальшивим станом в пристрої Боба. Якщо Боб вибирає базис 0°, то його модулятор нічого не робить, і дві компоненти поляризації фальшивого стану розділені кожна до її власного детектору. Схема інтенсивності вертикальної компоненти поляризації викликає «клацання» в D0 з ймовірністю, більше, ніж 0,8 (для ширини провалу 2 мкс). Схема інтенсивності горизонтальної компоненти поляризації зберігає D1 засліпленим. Якщо Боб, проте, вибирає базис 45°, кожна компонента поляризації повернута на 45° і розділена однаково в поляризаційному роздільнику променю. Половини двох компонент поляризації підсумовуються в кожному детекторі, що приводить до ідентичних схем інтенсивності, які зберігають обидва детектора засліпленими.

Три інших можливих результати вимірювань в базисах Єви розглядаються аналогічно. Таким чином атака фальшивого стану успішно виконується.

Атака віддаленого управління детекторами одиночних фотонів із стробіюванням. Наступним видом пристроїв, які може бути необхідним контролювати несанкціонованому користувачу при атаці з використанням фальшивих станів є детектори зі стробіюванням (gated detectors) [15].

Єва може засліпити детектори зі стробіюванням в системах квантового розподілу ключів, використовуючи яскраве освітлення, таким чином перетворивши їх в класичні, лінійні детектори. Детекторами тоді повністю керують класичні лазерні імпульси, накладені на інтенсивне постійне освітлення (електромагнітну хвилю з постійною амплітудою і частотою). Детектори точно вимірюють те, що диктує Єва, з відповідністю вимірювальних базисів. Боб виявляє саме результат вимірювання, відправлений Євою, тоді як у разі невідповідності вимірювальних базисів Боб взагалі нічого не виявляє. Єва може здійснити успішну атаку на криптосистему, отримавши

точну копію сирого ключа, не залишаючи при цьому слідів її присутності.

Щоб виявити окремі фотони, лавинні фотодіоди працюють в режимі Гейгера. Однак лавинні фотодіоди перебувають частину часу у стані зміщення під напругою пробою в лінійному режимі. У цей період детектор залишається чутливим до яскравого світла. Якщо у Єви є доступ до лавинних фотодіодів в лінійному режимі, вона може прослуховувати систему квантового розподілу ключів шляхом атаки «людина посередині» з направленням фальшивих станів. Єва використовує копію обладнання Боба, щоб виміряти стани від Аліси у випадковому базисі.

Після цього вона посилає свої результати вимірювання, але замість того, щоб відправити імпульси на рівні окремого фотона, вона відправляє яскраві запускові (triggered) імпульси з піковою потужністю трохи вище порога чутливості фотодіода. У Боба буде подія виявлення, тільки якщо його активний вибір базису співпадає з вибором базису Євою, інакше ніяких «клацань» детектора не відбудеться. Це змушує половину бітів бути втраченою, але на практиці це не проблема, тому що коефіцієнт пропускання від виходу Аліси до детектора Боба набагато нижче, ніж 1/2. Також у лавинних фотодіодів Боба мало коли спостерігається квантова ефективність більш ніж 50%, але яскраві запускові імпульси завжди викликають «клацання». Для Боба, що використовує пасивний вибір базису, Єва запускає пікову потужність трохи вище дворазового порога чутливості фотодіода, оскільки половина потужності йде на пов'язані базисні детектори. Тоді детектор Боба завжди «клацає».

Після обміну з метою отримання сирого ключа у Боба і Єви є ідентичні результати вимірювання та вибір базисів. Оскільки Аліса і Боб зв'язуються по відкритому каналу під час просіювання, корекції помилок і підсилення безпеки, Єва просто слухає цю класичну комунікацію і застосовує ті ж операції, які виконує Боб, щоб отримати ідентичний фінальний ключ.

Якщо здійснювати підслуховування, використовуючи тільки запускові імпульси, то матиме місце занадто високий квантовий рівень бітових помилок. Щоб уникнути цього, детектори Боба засліплюють. Детектори тоді нечутливі до одиночних фотонів. Таким чином, лавинний фотодіод ніколи не працює в режимі Гейгера, а скоріше є класичним фотодіодом.

Використовуючи копію обладнання Боба, щоб виявити сигнали Аліси, Єва посилає яскраві запускові імпульси замість окремих фотонів. Коли детектори будуть засліпленими, Боб виявить тільки яскраві запускові імпульси, якщо він буде використовувати той же базис, що і Єва. Інакше його детектори нічого не зареєструють. Отже, Єва отримує повну копію сирого ключа, не викликаючи додаткового квантового рівня бітових помилок. І детектори з пасивним заглушенням [14], і детектори зі стробіюванням, що використовуються у двох комерційно доступних систем квантового розподілу ключів [15], є уразливими для засліплення.

Атака віддаленого управління детекторами одиночних фотонів з активним заглушенням. Поряд з детекторами на основі лавинних фотодіодів з пасивним заглушенням і детекторів зі стробіюванням, в системах квантового розподілу ключів використовуються детектори з активним заглушенням лавини [16].

Детектори з активним заглушенням зазвичай використовуються в системах квантового розподілу ключів у видимому і близькому до інфрачервоного діапазонах. В роботі [16] показано, що ці детектори можуть також віддалено управлятися Євою.

У випадку двох недавно зламаних комерційних системах квантового розподілу ключів, що працюють на телекомунікаційних довжинах хвиль [15], перехід від режиму Гейгера до класичного режиму фотодіода був досягнутий за допомогою яскравого освітлення електромагнітною хвилею постійної інтенсивності. Таким способом досягалося зменшення напруги зсуву лавинного фотодіода нижче значення пробою.

Детектори з активним заглушенням можуть використовуватися після перетворення фотонів довжини хвилі у видимій області світла (тієї області, яка зазвичай використовується в оптоволоконних телекомунікаційних системах) в довжини хвиль, що наближаються до червоної межі видимого світла. У ряді випадків на цих ділянках довжин хвиль апаратура, що промислово випускається, має кращі характеристики.

В роботі [16] описано, як був досягнутий перехід до класичного режиму фотодіода не шляхом застосування випромінювання з постійною інтенсивністю (що ефективно в разі детекторів зі стробіюванням), але шляхом використання замість цього яскравого імпульсного освітлення на рівні менше ніж 10 мВт на тактовій частоті ≥70 кГц. Між імпульсами детектор був «сліпим» по відношенню до одиночних фотонів і не виробляв побічних відліків або залишкових імпульсів. Однак детектор «клацав» під керуванням Єви, якщо застосовувався класичний світловий імпульс потужністю більше порогової.

Підводячи підсумок огляду методів нападу на системи квантового розподілу ключів шляхом «засліплення» детекторів, можна констатувати наступне. Єва може використовувати так звану атаку «фальшивих станів» і здійснювати атаку «людина посередині», з тим щоб дізнатися про секретний ключ.

Приклад ефективного здійснення атаки «людина посередині» стосовно квантової криптосистеми – атака засліплення, яка використовує фізику детекторів одиночних фотонів: Єва відправляє імпульси яскравого світла, щоб перевести детектори з режиму Гейгера в лінійний режим, в якому детектори поводяться як класичні детектори. Потім через адаптовані яскраві імпульси (які називають також запусковими імпульсами), Єва може керувати функціями відгуку детекторів. Так, наприклад, вона може забезпечити таку конфігурацію фальшивих станів, що «клацання» у відповідних детекторах Боба відбуваються, тільки якщо є однаковими відповідні вимірювальні базиси Єви і Боба, і, як наслідок, відсутнє підвищення рівня помилок. Тобто мета полягає в тому,

щоб перетворити відповідь пристрою вимірювання Боба в той, який залежить від стратегії атаки Єви. З точки зору доказів безпеки, осліплення ламає стосовно практично реалізованих апаратних засобів фундаментальні уявлення про те, що ймовірність виявлення того чи іншого стану кубіта незалежна від вимірювального базису. Мається на увазі, що дані, «отримані» Бобом в результаті здійснення «квантових вимірювань» насправді згенеровані відповідно до даних, визначених Євою; і, тому Єва може дізнатися все про секретний ключі, не підвищуючи рівень помилок. Дійсно ідеальний метод управління відповідає випадку, коли функції відгуку детекторів Боба детерміновані і залежать тільки від імпульсів, що запускає Єва, і вибору вимірювального базису Бобом.

Квантовий хакінг (атаки, зумовлені недосконалістю обладнання) та класифікація атак на квантові криптосистеми. До квантового хакінгу в [4] відносять сім основних видів атак. Найбільш значимим з них є атака «фальшивих станів», яка детально описана вище. Другим видом атак є ушкодження лазерним променем певних елементів установки легітимного користувача. У ряді випадків легітимний користувач не виявляє такі ушкодження, які при цьому дозволяють зловмисникові потрібним йому чином управляти встаткуванням легітимного користувача.

Наступна атака використовує уразливість невідповідності ефективності виявлення фотонів. Оскільки на практиці метрологічна ідентичність двох детекторів може бути порушена, наприклад, може спостерігатися різниця в довжині шляху, подоланому фотоном при досягненні різних детекторів, зловмисник може використати цю обставину у своїх інтересах.

Удосконаленням атаки невідповідності ефективності виявлення є атаки часового зсуву. У цьому випадку зловмисник впливає на час досягнення фотонами прийомного пристрою легітимного користувача. Атака часового зсуву може бути здійснена більш успішно при використанні уразливості калібрування – наступного виду атак. У цьому випадку зловмисник, використовуючи уразливості в комплексі встаткування легітимного користувача, потрібним йому способом підбирає часові інтервали зсуву для того, щоб мінімізувати ймовірність виявлення атаки.

Успішне здійснення нападу може бути реалізовано не тільки шляхом використання уразливості детекторів. Так, наприклад, атаки залежності від довжини хвилі ефективності подільника пучка використовують недосконалість подільника пучка фотонів у плані залежності ефективності його роботи від частоти використовуваного світлового імпульсу.

Останнім видом атак «квантового хакінгу», відповідно до класифікації [4], є атака Троянського коня, також детально розглянута вище. Ми будемо називати «квантовий хакінг» атаками, зумовленими недосконалістю обладнання легітимних користувачів, у відповідності до вже усталеної у вітчизняний науковій літературі термінології.

Крім атак, розглянутих у [4], до квантового хакінгу ми вважаємо за доцільне віднести ще два виду.

До першого виду ми відносимо атаки розділення пучка та розділення числа фотонів. Принцип здійснення атак цього виду полягає у наступному. Оскільки приготування однофотонних станів є дуже складною технічною задачею на практиці при реалізації протоколів квантової криптографії, використовують ослаблені лазерні імпульси. Ці імпульси можуть бути добре представлені когерентними станами із середнім числом фотонів менше за одиницю. При цьому, однак, у деяких імпульсах з'являється більш ніж один фотон. Таким чином, зловмисник має можливість розділити сигнал та отримати певну інформацію, не підвищуючи суттєво рівень помилок у каналі [17, 18]. Особливо ефективно цей метод реалізується при здійсненні квантового вимірювання, такого, що не здійснює збурення (неруйнівного квантового вимірювання) [19].

Другим видом атак, який ми додатково включаємо до квантового хакінгу, є атаки, що ґрунтуються на заміні квантового каналу на канал з меншим рівнем завад та втрат. Основний метод перевірки відсутності прослуховування, що використовується у квантовій криптографії – неприйнятне збільшення рівня помилок у легітимних користувачів [20]. Однак зловмисник може замінити первісно організований легітимними користувачами канал з певним рівнем завад та втрат на канал з меншим рівнем завад. Легітимні користувачі при цьому, орієнтуючись на первісно заданий рівень припустимих помилок, не відрізняють помилки, викликані атакою зловмисника, від помилок, викликаних природними завадами. Тобто припустимий рівень помилок при використанні первісного каналу приймається легітимними користувачами вищім, ніж де-факто виникаючий внаслідок природних завад рівень помилок у каналі, змонтованим зловмисником. Останній при цьому може використати виникаючу різницю між уявним та фактичним рівнем помилок для несанкціонованого втручання. Для зловмисника в той же час важливо постійно підтримувати рівень виникаючих помилок на рівні не нижчому того, про який первісно домовилися користувачі. Це необхідно робити, навіть якщо зловмисник певний час не виконує прослуховування. У противному випадку легітимними користувачами на основі наявності неприродньо низького рівня помилок буде здійснено висновок про втручання в каналі зв'язку.

Таким чином, з урахуванням описаних нами атак розділення пучка та числа фотонів і атаки з заміною каналу на кращий до квантового хакінгу ми відносимо наступні атаки: *атаки фальшивих станів; пошкодження лазерним випромінюванням елементів криптосистеми; атака з використанням уразливості невідповідності виявлення; атака зсуву часу; атака з використанням вразливості калібрування; атаки залежності від довжини хвилі; атаки Троянського коня; атаки поділу пучка та поділу числа фотонів; атаки заміни квантового каналу на канал з меншим рівнем завад та втрат.*

На рисунку 1 показана розроблена нами розширена класифікація атак на квантові системи передачі конфіденційних даних, яка враховує основні відомі на даний час види атак. Атаки квантового хакінгу перелічено вище і не деталізовано на рис. 1.

Слід зробити зауваження щодо атак типу «людина посередині». Ми розташували їх в нашій класифікації у класі атак, зумовлених недосконалістю протоколів. Маються на увазі атаки, коли несанкціонований користувач має повну копію обладнання легітимних користувачів і, таким чином, повністю контролює як квантовий, так і класичний канали зв'язку між легітимними користувачами. Але, одна з можливих технічних реалізацій такої атаки – це атака віддаленого управління детекторами одиночних фотонів (атака фальшивих станів), яку ми розташували у класі атак, зумовлених недосконалістю обладнання. Цей зв'язок відображений на схемі (див. рис. 1).

Рис. 1. Розширена класифікація атак на квантові системи передачі конфіденційних даних

Висновки

У роботі виконано детальний аналіз атак типу «Троянський кінь» та атак віддаленого управління детекторами одиночних фотонів легітимного користувача. «Троянський кінь» відноситься до класу атак пасивного підслуховування і при певних умовах дозволяє несанкціонованому користувачу отримати правильне значення біта з 90%-ю ймовірністю. Атаки віддаленого управління детекторами одиночних фотонів для різних видів детекторів (з пасивним та активним заглушенням лавини, зі стробіюванням) дозволяють несанкціонованому користувачеві повністю управляти детекторами приймаючої сторони і можуть бути віднесені до класу атак «людина посередині». Представлено розширену класифікацію атак на квантові системи передачі конфіденційних даних, яка враховує основні відомі на даний час види атак та поділяє їх на три класи:

– пасивні атаки, можливі при використанні легітимними користувачами однофотонних джерел;

– пасивні та активні атаки, зумовлені недосконалістю обладнання систем квантового зв'язку (квантовий хакінг);

– пасивні та активні атаки, зумовлені недосконалістю самих протоколів.

На думку авторів, наявність запропонованої класифікації дозволить здійснювати оцінку стійкості протоколів квантової криптографії та приймати рішення щодо вибору комерційно доступних квантових криптосистем по критерію їх здатності протистояти існуючим та перспективних засобам квантового криптоаналізу.

Література

[1] O. Korchenko, Ye. Vasiliu, S. Gnatyuk, «Modern quantum technologies of information security against cyber – terrorist attacks», *Aviation: Research Journal of Vilnius Gediminas Technical University*, V. 14, No 2, p. 58–69, 2010.

[2] О. Корченко, Є. Васіліу, С. Гнатюк, В. Кінзерявий, «Атаки в квантових системах захисту інформації», *Вісник інженерної академії України*, № 2, с. 109–115, 2010.

[3] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, «The security of practical quantum key distribution», *Reviews of Modern Physics*. Vol. 81, Issue 3, p. 1301, 2009.

[4] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, G. Leuchs, «Attacks on practical quantum key distribution systems (and how to prevent them)», *Contemporary Physics*, Vol. 57, Issue 3, p. 366–387, 2016.

[5] A. Vakhitov, V. Makarov, D. Hjelme, «Large Pulse Attack as a Method of Conventional Optical Eavesdropping *in Quantum Cryptography*», Journal of Modern Optics, Vol. 48, Issue 13, p. 2023, 2001.

[6] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, «Trojan-Horse Attacks on Quantum-Key-Distribution Systems», *Physical Review A*, Vol. 73, Issue 2, 2006.

[7] M. Lucamarini, I. Choi, M.B. Ward, J.F. Dynes, Z.L. Yuan, and A.J. Shields, «Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution», *Physical Review X*., Vol. 5, Issue 3, 2015.

[8] C. Helstrom, «Quantum detection and estimation theory», *Journal of Statistical Physics*, Vol. 1, Issue 2, p. 231-252, 1969.

[9] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt and G. Leuchs, «Trojan-Horse Attacks Threaten the Security of Practical Quantum Cryptography», *New Journal of Physics*, Vol. 16, 2014.

[10] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt and G. Leuchs, «Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems», *IEEE Journal of Selected Topics in Quantum Electronic*s, Vol. 21, Issue 3, p. 168, 2015.

[11] V. Makarov and D.R. Hjelme, «Faked states attack on quantum cryptosystems», *Journal of Modern Optics*, Vol. 52, Issue 5, p. 691-705, 2005.

[12] С. Кулик, Е. Шапиро, С. Кулик, Т. Шмаонов, Д. Боумейстер и др., «Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления», М., Постмаркет, с. 33–73, 2002.

[13] С. Килин, Д. Хорошко, А. Низовцев, «Квантовая криптография: идеи и практика», Минск, Бел. наука, 391 с., 2007.

[14] V. Makarov, «Controlling passively quenched single photon detectors by bright light», *New Journal of Physics*, Vol. 11, 2009.

[15] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, «Hacking commercial quantum cryptography systems by tailored bright illumination», *Nature Photonics*, Vol. 4, Issue 10, p. 686-689, 2010.

[16] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar and Vadim Makarov, «Controlling an actively-quenched single photon detector with bright light», *Optics Express*, Vol. 19, Issue 23, p. 23590-23600, 2011.

[17] M. Dusek, O. Haderka, M. Hendrych, «Generalized beam-splitting attack in quantum cryptog raphy with dim coherent states», *Optics Communications*, Vol. 169, Issue 1-6., p. 103-108, 1999.

[18] G. Brassard, N. Lütkenhaus, T. Mor and B. Sanders, «Limitations on Practical Quantum Cryptog raphy», *Physical Review Letters*, Vol. 85, Issue 6, p. 1330, 2000.

[19] А. Холево, «О принципе квантовых неразрушающих измерений», *Журнал теоретической и математической физики*, Том 65, № 3, с. 415-422, 1985.

[20] A. Wójcik, «Eavesdropping on the «Ping-Pong» Quantum Communication Protocol», *Physical Review Letters*, Vol. 90, Issue 15, 2003.

УДК 003.26:004.056.55:621.39(045)

Лимарь И.В., Василиу Е.В., Рябуха А.Н., Жмурко Т.А. Классификация атак на квантовые системы передачи конфиденциальных данных

Аннотация. *В данной статье предложена расширенная классификация атак на протоколы и практически реализованные системы квантовой криптографии с учетом основных известных на сегодня видов нападений. Классификация разделяет атаки на три класса: пассивные атаки, которые возможные при использовании легитимными пользователями однофотонных источников; пассивные и активные атаки, обусловленные несовершенством оборудования систем квантовой связи (квантовый хакинг); пассивные и активные атаки, обусловленные несовершенством самых протоколов. Наличие такой классификации позволяет выполнять необходимую оценку стойкости протоколов квантовой криптографии и принимать решение относительно выбора доступных на рынке квантовых криптосистем по критерию их способности противостоять существующим и перспективным средствам квантового криптоанализа. Детально описаны атака Троянского коня и атака удаленного управления детекторами одиночных фотонов с использованием адаптированного яркого освещения. В рамках описания атаки управления детекторами изложен принцип использования фальшивых состояний, а также рассмотрены разновидности этой атаки, которые зависят от типа используемых в детекторах лавинных фотодиодов: с пассивным и активным способами гашения лавины, со стробированием.*

Ключевые слова: *квантовая криптография, квантовое распределение ключей, перехват информации, квантовый хакинг, детекторы единичных фотонов.*

Limar I., Vasiliu Ye., Riabukha O., Zhmurko T. Classification of the attacks on quantum systems for the transfer of confidential data

Abstract. *In this paper the extended classification of the attacks on the protocols and practically realized systems of quantum cryptography with taking into account the kinds of attacks, which are known at present time, is proposed. This classification subdivides attacks on three classes: the passive attacks, which are possible when the honest participants use single-photon sources, passive and active attacks, which are due to imperfection of the equipment of the quantum communication systems (quantum hacking), passive and active attacks, which are due to the own protocols imperfection. The existence of such classification lets to realize the necessary security estimation of quantum cryptography protocols and to make a decision concerning choice commercially available quantum cryptosystems by criterion of their ability to resist against present and perspective methods of quantum cryptanalysis. The Trojan-horse attack and attack of the remote control of the single-photon detectors with using of the tailored bright illumination in detail are described. In the frame of describing of the detectors control attack the principle of using of the faked states is stated. In addition, the varieties of such attack, which are depended from type of avalanche photodiodes: with passive and active method of avalanche quenching, gated photodiodes, are considered.*

Key words: *quantum cryptography, quantum key distribution, eavesdropping, quantum channel, quantum hacking, single photons detectors.*

Отримано *11 жовтня 2017 року*, затверджено редколегією 25 *жовтня 2017 року*