УДК 004.056.5

DOI: http://dx.doi.org/10.20535/2219-380413201546103

Калюжний І. Г.[1], *бакалавр*

КВАНТОВА КРИПТОГРАФІЯ: ПРИНЦИПИ, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

En

Quantum cryptography is a relatively new but promising method for secure data transmission. Today it is believed that it can ensure the absolute secrecy of data, resulting from the principles of quantum physics, on which it is based, namely the uncertainty principle of quantum Heisenberg. According to this principle cannot measure any aspect of photons without distorting thus irrevocably different option. That is the recipient of a message knows when attempting invasion in this necessarily knows. To create a quantum communication channel often use fiber optic lines or open space in which carriers serve single photons or pairs of entangled photons are often used.

Three tasks facing cryptography are:

1. Ensuring the confidentiality of messages sent via open communication channels.
2. Authentication messages that confirm the validity of the information received and sent.
3. Installing intrusion in fact, if it took place.

Given the importance of information security, quantum cryptography technology will soon be available not only banks or large corporations but also individuals. Leading IT companies are in search of optimum circuit solutions that

[1] *Національний технічний університет України "Київський політехнічний інститут", факультет інформатики та обчислювальної техніки*

would produce industrial equipment for the transmission of confidential information available for mass use. The main obstacles for implementation of quantum cryptography methods are short distances, which can transmit information with modern facilities, high cost and cumbersome equipment. To solve these problems prompted the idea of creating a hybrid air-fiber system using satellite communications is proposed. The use of artificial satellites for the transmission of photons through the air opens the possibility of secret key clients in any part of the Earth and even beyond.

It is also appropriate to review the possibility of using existing telecommunication and electrical networks for the transmission of quantum keys. The ideas p presented in the paper, open new space for scientific experiments.

Ru Рассмотрены методы передачи секретных ключей с помощью законов квантовой механики, приведены принципы, на которых основана квантовая криптография. Описана последовательность действий согласно протокола BB84. Перечислены основные проблемы практического использования методов квантового распределения ключа и предложены направления их решения. Рассмотрено современное состояние развития квантовой криптографии, деятельность некоторых компаний, которые занимаются разработкой и изготовлением оборудования, предназначенного для практического использования, приведены основные виды их продукции. Очерчены перспективы применения методов квантовой криптографии для широкого применения.

Вступ

Квантова криптографія – відносно новий, але багатообіцяючий метод безпечної передачі інформації. На сьогоднішній день уважаться, що вона може забезпечити абсолютну секретність передачі даних, що випливає з принципів квантової фізики, на яких вона заснована. Це відкриває величезні перспективи для повсюдного застосування криптографічних методів у всіх галузях. Беручи до уваги важливість інформаційної безпеки, технології квантової криптографії невдовзі будуть доступними не лише банкам або великим корпораціям, але і приватним особам. Провідні IT-компанії знаходяться в пошуку оптимальних схемотехнічних рішень, які дозволили б випускати промислове обладнання для передачі конфіденційної інформації, доступне для масового використання.

Постановка задачі

На сучасному етапі розвитку науки і техніки можливості квантової криптографії обмежені фізичними характеристиками обладнання та його високою вартістю, тому квантові системи шифрування поки що застосовуються для передачі секретних ключів на невеликі відстані та доступні незначній кількості великих корпорацій.

Метою даної роботи є пошук прийнятних технологічних рішень для застосування квантових криптографічних методів передачі інформації у будь-яку точку земної кулі та забезпечення користувачів доступними секретними ключами.

Аналіз існуючих рішень та практичне втілення ідей

Сьогодні дослідження в галузі квантової криптографії проводять багато компаній в усьому світі. Найвідоміші з них – *Toshiba, Mitsubishi, GAP-Optique, IBM*, технологічний інститут в Каліфорнії, Національна лабораторія в Лос-Аламосі. Вже зараз деякі компанії, як *ID Quantique, Smart Quantum, MagiQ* налагодили серійний випуск обладнання систем квантового розподілу ключів та встановлюють його своїм клієнтам – банкам, комерційним корпораціям, урядам держав.

Компанія *ID Quantique* є світовим лідером в області вирішення проблем захисту інформації методами квантової криптографії. Ця компанія була першою, що впровадила у серійне виробництво та комерційне використання прилади, дія яких заснована на принципах квантової фізики.

На сьогоднішній день *ID Quantique* виробляє три основні види обладнання [1]:

- високопродуктивні системи «Квантовий сейф», що забезпечують рішення мережевого шифрування для захисту даних при їх передачі та зберіганні. Дана платформа може шифрувати з високою пропускною здатністю трафіка – до 100 Gbps;
- квантові генератори випадкових чисел, які знайшли широке застосування у ігровій та лотерейній галузі;
- лічильник одиночних фотонів. Прилад дозволяє рахувати одиночні фотони, які потрапили на фотодетектор, довжин хвиль 1100-1600 нм. Прилади випускають двох типів – видимі лічильники фотонів на основі кремнієвих лавинних фотодіодів та інфрачервоні лічильники.

Компанія *MagiQ* більше 10 років тому однією з перших почала пропонувати комерційно доступну систему квантової криптографії під назвою *Navajo*. Серед розробок компанії є: синтезатор прямого цифрового синтезу, що забезпечує велику швидкість формування сигналу та високу точність; оптоволоконні датчики, а також квантова система криптографії *QPN Gateway Security*. Квантова система *Q-Box* з використанням одиночних фотонів розроблялася з метою використання у наукових, дослідницьких цілях [2].

Науковці лабораторії Лос-Аламоса розробили технологію *QKarD* [3], в якій методи шифрування інформації засновані на законах квантової механіки. *QKarD* являє собою портативний бездротовий прилад, простий у використанні.

Для аутентифікації *QKarD* використовує *PIN*-код або відбитки пальців. Користувачу потрібно авторизуватися і по оптоволоконному каналу зв’язку звернутися в сертифікаційний центр для генерації та отримання секретного ключа. Ключ зберігається в захищеній пам’яті приладу і використовується власником для шифрування інформації, аутентифікації та контролю доступу, забезпечення конфіденційності

зв'язку через повітряні канали, або для застосування у багатоканальній лінії зв'язку.

Методи квантової криптографії

Квантова криптографія заснована на принципі невизначеності квантових систем Гейзенберга. Згідно цього принципу неможливо виміряти будь-який параметр фотона, не спотворивши при цьому безповоротно іншого параметра [4]. Тобто отримувач повідомлення у випадку спроби вторгнення в систему обов'язково про це дізнається.

Для створення квантового каналу зв'язку найчастіше використовують оптоволоконні лінії або відкритий простір, носіями інформації в яких слугують одиночні фотони або пари заплутаних фотонів.

В основу квантової криптографії покладені наступні принципи квантової механіки [5]:

- неможливість зі стовідсотковою впевненістю розрізнити два неортогональних квантових стани;
- заборона на клонування. Завдяки лінійності та унітарності квантової механіки неможливо відтворити копію невідомого квантового стану без спотворення вихідного стану;
- наявність переплутаних квантових станів. Дві системи можуть знаходитися в стані взаємної кореляції. Внаслідок цього вимірювання параметра в одній системі призведе до змін цього параметра в іншій системі. Це пояснюється виникненням переплутаних квантових станів [6];
- причинність та суперпозиція. Якщо дві системи, стани яких об'єднані в певну суперпозицію, розділені в часі і при цьому не поєднані причинністю, то неможливо визначити стан суперпозиції, якщо проводити виміри параметрів послідовно в кожній із систем.

Три задачі, які стоять перед криптографією, це:

1. Забезпечення конфіденційності повідомлень, що відправляються через відкриті канали зв'язку.
2. Аутентифікація повідомлень, тобто підтвердження достовірності отриманої інформації та самого відправника.
3. Встановлення факту вторгнення в систему, якщо він мав місце [7].

Вирішення першої задачі полягає в проблемі розподілу секретного ключа, який використовується для шифрування повідомлень. Квантовий метод розподілу ключів відноситься до симетричних методів шифрування, тобто шифрувальний і дешифрувальний ключі або збігаються, або один ключ легко вираховується через інший. При цьому саме повідомлення передається через відкритий канал зв'язку, а квантовим каналом передають лише секретні ключі.

Інформація, яку передають по квантовому каналу, кодується за допомогою поляризації. В якості носіїв інформації використовують

одиночні фотони з різною поляризацією. Вони генеруються з заданою частотою, що гарантує повну секретність, адже будь-яка спроба перехвату фотона відразу стане помітною. Джерелом генерування фотонів виступає випромінювання напівпровідникового лазера. Довжина хвилі лазера визначає довжину хвилі згенерованих фотонів. Лазерні імпульси послаблюються за допомогою фільтрів до стану, коли один імпульс містить один фотон. Далі поляризований фотон направляється в оптоволоконний канал, по якому рухається до приймача фотонів. В кінцевому пункті відбувається фіксація станів фотонів, узгодження з відправником, аналіз та дешифрування повідомлення.

Основні проблеми квантової криптографії та напрями їх вирішення

Сьогодні існує декілька типів систем квантової передачі ключів, основні з них – системи з фазовим та поляризаційним кодуванням. Основною вимогою до квантового каналу є збереження стану та поляризації фотонів, щоб до отримувача дійшла достовірна інформація. І тут виникає перша проблема, яка значно обмежує використання методів квантової криптографії на практиці. В разі, коли для передачі ключів використовують оптоволоконну лінію, зі збільшенням відстані відбувається затухання сигналу через технологічні властивості самого оптоволокна. Сигнал потребує підсилення, але при сучасних технічних характеристиках таких засобів втрачається вихідна поляризація одиночних фотонів, або руйнується заплутаність фотонної пари, так само, як при спробі несанкціонованого доступу. До того ж високий рівень власних шумів, перешкод, які виникають у квантових каналах, часто не дає змоги отримати достовірну інформацію. Тому реальний зв’язок між користувачами поки що налагоджений на відстані в межах 150 км.

Одним з варіантів усунення проблеми затухання сигналу може бути створення спеціального квантового повторювача, який би підсилював сигнал, не порушуючи його вихідних характеристик. Цього можна досягти, використавши ідею квантової телепортації – перенесення параметрів одного квантового об’єкту на інший, що знаходиться від нього на відстані. Основною умовою для того, щоб стан об’єкту не змінився, є заборона на «зчитування» параметрів на всіх етапах. Квантовий стан фотона переноситься на атом. Через задану відстань цей атом телепортує свій стан на інший атом, і так до тих пір, поки кінцевий об’єкт не досягне отримувача інформації. Реалізація ідеї квантового повторювача виведе квантову криптографію на глобальний рівень інформаційної безпеки.

У випадку, коли секретні ключі передаються у вільному просторі, негативну роль відіграє турбулентність повітря та сонячне світло, тому тут відстані обмежені десятками кілометрів. Проблема деполяризації відсутня, але прийняттю достовірної інформації перешкоджає високий рівень шумів,

що залежить від стану навколишнього середовища, погодних умов, тощо. Ця проблема може бути вирішена за допомогою створення набагато потужнішого джерела випромінювання фотонів з використанням вузькополосної частотної та просторової фільтрації і наносекундних технологій. Це допоможе передавати та отримувати сигнали з допустимими похибками і на значно більші відстані. А використання штучних супутників для передачі інформації дозволить генерувати секретні ключі в любій точці Землі.

Ще одне вагоме обмеження використання квантової криптографії на практиці – складність процесу генерування однофотонних квантових станів. Для цього використовують установки, які продукують лазерні імпульси, що мають когерентні квантові стани. Але через технічні недоліки таких джерел імпульси можуть містити два, три або більше фотонів. Це призводить до того, що зловмисник може перехопити певну кількість фотонів, залишаючись непоміченим.

Також однією з перепон для практичної реалізації технологій квантової криптографії є необхідність встановлення у пунктах передачі та приймання інформації надскладного, громіздкого та синхронізованого між собою обладнання, до того ж занадто дорогого для широкого використання.

Для вирішення проблем поширення квантових криптосистем для передачі секретного ключа доцільно було б використовувати вже існуючі оптоволоконні телекомунікаційні мережі в поєднанні з супутниковим зв’язком та повітряним каналом. Ідея такої гібридної системи полягає в тому, щоб зменшити негативний вплив на точність передачі від природних факторів, негоди, одночасно забезпечивши значну відстань передачі повідомлення при відносно невеликих матеріальних затратах (рис. 1). В такій системі квант проходить шлях від супутників до наземних станцій по повітряному каналу, від наземних станцій до одержувача інформації - по оптоволоконному каналу. Це дозволить за допомогою супутників передавати конфіденційну інформацію в будь-яку точку земної кулі, де розміщені фотонні прийомними.

Рис. 1. Схема гібридної повітряно-оптоволоконної системи

Розглянемо на конкретному прикладі, як це може бути реалізовано в реальних умовах. Припустимо, що в лабораторіях в різних місцях одного континенту, позначимо умовно *A*1, *A*2, *A*3 проводяться секретні дослідження, результати яких потрібно передавати в центральний офіс *C*, що знаходиться на іншому континенті. Установка для зв'язку з супутником є в базовому пункті. В одному з міст континенту, на якому знаходяться лабораторії. Припустимо також, що між усіма підрозділами компанії налагоджена гібридна повітряно-оптоволоконна система зв'язку. Тоді схема передачі секретної інформації могла б виглядати наступним чином.

Зашифрована інформація передається по відкритому каналу від лабораторій *A*1, *A*2, *A*3 до центрального офісу *C*. З пунктів *A*1, *A*2, *A*3 передають згенеровані секретні ключі по прокладеним оптоволоконним лініям в пункт *B*. В певний момент часу, коли над пунктом *B* знаходиться супутник, квантові ключі по повітряному каналу за допомогою лазерного випромінювача передають до станції прийому, що знаходиться на супутнику. Супутник передає шифрувальні ключі до іншого супутника, що знаходиться на мінімальній відстані від пункту кінцевого прийому *C*, де сигнал фіксується та повідомлення дешифровується (рис. 2).

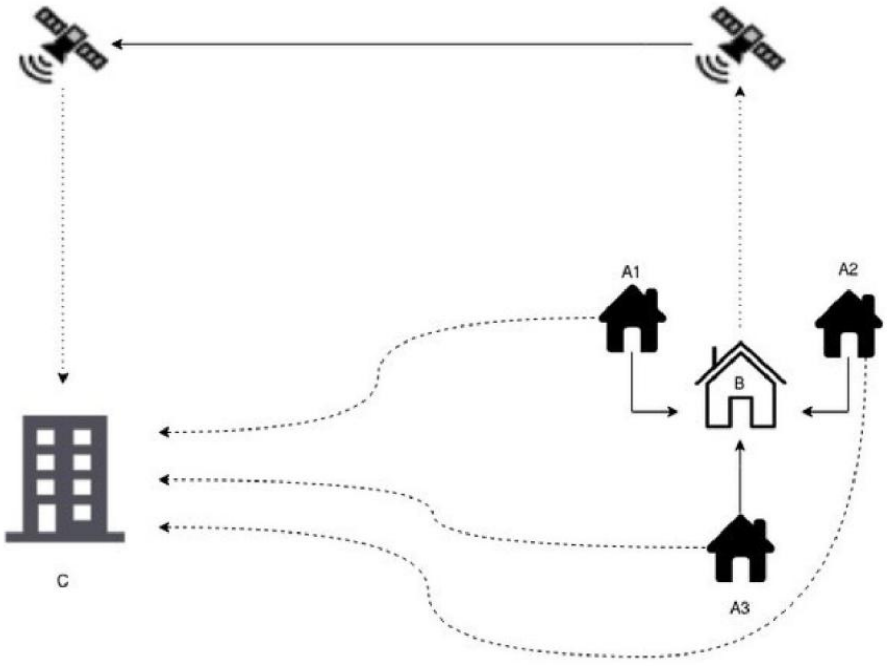

Рис. 2. Схема прикладу реалізації системи повітряно-оптоволоконного зв'язку

Приведена гібридна система є оптимальним варіантом вирішення подібної ситуації, тому що поєднує в собі переваги різних видів передачі ключів. По-перше, інформація по оптоволоконним лініям передається на порівняно невеликі відстані, тому в процесі руху фотони не затухають та не втрачають заданої поляризації і ключі дістаються до пункту *B* неушкодженими. Передача ключів повітряним каналом з пункту В до

супутника є достатньо ефективною, що було доведено експериментально китайськими дослідниками в 2012 році, коли фотони були передані по повітряному каналу на 97 км. Передача фотонів між супутниками безперешкодна, тут відсутні негативні фактори типу погодних умов, турбулентності повітря тощо. Отже, за допомогою приведеної повітряно-оптоволоконної схеми можна передавати конфіденційну інформацію на будь-які відстані без втрати достовірності.

Висновки

В даній статті визначено, що основними перешкодами для запровадження методів квантової криптографії є невеликі відстані, на які можна передавати інформацію сучасними засобами, значна вартість та громіздкість обладнання. Для вирішення цих проблем запропоновано ідею створення гібридної повітряно-оптоволоконної системи з використанням супутникового зв'язку. Використання штучних супутників для передачі фотонів через повітря відкриває можливість забезпечення секретними ключами клієнтів у будь-якій точці Землі, і навіть за її межами.

Доцільним є також розгляд можливості використання існуючих телекомунікаційних мереж для передачі квантових ключів. Ідеї, висунуті в статті, відкривають новий простір для наукових експериментів.

Програмісти, інженери та хакери постійно знаходять слабкі місця в системах криптографічного захисту, і періодично з'являється інформація про випадки їх злому або відкриття нової вразливості. Технології квантової криптографії з розвитком науки і техніки будуть удосконалюватися, і через певний проміжок часу ці проблеми будуть усунуті, але натомість виникатимуть інші, які ми зараз не можемо навіть уявити. Це процес безкінечний, та на даний момент квантова криптографія залишається найкращою та найперспективнішою системою захисту інформації.

Список використаної літератури

1. *IDQ* [Електронний ресурс]: [Інтернет-портал]. – Електронні дані. – [Швейцария, :Женева: ID Quantique, 2001-2015]. - Режим доступу: http://wpidq.cremarc.com/ (дата звернення 11.04.2015 р.). – Назва з екрана.
2. *MagiQ* [Електронний ресурс]: [Інтернет-портал]. – Електронні дані. – [США, :Нью-Йорк: Magiq Technologies, 1999-2015]. - Режим доступу: http://www.magiqtech.com/ (дата звернення 10.04.2015 р.). – Назва з екрана.
3. *Los Alamos National Laboratory* [Електронний ресурс]: [Інтернет-портал]. – Електронні дані. – [США, Лос-Аламос: Los Alamos National Laboratory, 1943-2015]. – Режим доступу: http://www.lanl.gov/projects/feynman-center/technologies/information-

technology-communications/qkard-quantum-smart-card.php (дата звернення 20.04.2015 р.). – Назва з екрана.

4. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / С. П. Кулик, Е.А. Шапиро (пер. с англ.); С. П. Кулик, Т. А. Шмаонов (ред. пер.); Д. Боумейстер и др. (ред.). — М.: Постмаркет, 2002. — 358с.
5. *Shor P. W.* Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Symposium on Foundations of Computer Science, Los Alamitos, ed. by Sh.Goldwasser (IEEE Computer Society Press), 1994, p.134.
6. *Скалли М. О., Зубайри М. С.* Квантовая оптика. / Пер. с англ. под ред. В. В. Самарцева. – М.: Физматлит, 2003. – 512с.
7. *Столлингс В*. Криптография и защита сетей: принципы и практика, – 2-е изд.: Пер. с англ. – М.: ИД «Вильямс», 2001. – 672 с.