ПЕРСПЕКТИВИ КВАНТОВОГО ШИФРУВАННЯ У СИСТЕМАХ ІНФОКОМУНІКАЦІЙ

Соколов О.К., Штангей С.В.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: oleksandr.sokolov1@nure.ua

Abstract

Quantum encryption is a promising direction in the field of information security that uses the principles of quantum mechanics to protect data. It uses the physical properties of quantum particles to generate and transmit encryption keys. The main advantage of quantum encryption is that it can guarantee the absolute security of the key. This means that any attempt to intercept or measure the key will cause it to change, which will be immediately apparent. However, despite its potential, quantum encryption is still in its early stages of development. There are many technical challenges to overcome before it becomes widely available. Despite these challenges, the prospects of quantum encryption in information communication systems remain high. With the development of quantum technologies, we can expect new and exciting opportunities in the field of information security.

Вступ

Квантова криптографія – це достатньо нова галузь криптографії, що використовує принципи квантової механіки для забезпечення безпеки комунікацій та обміну інформацією. Вона використовує фізичні властивості квантових частин, таких як квантові біти (або кубіти), для забезпечення конфіденційності та цілісності передачі даних.

Квантова криптографія має величезний потенціал у сфері інформаційних технологій та комунікацій. У сфері інокомунікацій, де безпека передачі даних має критичне значення, квантова криптографія може забезпечити високий рівень захисту.

Однією з основних переваг є надзвичайна стійкість квантових ключів до перехоплення. Квантові ключі гарантують конфіденційність, оскільки будь-яка спроба перехоплення ключа призведе до зміни стану квантового об'єкту, що буде помітно для співрозмовників, тим самим автоматично скасовуючи будь-яку спробу вторгнення в комунікацію.

Технологія квантової криптографії також має потенціал для розвитку безпечних квантових мереж, де дані можуть передаватися з використанням квантових каналів зв'язку. Це може відкрити нові можливості для безпечної передачі великих обсягів даних у сферах, де захист інформації є критичним, таких як фінанси, охорона здоров'я, важливі урядові комунікації та багато інших.

Принципи квантового шифрування

Квантова криптографія ґрунтується на принципі невизначеності, визначеному у квантових системах Гейзенберга. Згідно з цим принципом, неможливо виміряти будь-який параметр фотона, не впливаючи при цьому на інший параметр без можливості повернення його у попередній стан [1]. Іншими словами, спроба отримати інформацію про фотон обов'язково викличе зміни, які буде помічено отримувачем повідомлення.

Для створення квантового каналу зв'язку найчастіше використовують оптоволоконні лінії або відкритий простір. В цих системах інформацію передають за допомогою одиночних фотонів або пар заплутаних фотонів.

В основу квантової криптографії покладені наступні принципи квантової механіки [7]:

1) Невизначеність квантових систем Гейзенберга:
- Квантовий принцип невизначеності Гейзенберга стверджує, що точне вимірювання двох взаємно ортогональних параметрів одного фотона неможливе без спотворення іншого параметра. Це забезпечує неможливість безперервного і непомітного перехоплення квантових ключів, оскільки будь-яке втручання змінює стан системи.

2) Клонування і лінійність квантової механіки:
- Лінійність і унітарність квантової механіки роблять неможливим точне копіювання невідомого квантового стану без зміни вихідного стану. Це дозволяє виявити будь-яке незаконне спробу розкрити квантовий ключ.

3) Переплутані квантові стани:
- Застосування переплутаних станів дозволяє створити квантові ключі, які будуть взаємно залежними. Зміна стану одного фотона призведе до автоматичної зміни стану іншого, що робить неможливим вимірювання без помітних змін [2].

4) Причинність та суперпозиція:
- Принцип причинності та суперпозиції стверджує, що якщо дві системи знаходяться в певній суперпозиції та розділені в часі без причинної зв'язку, то вимірювання параметрів однієї системи не дасть інформації про стан суперпозиції. Це може використовуватися для створення безпечних квантових каналів.

Всі ці принципи використовуються для вирішення основних завдань криптографії:

1) Забезпечення конфіденційності повідомлень:
- Квантова криптографія надає засоби для створення квантових ключів, які гарантують конфіденційність повідомлень.

2) Аутентифікація повідомлень:
- Застосування квантових ключів також дозволяє відправнику і одержувачу перевіряти автентичність повідомлення.

3) Виявлення вторгнень [3]:
- Квантова криптографія може виявляти вторгнення через неможливість безпомилкової перехопки квантових ключів.

Розв'язання першої задачі полягає в розподілі секретного ключа для шифрування повідомлень. Квантовий метод розподілу ключів відноситься до симетричних методів шифрування, де шифрувальний і дешифрувальний ключі або збігаються, або один ключ може легко вираховуватися з іншого. У цьому випадку повідомлення передається через відкритий канал зв'язку, тоді як квантовим каналом передаються тільки секретні ключі.

Інформацію, що передається по квантовому каналу, кодують за допомогою поляризації. Одиночні фотони з різною поляризацією виступають носіями інформації і генеруються з заданою частотою, що забезпечує повну секретність, оскільки будь-яка спроба перехоплення фотона стає помітною. Напівпровідниковий лазер виступає джерелом генерації фотонів, а довжина хвилі лазера визначає довжину хвилі створених фотонів. Лазерні імпульси послаблюються за допомогою фільтрів до стану, коли один імпульс містить один фотон. Потім поляризований фотон направляється в оптоволоконний канал, по якому рухається до приймача фотонів. У кінцевому пункті відбувається фіксація станів фотонів, узгодження з відправником, аналіз та дешифрування повідомлення.

Рис. 1. Запропоновані системи захисту інформації на базі квантових технологій

Приклади використання квантового шифрування в реальних системах

Наразі існують системи, що базуються на квантовій криптографії:

- MagiQ QPN Security Gateway (QPN-8505) від MagiQ Technologies, США, є провідним рішенням для квантової криптографії, яке забезпечує передову мережеву безпеку та надійний захист від численних викликів, пов'язаних з розподілом та управлінням криптографічними ключами. З його допомогою фінансові організації можуть захистити свої найбільш критичні комунікаційні зв'язки від вторгнень та крадіжки даних. MagiQ QPN підтримує різноманітні архітектури мереж і надає інфраструктуру обміну криптографічними ключами для захисту інформаційних каналів.

    - Захист VPN за допомогою квантового розподілу ключів (до ста 256 бітних ключів у секунду на відстань до 140 км) та інтегрованого шифрування;
    - Використовуються такі протоколи: квантовий BB84, класичні 3DES (112 біт) та AES (256 біт).
    - Вартість мінімальної конфігурації € 80 тис. [6]

- Clavis2 та Cerberis - це продукти від ID Quantique, провідної компанії в області квантової кібербезпеки зі штаб-квартирою в Швейцарії.

    - Clavis2 (Clavis XG) - це система квантового розподілу ключів (QKD), яка забезпечує високий обсяг передачі ключів та дальній діапазон зв'язку. Вона ідеально підходить для інтеграції в довгодистанційні оптичні мережі, особливо в середовищах виробництва підприємств, урядових установ та телекомунікацій.
    - Cerberis (Cerberis XG) - це також система QKD, але вона розроблена для середнього діапазону зв'язку та стандартного обсягу передачі ключів. Вона добре підходить для зв'язку між основними та крайовими вузлами (вузлами кінцевого користувача), особливо в середовищах виробництва підприємств, урядових установ та телекомунікацій.

    Обидві системи використовують принципи квантової механіки для безпечного розподілу ключів, що генеруються QRNG, до різних місць. Вони забезпечують довгострокову конфіденційність та цілісність, максимізуючи довіру. [5]

Перспективні проекти та дослідження в галузі квантової криптографії

Secure Communication based on Quantum Cryptography (SECOQC) - це проект, який має на меті розробити квантову криптографію. Європейський Союз вирішив в 2004 році інвестувати 11 мільйонів євро в проект як спосіб обійти спроби шпигунства ECHELON.

SECOQC було створено для розробки та перевірки мережі для надійного та безпечного довготривалого зв'язку, заснованого на технології розподілу квантових ключів (QKD).

Архітектура мережі SECOQC може бути поділена на дві частини: довірені приватні мережі та квантові мережі, пов'язані через QBB (квантові магістралі). Приватні мережі - це звичайні мережі з кінцевими вузлами та QBB. Кожен QBB дозволяє квантовий канал зв'язку з іншим QBB і складається з числа пристроїв QKD, які пов'язані з іншими пристроями QKD через один-до-одного з'єднання. Завдяки цьому, SECOQC може забезпечити легшу реєстрацію нових кінцевих вузлів в мережі QKD та швидке відновлення від загроз на квантових каналах зв'язку. [4]

Висновки

Квантова криптографія відкриває нові можливості для систем інфокомунікацій, використовуючи принципи квантової фізики для захисту комунікацій. Однак, необхідно провести більше досліджень для подолання викликів, пов’язаних з надійністю і ефективністю передачі ключів. Незважаючи на це, перспективи квантового шифрування в системах інфокомунікацій виглядають дуже обіцяючими. Але одним з основних недоліків квантової криптографії є те, що вона працює лише на відносно невеликих відстанях. Це обмежує її застосування, особливо в мережах з великими відстанями між вузлами. Використання повторювачів може допомогти збільшити цю відстань, але це може створити слабкі місця в системі. Крім того, сьогоднішня квантова криптографія може захищати лише точкові з’єднання, розташовані приблизно на відстані 100 кілометрів одне від одного.

Література

1. The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation / ed. by D. B. (Editor), A. K. E. (Editor), A. Z. (Editor). Springer, 2000. 314 p.
2. Scully M. O. Quantum optics. Cambridge : Cambridge University Press, 1997. 630 p.
3. Stallings W. Cryptography and Network Security: Principles and Practice (2nd Edition). 2nd ed. Prentice Hall. 569 p.
4. CORDIS, cordis.europa.eu. Development of a Global Network for Secure Communication based on Quantum Cryptography | SECOQC Project | Fact Sheet | FP6 | CORDIS | European Commission. CORDIS | European Commission. URL: https://cordis.europa.eu/project/id/506813 (date of access: 15.11.2023).
5. Curran M. Clavis XG QKD System. ID Quantique. URL: https://www.idquantique.com/quantum-safe-security/products/clavis-xg-qkd-system/ (date of access: 15.11.2023).
6. MagiQ QPN™| Network Security | Somerville, MA. MagiQ Technologies. URL: https://www.magiqtech.com/solutions/network-security/ (date of access: 15.11.2023).
7. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring. 35th annual symposium on foundations of computer science, Santa Fe, NM, USA. URL: https://doi.org/10.1109/sfcs.1994.365700 (date of access: 16.11.2023).