УДК 004.056.55

М. Т. Мовчанюк
І. О. Бондаренко

КВАНТОВА КРИПТОГРАФІЯ: РЕВОЛЮЦІЙНИЙ ПІДХІД ДО КРИПТОГРАФІЇ

Вінницький національний технічний університет

Анотація

Доповідь присвячена огляду основних принципів квантової криптографії, яка є однією із перспективних галузей криптографії, що використовує закони квантової механіки для захисту інформації. В доповіді будуть розглянуто принципи квантової криптографії, які базуються на використанні властивостей квантових систем для створення безпечних криптографічних протоколів.

Ключові слова: безпека інформації, конфіденційність даних, шифрування, квантова криптографія, , кубіт, квантовий канал, протокол, принципи квантової криптографії.

Abstract

The report is devoted to an overview of the basic principles of quantum cryptography, which is a promising branch of cryptography that uses the laws of quantum mechanics to protect information. The principles of quantum cryptography will be discussed, which are based on the use of properties of quantum systems to create secure cryptographic protocols.

Keywords: information security, data privacy, encryption, quantum cryptography, , qubit, quantum channel, protocol, principles of quantum cryptography.

Вступ

Зв'язок та збереження інформації є ключовими аспектами сучасного світу. У наш цифровий вік, коли людство постійно обмінюється даними через Інтернет, захист інформації є надзвичайно важливим завданням. Класична криптографія, яка ґрунтується на математичних алгоритмах, була використовувана для захисту даних протягом багатьох років. Проте з появою квантової криптографії стало можливим забезпечення більш високого рівня захисту інформації.

Квантова криптографія є одним із перспективним напрямком розвитку криптографії, який використовує принципи квантової механіки для захисту інформації від зловмисників. Ця технологія важлива в світлі збільшення кількості кібератак на різноманітні об'єкти та відкриті системи зв'язку, які все частіше вимагають захисту конфіденційної інформації.

Результати дослідження

Квантова криптографія – метод захисту інформації, який використовує закони квантової механіки. Це новітній метод захисту даних, який базується на принципах квантової фізики, таких як незалежність вимірювань і стан квантової системи, який неможливо скопіювати або змінити непомітно [1]. Це дає змогу створювати криптографічні протоколи, стійкі до перехоплення та прослуховування, що робить квантову криптографію досить перспективним методом для захисту даних.

Одним із основних принципів квантової криптографії є використання квантових каналів зв'язку, які забезпечують безпеку передачі ключів [2]. За допомогою квантової криптографії, відправник може надсилати квантові біти одержувачу через квантовий канал. Одержувач змірює стани квантових бітів і надсилає відповідь відправнику, що дозволяє їм взаємодіяти та передавати інформацію. Якщо під час передачі квантових бітів виникає будь-яке втручання, то це може бути виявлено за допомогою інших методів квантової криптографії, які дозволяють визначити, що інформація була перехоплена.

Замість звичайних бітів використовуються квантові біти або кубіти, які можуть бути в будь-якому стані між 0 і 1. Це означає, що інформація, яка передається за допомогою кубітів, захищена від прослуховування третіми сторонами. Коли користувач надсилає свої дані, вони кодуються в кубіти та відправляються через квантовий канал одержувачу. Якщо хтось спробує підслухати ці дані, це змінить їх стан, що призведе до помилкових значень і сповістить сторони про спробу підслуховування [3].

При передачі інформації використовується протокол квантової криптографії, який забезпечує безпеку передачі даних. Основна ідея протоколу полягає в тому, що квантовий ключ може бути переданий як відправнику, так і одержувачу без можливості перехоплення або зміни його стану [4]. У разі спроби перехоплення квантового ключа, його стан змінюється, що виявляється відправником і призводить до відхилення від коректної передачі даних.

Одним із методів квантової криптографії є протокол Беннета-Брассарда (BB84), який дозволяє створити безпечний квантовий канал зв'язку для передачі ключів. Протокол BB84 використовує дві базові операції: вимір квантового стану та генерацію квантового стану. Під час передачі ключів квантовий стан пересилається зі сторони відправника до сторони одержувача, і виконуються виміри, які дозволяють визначити, чи був стан сприйнятий правильно [5].

Квантова криптографія надійна, оскільки зламати таку систему майже неможливо, навіть за допомогою квантових комп'ютерів, які ще не є настільки розвиненими, щоб здійснити таку атаку та стійка до ряду атак, які є успішними проти класичних криптографічних методів, таких як атаки "людина посередині" та атаки з перехопленням ключа [6]. Однак важливо зазначити, що квантова криптографія не є універсальним рішенням для забезпечення безпеки зв’язку, але вона дозволяє забезпечити високий рівень безпеки в обміні ключами і передачі даних. Також важливим є застосування відповідних протоколів забезпечення конфіденційності інформації під час збереження і передачі даних [7].

Принципи квантової криптографії базуються на використанні властивостей квантових систем для створення безпечних криптографічних протоколів. Основними принципами квантової криптографії є [8]:

1. Принцип невідомості: Ключі шифрування та розшифрування повинні бути відомі лише відправнику та одержувачу повідомлення, і не можуть бути отримані третьою стороною.

2. Принцип незмінності: Інформація, що передається, повинна бути захищена під час передачі від несанкціонованого доступу та модифікації.

3. Принцип безпеки: Квантова криптографія повинна забезпечувати безпеку передачі інформації, навіть якщо нападник має доступ до квантових систем, які використовуються для передачі.

4. Принцип невизначеності: Квантова криптографія використовує властивості квантових систем, таких, як невизначеність та взаємодія, для захисту інформації від несанкціонованого доступу.

Таким чином, квантова криптографія дозволяє створювати криптографічні протоколи, які є абсолютно безпечними від перехоплення та прослуховування. Квантова криптографія використовується для захисту даних у багатьох сферах, включаючи комунікації між фінансовими установами, урядовими органами та військовими підрозділами [9].

Одним із найважливіших завдань квантової криптографії є розширення діапазону передачі квантових ключів. В даний час квантові криптосистеми здатні передавати ключі на відстані в сотні кілометрів за допомогою оптичного волокна. Однак, для великих відстаней, наприклад, між континентами, потрібні нові технології передачі та отримання квантової інформації.

Одним із напрямів розвитку квантової криптографії є використання супутників для передачі квантових ключів. Нещодавні досягнення китайських вчених показали можливість передачі квантових ключів на відстань понад 1200 км за допомогою супутників [10]. Це відкриває нові можливості для захисту інформації на великій відстані, наприклад, в області фінансових та комунікаційних послуг.

Ще одним напрямком розвитку є розробка нових протоколів квантової криптографії, які забезпечать більшу безпеку передачі квантових ключів. Наприклад, вже існують протоколи, які дозволяють виявити будь-яке перехоплення кубітів під час передачі [11]. Такі протоколи можуть забезпечити ще більшу стійкість квантових криптосистем до атак хакерів та унеможливити їх розшифрування.

Висновки

У порівнянні з традиційними методами шифрування, які можуть бути розшифровані з використанням сучасних обчислювальних ресурсів, квантова криптографія забезпечує надзвичайно високий рівень захисту інформації. Квантова криптографія є перспективною галуззю криптографії, яка використовує закони квантової механіки для захисту інформації. Квантова криптографія дозволяє створювати безпечні криптографічні протоколи, які не можна підробити або зламати з використанням сучасних алгоритмів.

Незважаючи на те, що квантова криптографія ще не стала повсякденним інструментом, вона є перспективною галуззю, яка має потенціал змінити підхід до захисту інформації в майбутньому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Квантова криптографія. Пояснення [Електронний ресурс] // Quantum Xchange. – 2010. – Режим доступу: https://quantumxc.com/blog/quantum-cryptography-explained/ (дата звернення 02.03.2023).

2. Satish Kumar. Quantum Cryptography [Електронний ресурс] // Tutorialspoint. – 2023. – Режим доступу: http://surl.li/fjebs (дата звернення 05.03.2023).

3. Грамблінг Е. Квантові обчислення. Прогрес і перспективи / Е. Грамблінг, М. Горовіц. – Вашингтон: Національні академії наук, техніки та медицини, 2019. – 272 с.

4. Беннетт Ч. Х., Брассар Ж. Квантова криптографія. Теоретична інформатика. 2014. Т. 1, № 540. С. 7–11.

5. Ву М. К., Хун П. Ч., Квон П. Б. Практичний квантовий розподіл ключів, що не залежить від приладу вимірювання, із поляризаційним мультиплексуванням. IEEE Access. 2018. Т. 6. С. 58587–58593.

6. Тан Я.-Л., Інь Х.-Л., Чен С.-Ц. Польове випробування незалежного від вимірювального пристрою розподілу квантових ключів. IEEE. 2014. Т. 21, № 3. 6600407.

7. Ван Ш., Хе Д.-Ю., Інь Ч.-Ц. Обробка сигналів у подвійному розподілі квантового ключа. IEEE. 2022. Т. 14. С. 578–581.

8. Петц Д. Перегляд монотонності квантової відносної ентропії. Reviews in Mathematical Physics. 2003. Т. 15. С. 79–91.

9. Екерт А., Реннер Р. Остаточні фізичні межі конфіденційності. Nature. 2014. Т. 507. С. 443–447. Режим доступу: https://doi.org/10.1038/nature13132 (дата звернення 06.03.2023).

10. Liao, SK., Cai, WQ., Liu, WY. et al. Satellite-to-ground quantum key distribution. Nature. 2017. Т. 549. С. 43–47. Режим доступу: https://doi.org/10.1038/nature23655 (дата звернення 08.03.2023).

11. Керті М., Ло Х.-К., Тамакі К. Безпечний квантовий розподіл ключів. Фотоніка природи. 2014. Т. 8. С. 595–604.

Мовчанюк Мар'яна Тимофіївна – студентка групи 2КІТС-22м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: aelil.mary@gmail.com

Бондаренко Ірина Олексіївна – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Movchanyuk Mariana T. – student of 2CSITS-22m group, Department of Management and Information Security, Vinnytsa National Technical University, Vinnytsia**,** e-mail: aelil.mary@gmail.com

Bondarenko Iryna O. – assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua