Квантовий прямий безпечний зв'язок і квантове розділення секрету з використанням переплутаних квантових станів

УДК 003.26:621.39+530.145

Євген Василіу[1], Олександр Назаренко, Сергій Стайкуца

Державний університет інтелектуальних технологій і зв'язку,
[1]y.v_vasiliu@suitt.edu.ua

Квантові технології захисту інформації є одним із найбільш перспективних напрямів розвитку сучасної криптографії та систем захищеного зв'язку. Інтенсивний розвиток квантових обчислень створює потенційну загрозу для класичних криптографічних алгоритмів, що стимулює пошук нових підходів до забезпечення конфіденційності та цілісності інформації. У зв'язку з цим значну увагу привертають протоколи квантового прямого безпечного зв'язку (КПБЗ) та квантового розділення секрету (КРС), які використовують фундаментальні властивості квантової механіки для захищеного передавання даних [1-3].

Метою роботи є огляд та порівняльний аналіз протоколів квантового прямого безпечного зв'язку і квантового розділення секрету, що базуються на використанні переплутаних квантових станів кубітів та квантових систем більшої розмірності. Особливу увагу приділено пінг-понг протоколам зі станами Белла, багатокубітними ГХЦ-станами та кутритними переплутаними станами, а також аналізу їх інформаційної місткості та стійкості до некогерентних атак пасивного перехоплення.

На відміну від систем квантового розподілення ключів, у протоколах КПБЗ квантовий канал використовується для прямого передавання інформації, а не лише для формування спільного секретного ключа. Кодування класичної інформації виконується шляхом локальних унітарних операцій над частиною переплутаної квантової системи. Для протоколів із використанням станів Белла реалізується механізм квантового надщільного кодування, який дозволяє передавати два класичних біти за один цикл обміну квантовими частинками. Застосування багаточастинкових ГХЦ-станів та надщільного кодування забезпечує збільшення кількості переданих бітів та створює можливість реалізації багатокористувацьких схем захищеного квантового зв'язку.

Важливим елементом пінг-понг протоколів є наявність режиму контролю прослуховування каналу. У цьому режимі учасники виконують контрольні вимірювання квантових станів для виявлення спроб несанкціонованого втручання. Наявність підслуховування призводить до порушення квантових кореляцій між переплутаними частинками, що дозволяє виявити атаку з певною ймовірністю. Аналіз показує, що збільшення розмірності квантових систем та кількості частинок у багаточастинковому переплутаному стані підвищує рівень стійкості протоколів до атак перехоплення.

Окрему увагу приділено атакам пасивного перехоплення, які базуються на переплутуванні допоміжної квантової системи з передаваними кубітами та належать до класу некогерентних атак. Ефективність таких атак може оцінюватися за допомогою ентропії фон Неймана та ймовірності невиявлення перехоплення. Проведений аналіз демонструє, що протоколи з багато-

частинковими переплутаними станами характеризуються вищим рівнем стійкості порівняно з базовими схемами.

Для додаткового посилення стійкості може застосовуватися метод посилення таємності, який базується на використанні випадкових оборотних двійкових матриць та випадкової двійкової гами. Такий підхід забезпечує інформаційну незалежність переданих блоків від вихідного повідомлення навіть у разі часткового отримання інформації порушником.

Розглянуто також протоколи квантового розділення секрету, у яких відновлення конфіденційної інформації можливе лише за умови кооперації декількох учасників мережі. Використання переплутаних станів Белла та багатокубітних ГХЦ-станів дозволяє реалізувати схеми, у яких жоден із учасників окремо не може відновити секрет. Відновлення інформації здійснюється лише після обміну результатами вимірювань та інформацією про виконані кодувальні операції. Такий підхід забезпечує високий рівень захисту від внутрішніх і зовнішніх порушників та може бути використаний у розподілених інформаційних системах і критично важливих мережах.

Проведений огляд свідчить, що протоколи КПБЗ і КРС є перспективною основою для побудови майбутніх квантових мереж та систем захисту інформації. Серед основних переваг таких протоколів можна виділити можливість прямого передавання інформації, вбудоване виявлення підслуховування, підтримку багатокористувацьких сценаріїв та потенційно теоретико-інформаційний рівень захищеності. Водночас практична реалізація квантових систем зв'язку супроводжується значними технічними труднощами, пов'язаними з необхідністю використання ефективних джерел одиничних фотонів і переплутаних станів, квантової пам'яті, чутливих детекторів і захисту від впливу шумів та втрат у каналах передавання.

Подальший розвиток квантових технологій захисту інформації пов'язаний із вдосконаленням квантових каналів зв'язку, підвищенням завадостійкості протоколів, створенням масштабованих квантових мереж та інтеграцією квантових і постквантових криптографічних методів. Очікується, що розвиток супутникового квантового зв'язку та глобальних квантових мереж стане основою для формування нової глобальної безпечної інформаційної інфраструктури.

1. Vasiliu Y. Modern Quantum Technologies of Cryptographic Protection of Information. *Cybernetics and Systems Analysis*. – 2025. – Vol. 61, no. 4. – P. 671 – 684.
2. Pan D., Long G.L., Yin L., Sheng Y.B., Ruan D., Ng S.X., Lu J., Hanzo L. The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet. *IEEE Communications Surveys & Tutorials*. – 2024. – Vol. 26, no. 3. – P. 1898 – 1949.
3. Liu S., Lu Z., Wang P. et al. Experimental demonstration of multiparty quantum secret sharing and conference key agreement. *npj Quantum Information*. – 2023. – Vol. 9. – 92.