

Квантовий прямий безпечний зв'язок і квантове розділення секрету з переплутаними станами кубітів і квантових систем більшої розмірності

Квантова криптографія являє собою нову парадигму криптографічного захисту інформації з використанням законів квантової механіки та відповідних квантових властивостей носіїв інформації – фотонів для усунення обмежень класичних криптографічних протоколів та підвищення стійкості криптопротоколів аж до теоретико-інформаційного рівня.

На сьогодні найбільш розвиненим напрямом квантової криптографії є квантові протоколи розподілення ключів. Це єдиний напрям, що вже реалізований не тільки у лабораторних умовах, а і використовується для розподілення таємних ключів у системах шифрування в багатьох розвинених країнах світу.

Інші напрями – квантовий прямий безпечний зв'язок (КПБЗ) та квантове розділення секрету (КРС) також мають значні переваги над методами класичної криптографії.

Головною особливістю протоколів КПБЗ є відсутність криптографічних перетворень, отже, використання КПБЗ взагалі усуває необхідність попереднього обміну таємними ключами. У цих протоколах таємне повідомлення безпосередньо кодується станами кубітів (кудитів), які надсилаються через квантовий канал.

Розглядаються схеми протоколів типу пінг-понг з переплутаними дво-, три та чотирикубітними станами, а також з переплутаними парами кутритів. Виконано порівняльний аналіз стійкості зазначених протоколів до некогерентної атаки пасивного перехоплення. Всі пінг-понг протоколи мають асимптотичну стійкість до цієї атаки. Розроблено методи підсилення стійкості до атаки пасивного перехоплення, які придатні для будь-якого варіанта пінг-понг протоколу з дискретними квантовими станами.

Протоколи на основі використання блоків переплутаних кубітів (кудитів) дають змогу виявити спроби підслуховування квантового каналу до початку передавання самого повідомлення. Завдяки цьому можна гарантувати безпеку передавання: у разі виявлення підслуховування до передавання повідомлення законні користувачі переривають сеанс зв'язку, і жодна інформація не потрапляє до зломисника. Проте для зберігання таких блоків кубітів потрібна квантова пам'ять великого обсягу. Як відомо, технологію квантової пам'яті активно розробляють, але поки що цю технологію ще не можна масово застосувати у стандартному телекомунікаційному обладнанні. Тому протоколи типу пінг-понг на сьогодні мають значну перевагу з технічної точки зору, але потребують додаткових методів підсилення стійкості до атаки пасивного перехоплення.

Розділення секрету – це фундаментальний криптографічний примітив, який використовують для безпечного поширення даних. Секрет розподіляється серед визначеної групи з n учасників, кожному з яких надсилається деяка частка секрету. Відтворити секрет може тільки коаліція з t учасників, де $t \leq n$ (так звана (t, n) -порогова схема).

Квантове розділення секрету є розширенням цього криптографічного примітиву на використання квантово-механічних властивостей фотонів, що дає змогу підвищити безпеку розділення секрету за межі класичних підходів. Так, безумовною перевагою квантових протоколів розділення секрету над класичними є принципова можливість завжди виявити підслуховування каналу зв'язку у випадку, якщо розділення секрету відбувається віддалено. Також квантові протоколи розділення секрету завдяки використанню переплутаних квантових станів більш захищені від нечесних дій учасників самого протоколу.

Розглянуто квантові протоколи розділення секрету з парами переплутаних кубітів та кутритів, що ґрунтуються на схемі пінг-понг протоколу. Проаналізовано стійкість цих протоколів до некогерентної атаки пасивного перехоплення.

Відомості про доповідача:

Васіліу Євген Вікторович

науковий ступінь – д.т.н.

вчене звання – професор

посада – декан ф-ту Інформаційних технологій та кібербезпеки

установа – Державний університет інтелектуальних технологій і зв'язку (м. Одеса)