УДК 004.056.53

В. В. Горіна,
Є. В. Негодюк
Національний авіаційний університет, Київ

ЗАСТОСУВАННЯ КВАНТОВОЇ ФІЗИКИ В КРИПТОГРАФІЇ ТА ЗАХИСТІ ДАНИХ

На сьогодення Інтеренет не тільки став необхідною складовою нашого життя, але й значно полегшив нашу повсякденну діяльність та забезпечив доступ до багатьох ресурсів та інформації.. Однак разом з цими плюсами він несе в собі вагому загрозу, а саме: втрату даних та використання їх зловмисниками для своїх корисливих цілей. Тому у сучасному світі важливим питанням є захист даних. Одним із найбільш поширених методів захисту є криптографічні протоколи, що використовують математичні алгоритми для захисту даних перед їх передачею, таких як RSA, AES і DES. Ці алгоритми шифрують дані за допомогою ключа, що генерується за певними правилами, і призначені для того, щоб зберегти інформацію в секреті, коли вона пересилається через відкриті мережі.

Проте, з появою квантових комп'ютерів стало очевидним, що ці алгоритми можуть бути легко розшифровані. Квантові комп'ютери здатні до швидкого розв'язування проблем, які займали кілька років для класичного комп'ютера, таких як факторизація великих простих чисел. Це вказує на те, що квантовий комп'ютер може легко розшифрувати дані, зашифровані звичайними алгоритмами.

Одним з підходів до розв'язання цієї задачі є застосування квантової криптографії, яка використовує властивості квантових частинок для створення безпечних криптографічних ключів та захисту передачі даних. Популярний метод квантової криптографії - це квантовий ключовий обмін (QKD). Він базується на використанні квантових властивостей світла, щоб створити безпечний криптографічний ключ між сторонами комунікації. Ключовим моментом у QKD є те, що при спробі перехоплення сигнального стану зі сторони зловмисника, він змінюється в результаті принципу невизначеності Гейзенберга.

Однією з основних переваг QKD є безумовна безпека, яку він забезпечує. Тобто квантовий ключ, який створюється в процесі

QKD, не може бути скомпрометований віддаленою стороною, навіть якщо він володіє найсучаснішими комп'ютерами та алгоритмами. Це відрізняє QKD від традиційних методів криптографії, які можуть бути підірвані сучасними комп'ютерами з високим рівнем обчислювальної потужності та складними алгоритмами. Це означає, що навіть якщо зловмисник отримує доступ до зашифрованих даних, не можна розшифрувати їх без квантового ключа. Таким чином, QKD забезпечує високий рівень безпеки для захисту конфіденційної інформації.

Недоліками QKD є технічна складність та високі витрати на системи розгортання. Використання квантової технології для створення безпечних ключів вимагає спеціального обладнання, яке є досить складним у виготовленні та вимагає спеціальної експертизи для його обслуговування. Процес QKD вимагає прямої видимості між приладами, що означає, що він не підходить для захисту даних на великій відстані.

Отже, розвиток квантової криптографії має значний потенціал у майбутньому, він забезпечує безумовну безпеку, що робить її привабливою для захисту даних у важливих сферах.Одним із напрямів розвитку квантової криптографії є підвищення ефективності. Іншим напрямком розвитку квантової криптографії є пошук нових методів захисту даних на основі квантової фізики, таких як квантова стеганографія, квантове шифрування та інші. Ці методи можуть забезпечити додатковий рівень безпеки та конфіденційності даних. Крім того, квантова криптографія може бути використана для захисту від майбутніх квантових комп'ютерів, які здатні розгадувати складні криптографічні алгоритми, які сьогодні використовують. Квантова криптографія може стати елементом забезпечення безпеки майбутнього квантового Інтернету.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Nielsen, Michael A. ta Chuang, Isaac L. "Quantum enumeration and quantum information",Cambridge University Press, 2010.