Contribution ID: **285** Type: **Усна**

ПЕРСПЕКТИВИ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

Abstract

Сучасна криптологія виділяє проблемні задачі повного розкриття, пов’язані з можливостями використання методів та алгоритмів квантового криптоаналізу [1]. Особливість квантових комп’ютерів полягає в тому, що для виконання обчислень вони використовують такі фізичні ефекти, як суперпозиція станів і сплутування. В даний час їх продуктивність набагато нижче, ніж у стандартних комп’ютерів. Однак деякі алгоритми перевершили стандартні комп’ютери у швидкодії в 100 млн. разів [2]. Важливою властивістю квантових об’єктів є можливість здійснювати паралельні операції. Так, для системи із N кубітів, що перебуває в переплутаному стані, ефективно кодується відразу 2N чисел. Тому операція над такою системою, завдяки когерентності станів різних кубітів, впливає на всі доданки в сумі і це дозволяє обробляти відразу всі 2N чисел. Це може привести до злому протоколів безпеки, заснованих на криптографічних алгоритмах.

Contact Phone

Primary authors: ТЕЛІЖЕНКО, О.Б. (Інститут СЗРУ); CHETVERIKOV , Ivan

Presenter: ТЕЛІЖЕНКО, О.Б. (Інститут СЗРУ)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України