Назва:

Квантове розподілення таємних ключів шифрування – новітня технологія криптографічного захисту інформації

Короткий опис:

Коротко розглядаються основні фізичні принципи, які лежать в основі квантових технологій захисту інформації (квантової криптографії). Надається характеристика основним напрямам сучасної квантової криптографії.

Детально розглядається один з напрямів квантової криптографії – квантові протоколи розподілення ключів. На сьогодні це єдиний напрям квантової криптографії, що реалізований не тільки у лабораторних умовах, а і використовується для розподілення таємних ключів у системах шифрування в багатьох розвинених країнах світу.

Розглядаються основні види квантових протоколів розподілення ключів з дискретними квантовими станами, зокрема протокол BB84, протокол з 6-ма станами та протокол Екерта. Показується стійкість цих протоколів до простої атаки «перехоплення – повторної посилки кубітів».

Наводиться загальна класифікація атак на квантові протоколи розподілення ключів та надаються основні характеристики атак. Наводяться результати досліджень стійкості до різних атак (зокрема, некогерентних атак та атаки поділу числа фотонів) протоколів BB84 і з 6-ма станами та узагальнень цих протоколів на багатовимірні квантові системи. Аналізується стек квантових протоколів розподілення ключів.

Наводяться відомості щодо існуючих на сьогодні мереж квантового розподілення ключів.

Коротко розглядаються основні переваги та недоліки квантових протоколів розподілення ключів.

Відомості про доповідача:
Василіу 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 (Одеса)