УДК 003.26:621.39+530.145

Є.В. ВАСІЛІУ
Державний університет інтелектуальних технологій і зв'язку, Одеса, Україна,
e-mail: *y.v_vasiliu@suitt.edu.ua*, *ye.vasiliu@gmail.com*.

СУЧАСНІ КВАНТОВІ ТЕХНОЛОГІЇ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. 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. У роботі наведено загальний огляд та аналіз сучасних квантових технологій захисту інформації, зокрема протоколів квантового розподілення ключів, квантового прямого безпечного зв'язку, квантового розділення секрету. Стисло розглянуто декілька інших напрямів квантової криптографії, як-от: квантовий цифровий підпис, квантове бітове зобов'язання, квантова стеганографія тощо. Проаналізовано переваги та недоліки протоколів квантової криптографії, перспективи та проблеми їхнього практичного впровадження. Надано короткий огляд законів квантової фізики, на яких ґрунтується стійкість протоколів квантової криптографії.

Ключові слова: квантова криптографія, фізичні основи квантової криптографії, кубіт, кудит, переплутані кубіти та кудити, квантове розподілення ключів, квантовий прямий безпечний зв'язок, квантове розділення секрету.

ВСТУП

На сьогодні ключовим фактором, що впливає на національну безпеку держави, є рівень захищеності її інформаційного середовища. Актуальність інформаційної безпеки зростає як через стрімкий розвиток комп'ютерних технологій, так і внаслідок значного зростання кількості злочинних та інших протиправних дій, спрямованих на порушення конфіденційності, цілісності та достовірності даних. Важливу роль у гарантуванні інформаційної безпеки в сучасних інформаційно-комунікаційних системах (ІКС) відіграють криптографічні методи захисту інформації.

Квантова криптографія пропонує принципово новий підхід до безпеки ІКС, використовуючи принципи квантової механіки, і тим самим надає рішення, які захищають передавання даних у спосіб, що є принципово безпечнішим, ніж класична криптографія. Традиційні криптографічні системи, зокрема RSA та криптографія на основі еліптичних кривих, спираються на обчислювальну складність таких задач, як розкладання цілих чисел на множники та задача дискретного логарифмування. Однак ці класичні методи потенційно вразливі для квантових комп'ютерів, які могли б ефективно розв'язувати ці задачі за допомогою таких алгоритмів, як алгоритм Шора [1], створюючи загрозу для поточної інфраструктури безпеки.

На відміну від класичної криптографії, яка спирається на обчислювальну складність, квантова криптографія ґрунтується на законах фізики, зокрема на таких принципах квантової механіки, як суперпозиція, переплутаність і теорема про заборону клонування. Ці квантові явища дають змогу за певних умов створювати криптографічні системи з теоретико-інформаційною стійкістю, пропонуючи нові способи забезпечення конфіденційності, цілісності та автентичності передаваних даних.

На сьогодні одним із основних квантових методів захисту інформації є квантове розподілення ключів (КРК), яке дає змогу двом сторонам, Алісі та Бобу, безпечно обмінюватися таємними криптографічними ключами через незахищений канал зв'язку [2–4]. Крім КРК, до складу квантових технологій захисту інформації входять: квантовий прямий безпечний зв'язок, який являє собою захищений від підслуховування зв'язок без потреби у використанні спільного секретного ключа, а також квантове розділення секрету, квантовий потоковий шифр, квантовий цифровий підпис та квантова стеганографія. Детальний огляд сучасного стану теоретичних досліджень та практичного впровадження деяких