УДК 004.056

О.К. Конопліцька-Слободенюк[1]
Кіровоградський національний технічний університет

Перспективи розвитку квантової криптографії

Вступ. Те, що інформація має цінність, люди усвідомили дуже давно. Захист від витоку конфіденційної інформації до неавторизованих осіб є однією з найважливіших проблем сучасного інформаційного суспільства.

Основна частина. Виниклий в середині 80-х років XX століття новий напрям захисту інформації в телекомунікаційних мережах, що отримав назву квантової криптографії, швидко розвивається в останнє десятиріччя . Одним з напрямів квантової криптографії є квантовий безпечний прямий зв'язок, де легітимні користувачі обмінюються квантовими частками по квантовому каналу зв'язку і виконують певні операції і вимірювання над цими частками, а також обмінюються додатковою інформацією по звичайному (не квантовому) каналу зв'язку з автентифікацією. Практично в якості квантових часток використовують фотони, а як квантові канали – оптоволоконні лінії зв'язку. При цьому безпека передачі інформації з використанням квантових протоколів безпечного зв'язку гарантується законами квантової фізики. Використовуючи квантові явища, можна спроектувати і створити таку систему зв'язку, яка завжди може виявляти підслуховування. Це забезпечується тим, що спроба виміру взаємозв'язаних параметрів в квантовій системі вносить до неї порушення, руйнуючи вихідні сигнали, а значить, по рівню шуму в каналі легітимні користувачі можуть розпізнати міру активності перехоплювача.

Найпростішим способом знімання інформації у звичайних оптичних телекомунікаційних мережах є розділення пучка фотонів. Однак у протоколах квантової криптографії передавання повинно відбуватися за допомогою одиночних фотонів, і в такому випадку порушник не може відвести частину сигналу. Тому, подібні методи перехоплення інформації не можуть бути застосовані у системах квантової криптографії в ідеальних умовах однофотонних сигналів (до того ж, такі джерела сигналів поки що не створені). На практиці наразі використовують слабкі когерентні імпульси, випромінювані лазерними світлодіодами. Число фотонів в імпульсі визначається розподілом Пуассона, тобто частина переданих імпульсів містить два й більше фотони.

Висновки. Нині одним з найважливіших досягнень в області квантової криптографії є те, що вчені змогли показати можливість передачі даних по квантовому каналу з швидкістю до 1 Мбіт/с. Це стало можливо завдяки технології розділення каналів зв'язку по довжинах хвиль і їх одноразового використання в загальному середовищі. Що до речі, дозволяє одночасне використання як відкритого, так і закритого каналу зв'язку. Експериментальні дані дозволяють зробити прогноз на досягнення кращих параметрів в майбутньому.

[1] викладач кафедри програмного забезпечення