УДК 004.056.55
Зайко Т.А.[1], Івахненко Б.О.[2]
[1]канд. техн. наук, доц. НУ «Запорізька Політехніка»
[2]студ. гр. КНТ-118 НУ «Запорізька Політехніка»

КВАНТОВА КРИПТОГРАФІЯ

Для вирішення завдань збереження даних нам необхідний найсучасніший метод криптографічного шифрування. Таким методом є квантова криптографія.

Технологія квантового розподілу криптографічних ключів вирішує одну з основних завдань криптографії – гарантоване на рівні фундаментальних законів природи розподіл ключів між віддаленими користувачами по відкритих каналах зв'язку

Вперше ідея захисту інформації за допомогою квантових об'єктів була запропонована Стівеном Візнер в 1970 році. Через десятиліття Чарльз Беннет і Жиль Брассар запропонували передавати особистий ключ з використанням квантових об'єктів, ними була запропонована схема BB84.

До початку чергового раунду генерації сеансового ключа передбачається, що у Аліси і Боба, як учасників протоколу, є:

– квантовий канал зв'язку;

– класичний канал зв'язку.

Протокол гарантує, що втручання зловмисника в протокол можна помітити аж до тих пір, поки зловмисник не зможе контролювати і на читання, і на запис всі канали спілкування відразу.

Протокол складається з трьох частин:

– передача і прийом фотона по квантовому каналу зв'язку від Аліси до Боба;

– передача Бобом інформації про використані анализаторах;

– передача Алісою інформації про збіг обраних аналізаторів і вихідних поляризаций.

Далі Беннет запропоновал для реєстрації змін в переданих за допомогою квантових перетворень даних використовувати наступний алгоритм:

– відправник і одержувач домовляються про довільній перестановці бітів в рядках, щоб зробити положення помилок випадковими;

– рядки діляться на блоки розміру k (k вибирається так, щоб ймовірність помилки в блоці була мала);

– для кожного блоку відправник і одержувач обчислюють і відкрито сповіщають один одного про отримані результати. Останній біт кожного блоку видаляється;

– для кожного блоку, де парність виявилася різною, одержувач і відправник виробляють ітераційний пошук і виправлення невірних бітів.

– щоб виключити кратні помилки, які можуть бути не помічені, операції попередніх пунктів повторюються для більшого значення k;

– якщо відмінностей немає, після m ітерацій одержувач і відправник отримують ідентичні рядки з ймовірністю помилки 2-m.

Схема реалізація односпрямованого каналу з квантовим шифруванням показана на рис. 1. Передавальна сторона знаходиться зліва, а приймаюча - справа. Осередки Покеля служать для імпульсної варіації поляризації потоку квантів передавачем і для аналізу імпульсів поляризації приймачем. Передавач може формувати одне з чотирьох станів поляризації (0, 45, 90 і 135 градусів). Власне передані дані надходять у вигляді керуючих сигналів на ці осередки. В якості носія даних може використовуватися оптичне волокно. В якості первинного джерела світла можна використовувати і лазер.

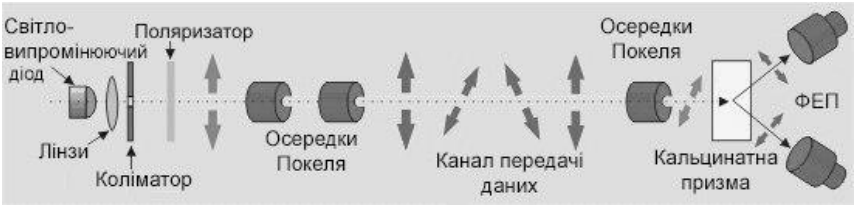

Рисунок 1 – Реалізація односпрямованого каналу з квантовим шифруванням

На приймаючій стороні після осередки Покеля ставиться каліцтва призма, яка розщеплює пучок на два фотодетектора (ФЕУ), що вимірюють дві ортогональні складові поляризації. При формуванні переданих імпульсів квантів доводиться вирішувати проблему їх інтенсивності. Якщо квантів в імпульсі 1000, є ймовірність того, що 100 квантів по шляху буде відведено зловмисником на свій приймач. Аналізуючи пізніше відкриті переговори проміжній стороною, він може отримати потрібну йому інформацію. В ідеалі число квантів в імпульсі має бути близько одного. Тут будь-яка спроба відводу частини квантів зловмисником призведе до істотного зростання числа помилок у приймаючої сторони. В цьому випадку прийняті дані повинні бути відкинуті і спроба передачі повторена. Але, роблячи канал більш стійким до перехоплення, ми в цьому випадку стикаємося з проблемою "темнового" шуму (видача сигналу в відсутності фотонів на вході) приймача (адже ми змушені підвищувати його чутливість). Для того щоб забезпечити

надійне транспортування даних логічного нуля і одиниці можуть відповідати певні послідовності станів, що допускають корекцію одинарних і навіть кратних помилок.

Подальшого поліпшення надійності криптосистеми можна досягти, використовуючи ефект EPR (Einstein-Podolsky-Rosen).

На даному етапі квантова криптографія тільки наближається до практичного рівня використання.