

КВАНТОВА КРИПТОГРАФІЯ. ДОСЛІДЖЕННЯ І РЕАЛЬНІСТЬ

Михалевич О. В.

Науковий керівник – проф., д. т. н., Лужецький В. А.

Стан квантового об'єкту (тобто, грубо кажучи, об'єкту дуже малої маси і розмірів, наприклад, електрона або фотона) може бути визначене вимірюванням. Проте відразу після виконання цього вимірювання квантовий об'єкт неминуче переходить в інший стан, причому передбачити цей стан неможливо. Отже, якщо як носії інформації використовувати квантові частинки, то спроба перехопити повідомлення приведе до зміни стану частинок, що дозволить виявити порушення секретності передачі. Крім того, неможливо отримати повну інформацію про квантовий об'єкт, і отже, неможливо його скопіювати. Ці властивості квантових об'єктів роблять їх «невловимими».

Носіями інформації в протоколі BB84 є фотони, поляризовані під кутами 0, 45, 90, 135 градусів. Відповідно до законів квантової фізики, за допомогою вимірювання можна розрізнити лише два ортогональні стани: якщо відомо, що фотон поляризований або вертикально, або горизонтально, то шляхом вимірювання, можна встановити - як саме; те ж саме можна затверджувати щодо поляризації під кутами 45 і 135 градусів. Проте з достовірністю відрізнити вертикально поляризований фотон від фотона, поляризованого під кутом 45°, неможливо. Поляризація – надання фотону швидкості и напрямку обертання навколо своєї осі! Ці особливості поведінки квантових об'єктів лягли в основу протоколу квантового розповсюдження ключа. Щоб обмінятися ключем, Аліса і Боб роблять наступні дії:

Аліса посилає Бобу фотон в одному з поляризованих станів (0, 45, 90, 135 градусів) і записує кут поляризації. Відлік кутів ведеться від напрямку "вертикально вгору" за годинниковою стрілкою. У реальних же системах перед процесом передачі ключа устаткування спеціально юстирується для забезпечення однакового режиму відліку на приймачі і передавачі (причому це юстирування доводиться проводити періодично в процесі передачі), а "просторове розташування" початку відліку кута -- неістотно.

Боб має в своєму розпорядженні два аналізатори: один розпізнає вертикально-горизонтальну поляризацію, інший - діагональну. Для кожного фотона Боб випадково вибирає один з аналізаторів і записує тип аналізатора і результат вимірювань. По загальнодоступному каналу зв'язку Боб повідомляє Алісу, які аналізатори використовувалися, але не повідомляє, які результати були отримані. Аліса по загальнодоступному каналу зв'язку повідомляє Боба, які аналізатори він вибрав правильно. Ті фотони, для яких Боб невірно вибрав аналізатор, відкидаються.