Photon as qubits

The energy associated with light is quantized in units of \( h \), where \( h \) is Planck's constant. A photon is a quantum particle of light, and its energy is given by \( E = hf \), where \( f \) is the frequency of light in Hertz. Each photon is a qubit called a "photon".

If we take a set of wires containing different numbers of electrons (states 0 or 1), and classical waves of light (states 0 or 1), we can learn that this analogy is correct for quantum computers. A single photon is actually a real level system just as a qubit.

Quantum communication: Each photon transmitted on an optical fibre sends one bit of information

- But how to send security? They can use "ephemeral key" communication. Hunt Alice and Bob and send a photon in a box - which could be done by laser beams.
- Alice encodes her message M by transmitting M. Bob knows the key E and he can decode for message M.
- The method's 100% secure against eavesdropping. Bob just reads for the first bit is transmitted. If he sends another message \( M' \), then Eve can eavesdrop, but in (B, M') she can choose another message coding to break down in \( M, M' \).

Quantum key distribution: BB84 protocol (Bennet, Brassard 1984)

- Problem: How can Alice and Bob share a key remotely without allowing Eve to learn the key? Quantum mechanics provides a 100% secure mechanism that allows them to do just that.

BB84

- After Bob receives all the qubits, he measures his sequence of 0s and 1s. Alice sends her choices to Bob. Alice can send 0 or 1 to indicate the type of basis used by Alice.
- As each qubit arrives, Bob remembers whether the basis in the type 1 or type 2 (with or in a polarized) or in the type 3 or type 4 (10 basis).
- Security against Eve

- Alice virtually switched between type 1 and type 2 to provide security against Eve. If Eve had interfered them up above it would have acquired the same type of information as Bob without being detected (provided Eve was of type 1).
- With Alice switching randomly, the basis that can do this to make random in type 1 and type 2 (just like Bob), and then sending their own. Once Eve knows the sequence of interference cubes does Alice agreed upon, only an unknown "half" of her measurements are in agreement with Alice's choice (type 1 or 2). On average half of the positions (p) will be "corrupted" by Bob's measurement, so in a box is a code for Bob and with Alice's choice. Eve has never been intercepted, but her method is in itself a way to check for this.
- The number is 50% (Eve would be able to guess which basis Alice and Bob used. If more than 50% of them aren't agreed, they reject the signal, but this is very difficult to determine if Alice and Bob do nothing, they set an upper bound on the security of their channel.

Let's play the Alice-Eve-Bob game

- Before the talks by Apple and the competition between the main groups, there are two talks by Bob and Alice with the messages.

Assume Eve to be non-talking

- When the talks by Apple and the competition between the main groups, there are two talks by Bob and Alice with the messages.

Assume Eve to be listening

- When the talks by Apple and the competition between the main groups, there are two talks by Bob and Alice with the messages.

Quantum tomography

- See also Alice to have a unique qudit state (s, 4) with a complex of a Schmidt (C). The Schmidt component is the Schmidt component of the Schmidt (C).

- Each measurement she makes (after applying a unitary transformation of her choice) yields either 0 or 1 and destroys the possibility for her to learn the value of complex coefficients a at all. However, if she can create the state \( |\psi\rangle\) from any pure state, she can come up with the Schmidt (C). After doing this, she can see the Schmidt (C) and determine all the Schmidt (C).

Question: How many different bits she needs to measure on? (Bold question that marks)

- The process of approximating a is called quantum tomography. It's a very costly process.

Summary

- Single photons are flying qubits. They provide a practical means to do quantum communication. We have learned that this alternative state of a photon (or qudit) is very useful.
- Secure communication requires a private key, a random string of bits only known by the sender and the receiver. Quantum key distribution (QKD) provides an ingenious method for her to share a random string of bits that allows the sender and receiver to share their messages. With 100% security and ability to detect a possible eavesdropping event. Note: Quantum mechanics does not provide automatic communication of encoding and decoding - it only enables private communication of a random message.