量子密钥分发原理

马若般 19307110031

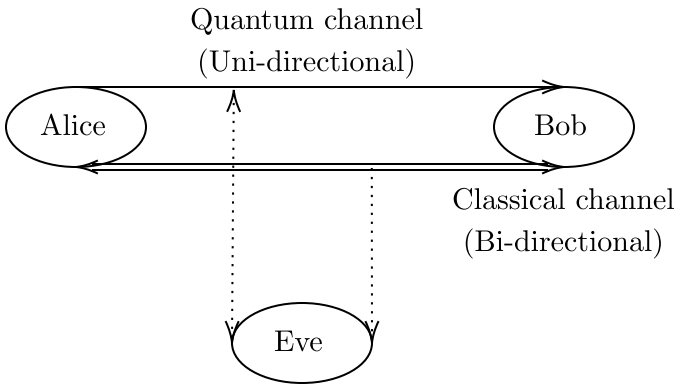
1. Quantum Key Distribution (BB84 Protocol)

References:

1. *Mikio Nakahara & Tetsuo Ohmi*. Quantum Computing: From Linear Algebra to Physical Realizations[M]. CRC Press, 2008: 60-62.

Quantum key distribution is a secure way of distributing an encryption and decyption key by making use of qubits. The sender and the receiver can detect a possible 3rd party eavesdropping their communication by comparing the sequence sent with the received one.

Now we introduce one of the QKD ways called BB84 protocol, which is a pratical use of
single qubits.



Drawing 1: Quantum key distribution (BB84 protocol).

Suppose Alice wants to send Bob a one-time pad key to encode and decode her secret message. Alice can send Bob photons through a uni-directional quantum channel, and there is also a bi-directional classical channel between them. 2 coding systems can be employed for the photons:

$$\text{coding system (1):} \quad 0 \mapsto |\updownarrow\rangle,\ 1 \mapsto |\leftrightarrow\rangle,$$
$$\text{coding system (2):} \quad 0 \mapsto |AD\rangle,\ 1 \mapsto |D\rangle,$$

where $|AD\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle + |\leftrightarrow\rangle\right)$ and $|D\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle - |\leftrightarrow\rangle\right)$. These four states represents four different linear polarized states of photons.

1. Alice chooses one of the 2 coding systems randomly for each photon and Bob also does so independently of Alice to measure the photons. Suppose $4N$ photons are sent from Alice to Bob through the quantum channel.
2. After all the photons has been sent, Alice and Bob exchange the sequence of coding systems they employed through the classical channel.
3. They discard the cases for which they employed different coding systems. In all $4N$ cases, $\sim 2N$ cases should be discarded, so $\sim 2N$ cases are still left, and for these cases Alice and Bob employed the same coding system.

4. To make sure that the quantum channel has not been eavesdropped, Alice and Bob exchange N of the $2N$ bits still left through the classical channel.
   (a) If there is no eavesdropper, these N bits should all be the same.
   (b) If an eavesdropper Eve is in action, and after eavesdropping the photons, she immediately sends Bob her results in order to hide her presense. Suppose for a photon, Alice employs coding system (1) and sends 0:
      i. If Eve uses coding system (1) (probability 1/2) and gets the outcome 0, then Bob is certain to get the outcome 0. The probability of this situation is 1/2.
      ii. If Eve uses coding system (2) (probability 1/2), then whatever outcome Eve gets, Bob may get the outcome 0 with probability 1/2. The probability of this situation is 1/4.
      iii. If Eve uses coding system (2) (probability 1/2), then whatever outcome Eve gets, Bob may get the outcome 1 with probability 1/2. The probability of this situation is 1/4.

   Therefore, there is a probability of 1/4 that the photons Alice sends disagrees with the photons Bob receives. Therefore Alice and Bob will know that the quantum channel has been eavesdropped, so they change a quantum channel and repeat the procedures above again until they verifies their safety.
5. After Alice and Bob verifies their safety, they discard the N bits exchanged in step 4 and use the remaining N bits to generate a one-time pad key.