Simulations of Quantum Cryptography

Bennett-Brassard Quantum Key Distribution Protocol (1984)

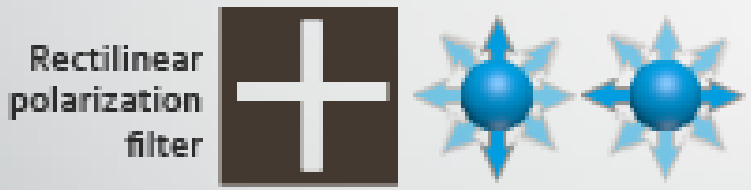
Context

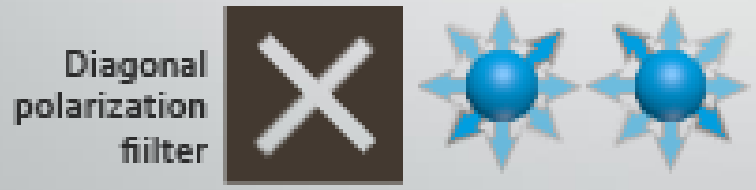
- Alice and Bob want to send secret messages. They decide to use the Bennett-Brassard protocol to determine a secret quantum-cryptographic key that will allow them to encrypt their messages in a highly secured way.

How do they determine this key?

1

Alice sends photons through either the 0 or the 1 slot of the rectilinear or diagonal polarizing filters. She writes down the various orientations of the photons she sends.





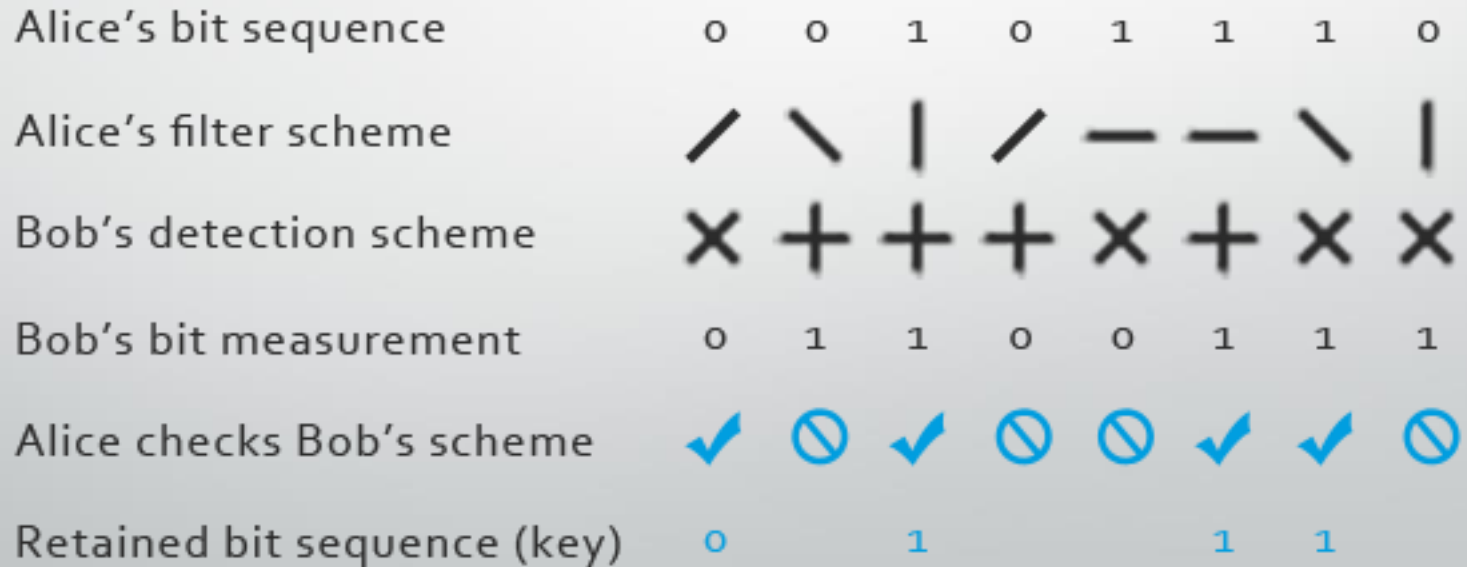
Bit value	0	1

For every photon he receives, Bob chooses a filter and uses it to detect the photon. He writes down the filter he uses and the bit value he measures.

2

3 Once Bob has received all the photons, he uses a public channel to tell Alice which filter he used to measure every photon.

4 Alice tells Bob which filter he uses correctly. The bits corresponding to the photons that have been correctly measured will be used to form the key.



What if someone is trying to eavesdrop on Alice and Bob?

- Eve the eavesdropper has only rectilinear and diagonal filters and does not know which filter Alice used to polarize a photon. She randomly chooses one filter:
  - She chooses the correct filter (50% chance)
  - She chooses the wrong filter (50% chance)

- The probability an intercepted photon generates an error in the key equals :

$$50\% * 50\% = 25\%$$

(Eve choosing the wrong filter X Bob's bit measurement being wrong)

How can Alice and Bob protect their key from Eve?

- Once Alice has checked Bob's detection scheme, they have to « sacrifice » a part of their bits to test the key's security. They share, on a public channel, the value of random bits.
  - No error found
  - Error found

- *N.B : Sacrificing only 10 bits gives 94% chance of detecting Eve*

$$1 - \left(\frac{3}{4}\right)^{n}$$, *n being the number of bits sacrificed*

Symbols we will use during our simulation