Quantum Key Distribution

Public Key Cryptography

✓ Polarization is a quantum Mechanical ~~shape~~ property

✓ Photon can be in a superposition state of two mutually exclusive outcomes. By measuring it collapses to one state

⇒ By Intruder can be detected if any of the photons in stream get collapsed → Eves dropper. Cannot measure without disturbing them.

BB84 Protocol — Bennet & Brassard 1984 — E91

Rectilinear basis + → 0 ↑ 1

Diagonal basis × ↗ 0 ↖ 1

Photons are easy to generate with a commercial laser.

✓ Both Alice and Bob choose Bases and Bits randomly.

- whatever bit Alice send, Bob ~~get~~ for sure accurately received if two basis are same
- If two bases are different, the measurement is useless.
- The sequence of Bases used by Alice and Bob will be shared publicly, a priori
- Interceptor can get the bases but not the bits themselves.
- Only Alice and Bob knows the bits. It is one time key
- Both Alice & Bob has Common Secret Key
- To establish an n bit key, a total of 2n bits have to be sent. as the prob. of using the same bit orientation is 50%
- BB84 is a perfect, secure Protocol

Alice and Bob communicate through public quantum channel as well as Public classical channel.

How eavesdropping is detected:

Photons are the smallest unit and cannot be divided further. If a photon is intercepted by an eavesdropper, the # of photons that reach the receiver will be reduced.

Eavesdropper do not knows the transmission basis of the sender.

Further, when a photon is observed, its state changes; so that photon returned from eavesdropper will differ from the original.

Transmissing End	Trans bits	0 0 1 0 1 0 1 0 1 1 0
	Trans basis	× + × + × + + × × × +
	Trans. info	↗ → ↖ → ↖ → ↑ ↗ ↖ ↖ →
Receiving End	Measuring basis	+ + × × + + × + × × ×
	Recd. Result	↖ → ↖ ↗ ↗ → ↖ ↑ ↖ ↖ ↗
	Recd bits	1 0 1 0 0 0 1 1 1 1 0
Basis Match		N Y Y N N Y N N Y Y N
Derived Key		0 1 0 1 1

The derived key is 01011

How to check eavesdropping:

Alice and Bob compare a subset of their raw key. If they find discrepancies, they calculate the QBER. If QBER is below the threshold, they proceed by carrying out error correction.