QuiqSafe

Quantum Encryption Application

$(\mathcal{RS})^2$

IQuHackathon Quantum Encryption challenge

Outline

What does QuiqSafe do?

- An instant group messaging application equipped with quantum key distribution to protect your messages being read by someone else
- Application runss on BB84 protocol

BB84 protocol

- BB84 is a quantum key distribution scheme
- Developed by **Charles Bennett** and **Gilles Brassard** in 1984.
- The first quantum cryptography protocol.

Basis

- Binary 0 $\Rightarrow$ polarization of 0 degrees in the rectilinear bases or 45 degrees in the diagonal bases
- Binary 1 $\Rightarrow$ 90 degrees in the rectilinear bases or 135 in diagonal bases.

Protocol(First phase)

Alice chooses a random string of bits

$\Downarrow$

Alice encodes the bit with randomly choose a basis(rectilinear or diagonal)

$\Downarrow$

Alice transmits a photon to Bob for each bit with the corresponding polarization

$\Downarrow$

Bob measures each received photon's polarization by a randomly chosen basis

Protocol(Second phase)

Bob notifies Alice over any insecure channel what basis he used to measure each photon

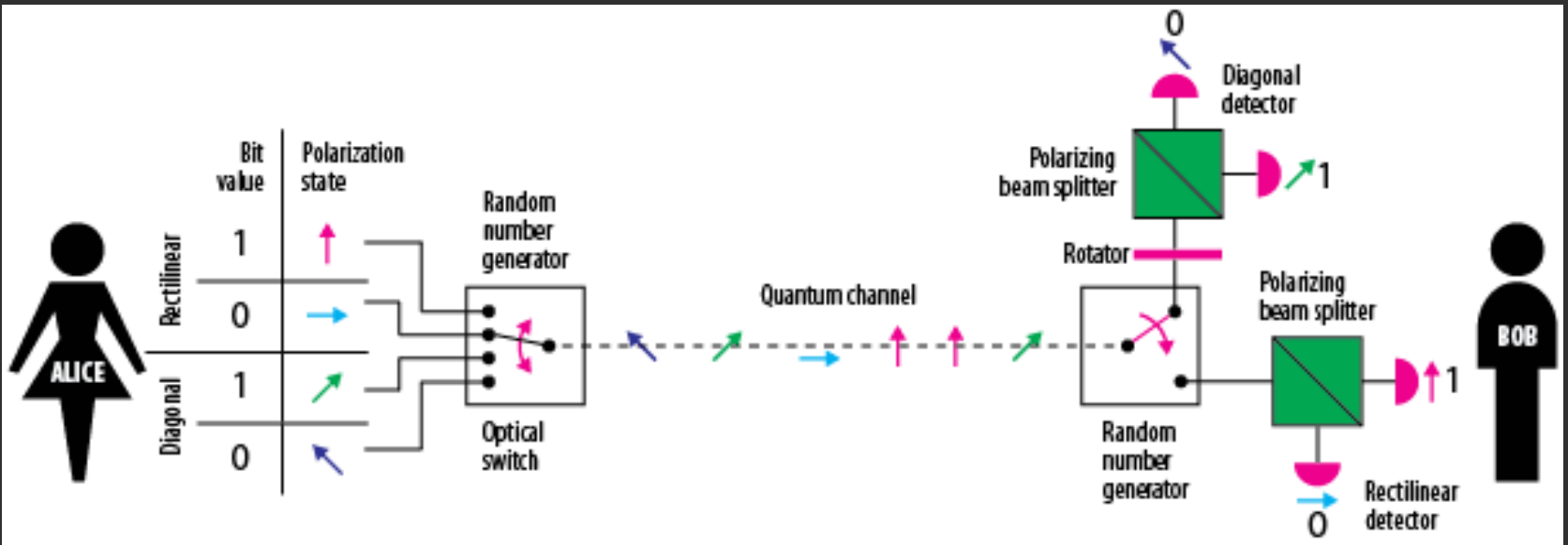
$\Downarrow$

Alice reports back to Bob whether he has chosen the correct basis for each photon

$\Downarrow$

Alice and Bob discard the bits corresponding to the photons which Bob measured with a different basis

Shifted key



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✔		✔		✔	✔	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

Eavesdropper Eve

- No cloning theorem $\Rightarrow$ Eve has to measure the photons sent by Alice before sending them on to Bob.
- Heisenberg principle $\Rightarrow$ Eve cannot the message sent by Alice by guessing the encoding basis.

The End