02/11/22

Quantum Key Distribution

Two basics of QKD

Bennet - Blassand 1984 → BB84

Bennet 1992

Goal: Generating a common secret

share a quantum

A ~~~~~~~~~~ B

channel

One-time pad: $S_1 \dots S_N$

Message of A: $M_1 \dots M_N \in \{0,1\}^N$

A "encodes" her message: $M_i' = M_i \oplus S_i \in \{0,1\}$

A sends $M_1' \dots M_N'$ to Bob

B receives $M_1' \dots M_N'$ and decodes

$$M_i' \oplus S_i = \boxed{M_i}$$

BB84 Protocol

1) "Encoding" Phase in A Lab.

2) "Decoding" Phase in B Lab.

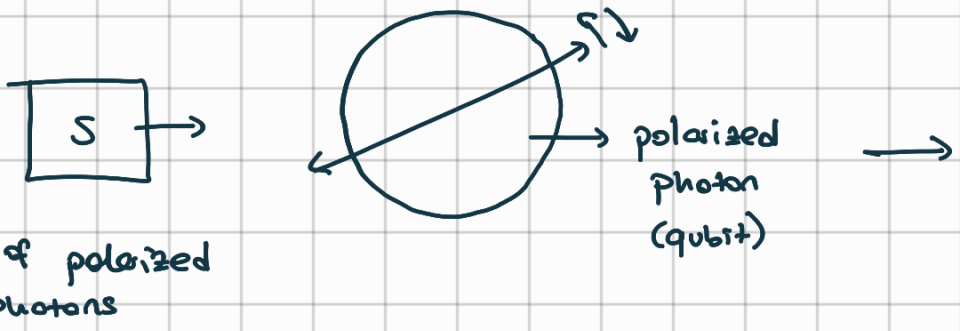
3) Public communication phase

4) One-time pad generation + Security test

Phase 1: A-Lab

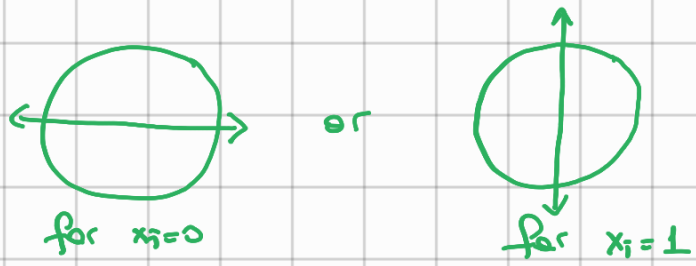
$e_1 e_2 \ldots\ldots e_N \in \{0,1\}^N$ $\quad prob(e_1 = \begin{matrix}0\\1\end{matrix}) = \frac{1}{2}$

$x_1 x_2 \ldots\ldots x_N \in \{0,1\}^N$ $\quad prob(x_i = \begin{matrix}0\\1\end{matrix}) = \frac{1}{2}$



Source of polarized photons

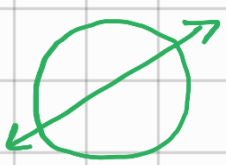
If $e_i = 0$ Alice pol. the photon in $|H\rangle$ or $|V\rangle$ states



State that goes to Bob is $|x_i\rangle = \{|0\rangle, |1\rangle\}$

These are state of computational basis or of 2 basis

If $e_i = 1$ Alice pol. the photon



for $x_i = 0$ for $x_i = 1$

states: $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

↓

X basis (Hadamard basis)

Phase 2. B Lab

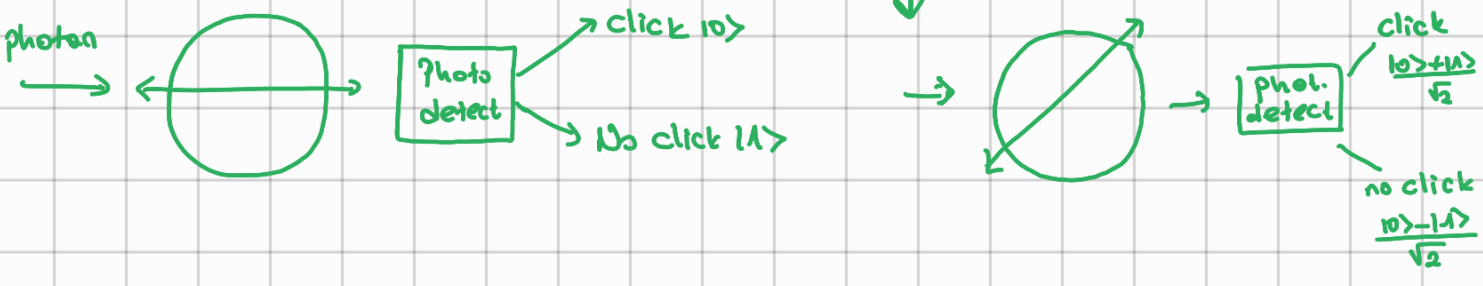
Bob receives at each instant, $i = 1 \dots N$

are of 4 states $|0\rangle$, $|1\rangle$, $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

Generate a random iid sequence $d_1 \dots d_N$ $\text{prob}(d_1 = \frac{0}{1}) = \frac{1}{2}$

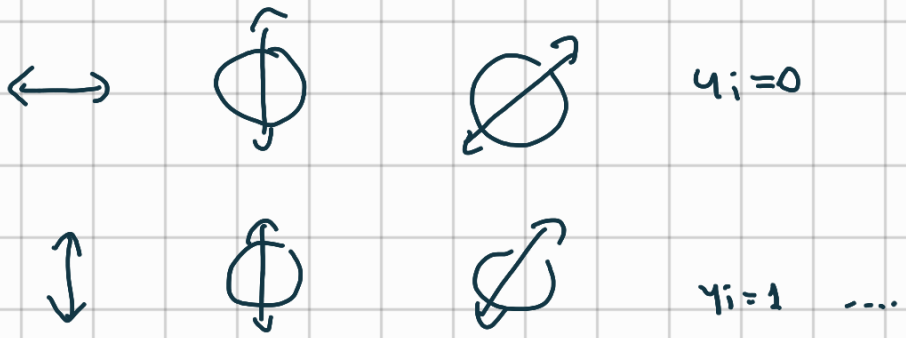
If $d_i = 0$ Measured basis + $\{|0\rangle, |1\rangle\}$

If $d_i = 1$ Measured basis X $\left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$



Records $\boxed{y_i = 0}$ if $|0\rangle$ or $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ are obtained (click)

$\boxed{y_i = 1}$ if $|1\rangle$ or $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ are obtained (no clic)



Phase 3 Public Communication Phase

→ A & B share a classical communication channel and reveal publicly $(e_1 \ldots e_N)$ & $(d_1, \ldots, d_N)$

→ Two possibilities <u>at most</u> $i = 1 \ldots N$

$e_i = d_i$ prob $(e_i = d_i) = \frac{1}{2}$

$e_i \neq d_i$ prob $(e_i \neq d_i) = \frac{1}{2}$

Lemma:

$$\text{Prob}(x_i = y_i \mid e_i = d_i) = 1$$
$$\text{Prob}(x_i \neq y_i \mid e_i = d_i) = 0$$
$$\text{Prob}(x_i = y_i \mid e_i \neq d_i) = 1/2$$
$$\text{Prob}(x_i \neq y_i \mid e_i \neq d_i) = 1/2$$

Consequence of lemma:

A & B select (→?) the bits x_i and y_i such that $e_i = d_i$.

And form the one-time pad with this subset of bits.

Average length of one-time pad is $\frac{N}{2}$

$$\{ x_i = y_i \mid e_i = d_i \}$$

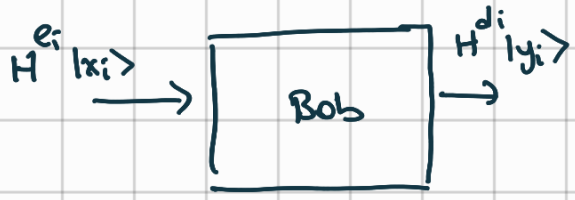
Proof of Lemma

Alice send a qubit to Bob : $H^{e_i} |x_i\rangle \in \left\{ |0\rangle, |1\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right\}$

Bob receives a perfect state and measures and gets

$$\{ \underbrace{|0\rangle, |1\rangle}_{\text{Z-basis, } d_i=0}, \underbrace{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}}_{\text{X basis, } d_i=1} \}$$

$\text{Prob}\left(\underbrace{H^{e_i}|x_i\rangle}_{\text{before meas.}} \longrightarrow \underbrace{H^{d_i}|y_i\rangle}_{\text{after meas.}} \right)$



$$= \left| \left(\langle y_i | H^{d_i} \right) \left(H^{e_i} | x_i \rangle \right) \right|^2$$

$$= \left| \langle y_i | H^{d_i} H^{e_i} | x_i \rangle \right|^2$$

→ $e_i = d_i$: H^0 or $H^2 = \mathbb{1}$

$$|\langle y_i | x_i \rangle|^2 = \begin{cases} 1 & \text{if } x_i = y_i \\ 0 & \text{if } x_i \neq y_i \end{cases}$$

→ $e_i \neq d_i$: $|\langle y_i | H | x_i \rangle|^2 = \frac{1}{2}$

$|\frac{1}{\sqrt{2}}|^2$

$$\langle 1 | H | 0 \rangle = \frac{1}{\sqrt{2}} (\langle 1 | 0 \rangle + \langle 1 | 1 \rangle) = \frac{1}{\sqrt{2}}$$

Phase 4 One-time pad generation

$\{ x_i = y_i \mid \text{with } i \text{ at } e_i = d_i \}$ → Avg length $= \frac{N}{2}$

Security test to assess what happens on the line

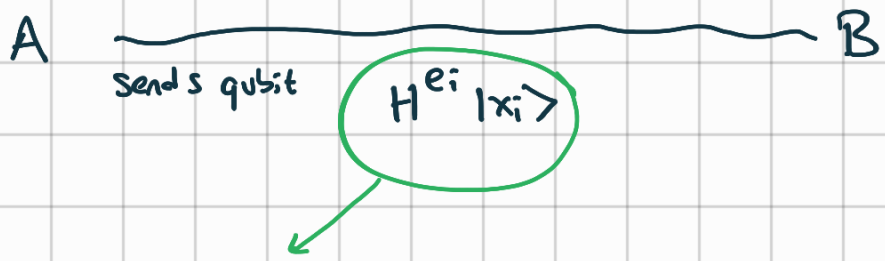
A & B sacrifies a fraction ε ($\varepsilon \ll 1$) of the one-time pad

Reveal publicly $\varepsilon \frac{N}{2}$ bits x_i & y_i from one-time pad

$$\frac{\#\{ i \text{ that are revealed for which } x_i = y_i \}}{\varepsilon \frac{N}{2}} \overset{\text{test}}{\simeq} 1$$

If test does not pass → Abort communication

Discuss attacks from Eavesdropper



① Measurement + send to Bob the results of Meas

$$\underset{Eve}{Prob}(x_i = y_i \mid e_i = d_i) = \frac{3}{4}$$

② Copy of State for late + send to Bob the orginal

$$x_i = y = y_i^{Eve} \; ??$$

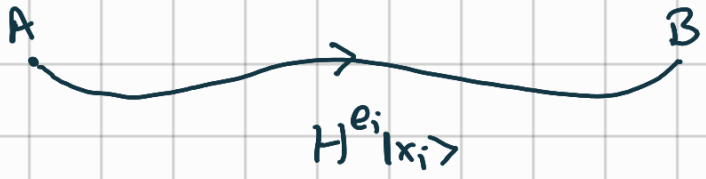
IMPOSSIBLE

to clone a collection of

non-orthogonal quantum states

03/11/22

Measurement Attack of Eavesdropper



Eve measures in same basis $E_i = 0, 1$ randomly

$E_i = 0$ measures in $\{|0\rangle, |1\rangle\}$ basis

$E_i = 1$ measures in $\{H|0\rangle, H|1\rangle\}$ basis

↳ | $|y_i^{Eve}\rangle \rightarrow$ Record $y_i^{Eve} = 0,1$

↳ $H|y_i^{Eve}\rangle \rightarrow$ Record $y_i^{Eve} = 0,1$

Eve has $y_1^{Eve}, y_2^{Eve}, \dots y_N^{Eve}$

Lemma: $\text{Prob}_{Eve}(x_i = y_i \mid e_i = d_i) = \frac{3}{4}$

$\text{Prob}_{Eve}(x_i \neq y_i \mid e_i = d_i) = \frac{1}{4}$

Proof: $E_i = e_i$ or $E_i \neq e_i$

y_i^{Eve} $\quad d_i = E_i$

$\text{Prob}(x_i = y_i \mid e_i = d_i, E_i = e_i)\, P(E_i = e_i) +$

$\text{Prob}(x_i \neq y_i \mid e_i = d_i, E_i \neq e_i)\, P(E_i \neq e_i)$

Eve needs $H^{E_i}|y_i^{Eve}\rangle$

→ $\text{Prob}(y_i = y_i^{Eve} \mid d_i = E_i) = 1$

$= 1 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$

Copy Attack of Eavesdropper

Eve generates $e_i = 0, 1$

$e_i = 0$ tries to copy state $|H^{e_i}|x_i\rangle$ with device 1 → success only if $e_i = 0$

$e_i = 1$ " " " " with device 2 → success only if $e_i = 1$

What does it mean to copy?

Device is a unitary Matrix $U: \mathcal{H} \otimes \underset{\text{storage}}{\mathcal{H}} \to \mathcal{H} \otimes \mathcal{H}$

$$U|\phi\rangle \otimes |\text{Blank}\rangle = |\phi\rangle \otimes |\phi\rangle$$

No cloning Theorem: $\exists U$ s.t this equality holds for non-orthogonal states.

Proof: $U|\phi_1\rangle \otimes |\underset{\text{blank}}{B}\rangle = |\phi_1\rangle \otimes |\phi_1\rangle$

$$\langle\phi_2| \otimes \langle B| U^+ = \langle \phi_2| \otimes \langle \phi_2|$$

$$\langle\phi_2| \otimes \langle B| U^+ U |\phi_1\rangle \otimes |B\rangle = \langle\phi_2| \otimes \langle\phi_2| \, |\phi_1\rangle \otimes |\phi_1\rangle$$

$$\langle \phi_2 | \phi_1 \rangle = \langle \phi_2 | \phi_1 \rangle^2 \quad \lightning$$

Contradiction