QKD : THE SETTING

Classroom exercise :

Some naïve solutions ?

- send key over classical channel ?
- send {random $|0\rangle, |1\rangle, |+\rangle, |-\rangle$} over quantum channel

  Bob says "I got them"

  then Alice reveals bases.

  Bob measures to get an answer.

Before we discuss the protocol, some notation

$|x\rangle_\theta$: State "x" in basis "θ". $\theta = 0$: computational, $\theta = 1$: Hadamard

So $|0\rangle_0 = |0\rangle$, $|1\rangle_0 = |1\rangle$, $|0\rangle_1 = |+\rangle$, $|1\rangle_1 = |-\rangle$

ALICE

BOB

Sample $x = x_1 x_2 \dots x_n$

$\theta = \theta_1 \theta_2 \dots \theta_n$

Set $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle \dots |\psi_n\rangle$

where $|\psi_i\rangle = |x_i\rangle_{\theta_i}$

QUANTUM CHANNEL

$|\psi\rangle = |\psi_1\rangle, |\psi_2\rangle \dots |\psi_n\rangle \longrightarrow$

Keeps $|\psi_1\rangle, |\psi_2\rangle \dots |\psi_n\rangle$

CLASSICAL CHANNEL

$\longleftarrow$ "I received n states"

CLASSICAL CHANNEL

$S \subseteq [n], |S| = \frac{n}{2}, \{x_i, \theta_i\}_{i \in S} \longrightarrow$

$\forall i \in S$, measure $|\psi_i\rangle$ in basis θ_i. Outcome $\tilde{x}_i$

If $\exists i \in S$ s.t. $x_i \neq \tilde{x}_i$, abort.

$\longleftarrow$ Else

CLASSICAL CHANNEL

$\longleftarrow$ "The check passed"

CLASSICAL CHANNEL

$\{\theta_i\}_{i \in [n] \setminus S} \longrightarrow$

$\forall i \in [n] \setminus S$, measure $|\psi_i\rangle$ in basis θ_i. Outcome $\tilde{x}_i$

OUTPUT Key $= \{x_i\}_{i \in [n] \setminus S}$

OUTPUT Key $= \{\tilde{x}_i\}_{i \in [n] \setminus S}$

ANALYZING QKD

Lets consider what happens from Eve's perspective.

Sample $x = x_1 x_2 \dots x_n$
$\theta = \theta_1 \theta_2 \dots \theta_n$

Set $|\Psi\rangle = |\psi_1\rangle|\psi_2\rangle \dots |\psi_n\rangle$
where $|\psi_i\rangle = |x_i\rangle_{\theta_i}$

QUANTUM CHANNEL
$|\Psi\rangle = |\psi_1\rangle, |\psi_2\rangle \dots |\psi_n\rangle \rightarrow$

→ to Bob
$|\Phi_1\rangle, |\Phi_2\rangle \dots |\Phi_n\rangle$
$|\tilde{\Phi}_1\rangle, |\tilde{\Phi}_2\rangle \dots |\tilde{\Phi}_n\rangle$

Keeps $|\tilde{\Phi}_1\rangle, |\tilde{\Phi}_2\rangle \dots |\tilde{\Phi}_n\rangle$

CLASSICAL CHANNEL
← "I received n states" (Bob)

CLASSICAL CHANNEL
$S \subseteq [n], |S| = \frac{n}{2}, \{x_i, \theta_i\}_{i \in S} \rightarrow$ (Alice)

$\forall i \in S$, Bob measures $|\Phi_i\rangle$ in basis θ_i. Outcome $\tilde{x}_i$

If $\exists i \in S$ s.t. $x_i \neq \tilde{x}_i$, abort

← Else

CLASSICAL CHANNEL
← "The check passed" (Bob)

CLASSICAL CHANNEL
$\{\theta_i\}_{i \in [n] \setminus S} \rightarrow$

$\forall i \in [n] \setminus S$, Bob measures $|\Phi_i\rangle$ in basis θ_i. Outcome $\tilde{x}_i$

OUTPUT Key = $\{x_i\}_{i \in [n] \setminus S}$

OUTPUT Key = $\{\tilde{x}_i\}_{i \in [n] \setminus S}$

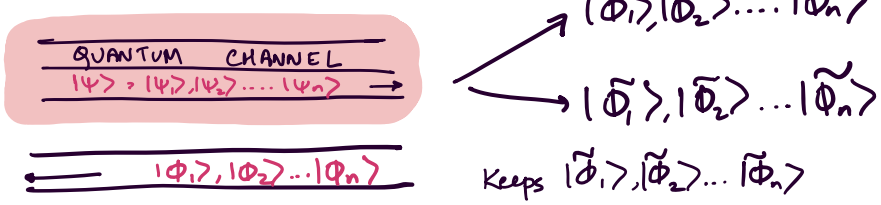
ANALYZING QKD

Lets consider what happens from Eve's perspective.

CHALLENGER
- ALICE + BOB

Sample $x = x_1 x_2 \dots x_n$
$\theta = \theta_1 \theta_2 \dots \theta_n$

Set $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle \dots |\psi_n\rangle$
where $|\psi_i\rangle = |x_i\rangle_{\theta_i}$



1. Pick $S \subseteq [n], |S| = \frac{n}{2}$
2. $\forall i \in S$, measure $|\phi_i\rangle$ in basis θ_i. Outcome $\tilde{x}_i$
3. If $\exists i \in S$ s.t. $x_i \neq \tilde{x}_i$, abort
4. Else output key $= \{x_i\}_{i \in [n] \setminus S}$

EQUIVALENTLY

(Changes from last slide in purple)

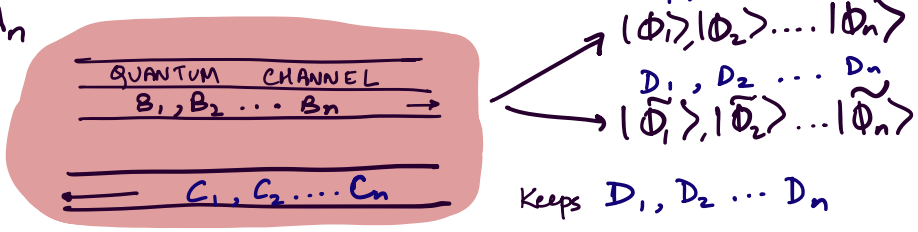
We will "defer" measurements.

CHALLENGER
- ALICE + BOB

Sample n EPR pairs

$(A_1, B_1), (A_2, B_2) \dots (A_n, B_n)$

Keep $A_1, A_2, \dots A_n$



1. Pick $S \subseteq [n], |S| = \frac{n}{2}$. Pick basis $\{\theta_i\}_{i \in S}$ at random.
2. $\forall i \in S$, measure $|\Phi_i\rangle$ in basis θ_i. Outcome $\tilde{x}_i$
3. If $\exists i \in S$ s.t. ~~$x_i \neq \tilde{x}_i$, abort~~ measuring $A_i \neq$ measuring C_i, abort.
4. Else ~~output key = $\{x_i\}_{i \in [n] \setminus S}$~~

   pick basis $\{\theta_i\}_{i \in [n] \setminus S}$ at random.

   Output key = $\{x_i\}_{i \in [n] \setminus S}$ where x_i is outcome of measuring A_i in basis θ_i.

EQUIVALENTLY

(changes from last slide in green)

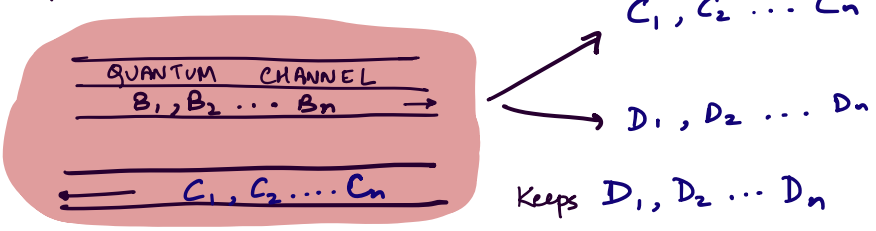
We will "defer" measurements.

CHALLENGER
- ALICE + BOB

Sample n EPR pairs

$(A_1, B_1), (A_2, B_2) \dots (A_n, B_n)$

Keep $A_1, A_2, \dots A_n$



1. Pick $S \subseteq [n], |S| = \frac{n}{2}$. Pick basis $\{\theta_i\}_{i \in S}$ at random

2. $\forall i \in S$, measure $|\Phi_i\rangle$ in basis θ_i. Outcome $\tilde{x}_i$

3. If $\exists i \in S$ s.t. ~~$x_i \neq \tilde{x}_i$, abort~~ measuring $A_i \neq$ measuring C_i, abort.

4. Else ~~output key = $\{x_i\}_{i \in [n] \setminus S}$~~

pick basis $\{\theta_i\}_{i \in [n] \setminus S}$ at random.

Output key = $\{x_i\}_{i \in [n] \setminus S}$ where x_i is outcome of measuring A_i in basis θ_i.

INTUITION: check passes iff $\forall i \in S$, (A_i, B_i) are EPR

Therefore, $\forall i \in [n] \setminus S$, most (A_i, C_i) are also EPR.

$\Rightarrow \{x_i\}_{i \in [n] \setminus S}$ are random from Eve's perspective.