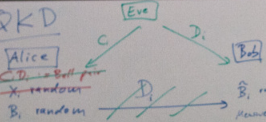
QKD

①



~~C_iD_i := Bell pair~~

~~x_i random~~

B_i random

~~$D_i := |x_i\rangle_{B_i}$~~

Measure C_i using B_i
$\rightsquigarrow x_i$

$\hat{B}_i$ random
measure D_i using $\hat{B}_i$
$\rightsquigarrow \tilde{x}_i$

exchange $B_i, \hat{B}_i$

compare 50% of $x_i \tilde{x}_i$

Remaining bits: Key

---

④

Fact: If $|\Psi\rangle$ is not close to being Bell pairs $\Longrightarrow$ Test fails with high probab.

Hence: When "Bell test" succeeds
$\Longrightarrow$ State C_iD_i close to Bell pairs
$\Longrightarrow$ Key is secure (monogamy)

---

②

Trick 1: Bell pair $\frac{1}{\sqrt{2}}|00\rangle + |11\rangle$

$$x_i \leftarrow \{0,1\} \qquad\qquad C_iD_i := \text{Bell pair}$$
$$B_i \leftarrow \{+,\times\} \quad \equiv \quad B_i \leftarrow \{+,\times\}$$
$$D_i := |x_i\rangle_{B_i} \qquad\qquad x_i := [\text{measure } C_i \text{ with } B_i]$$

Trick 2:

If proto is secure when Eve picks C_iD_i
$\Longrightarrow$ Proto secure when Alice picks C_iD_i

---

③

We abstract the structure of proto:

- Eve produces $|\Psi\rangle$
- Alice & Bob perform some randomized test
  Namely: For some random indices, check $C_i = D_i$ in random basis
- Alice & Bob use remainder

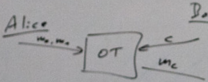
- What do we have?
  - ↳ Unconditionally secure key exchange
  - ↳ Use: Quantum channel + Authentic. channel
  - ↳ Authentic. channel via OT-MAC uncond.
  - ↳ Needs shared key infrastructure
- Idea: Use PKI for public key auth.

  ⟹ Not uncond. secure

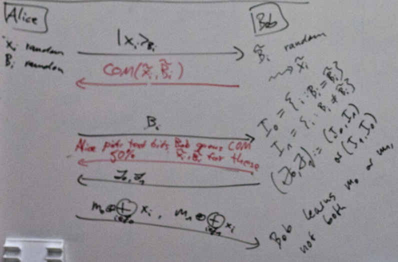
  But: LT-secure

⟹ Q-channel + PKI ⟹ LT-sec. confid. channels

Recall: OT



- Impossible classically LT-securely
- Quantum?



∴ Not secure!

↳ Bob can wait for B_i, measure $\tilde{x}_i$ only then

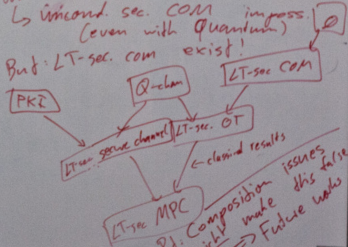
⟹ $x_i = \tilde{x}_i$ for all i

⟹ Bob learns all

⟹ Use COM

⟹ Secure.

- Where does COM come from?
  ↳ uncond. sec. COM imposs. (even with quantum)
- But: LT-sec. com exist!



- But: Composition issues might make this false
  ⟹ Future work