QKD

Alice  C.D. + Bell pair  \( \frac{\sqrt{2}}{\sqrt{1+1}} \)  100  11  \( x_i \)  0, 1

C, random
B, random

Bob  D_i  \( \hat{b}_i \)  random  measure D_i using \( \hat{b}_i \)

D_i  1x_i, \hat{b}_i

Eve  C

Fact: 14 is not close to being Bell pairs \( \Rightarrow \) Test fails with high probability.

Hence: When "Bell test" succeeds

\( \Rightarrow \) State C;D_i close to Bell pairs

\( \Rightarrow \) Key is secure (monogamy)

Trick 1: Bell pair  \( \frac{\sqrt{2}}{\sqrt{1+1}} \)  100  11

\( x_i \)  0, 1, 3
\( b_i \)  0, 1, 3
\( D_i \)  1x_i, \( \hat{b}_i \)

\( C, D_i \)  Bell pair

\( C_i, D_i \)  Bell pair

\( \hat{b}_i \)  measure C_i with \( \hat{b}_i \)

Trick 2:

If proto is secure when Eve
picks C;D_i

\( \Rightarrow \) Proto secure when Alice picks C;D_i

We abstract the structure of proto:

Eve produces 14

- Alice \& Bob perform some randomized test
- For some random indices, check C_i = D_i
- Alice \& Bob use remainder
What do we have?

- Unconditionally secure key exchange
- Use: Quantum channel + Authentic. channel
- Authentic. channel via OT-MAC uncond.
- Need shared key infrastructure.
  - Idea: Use PKI for public key auth.
    - Not uncond. secure
  - But: LT-secure

=> Q-channel + PKI => LT-see. confid. channels
Recall: OT

Alice → OT (B) → e → mc

- Impossible classically, LT-secure?
- Quantum?

Alice

Bob

|x, y| ← x, y, random

|c(x, y)| ← random

B, random

Alice publicly test bits Bob grown COM 50% for these

Bob leaves mc not look m, e

|TCP| ← PKC

Q-chan

LT-sec COM

LT-sec MPC

Not secure!

L ⇒ Bob can wait for Bi, measure xi, only then
 ⇒ x1 = x1 for all i
 ⇒ Bob learns all

⇒ Use COM

⇒ Secure.

Where does COM come from?
L ⇒ unconditional, COM impossible (even with quantum)

But: LT-sec. com. exist!

classical results

LT-sec. issues

Ph: Composition makes this false
⇒ Future useful