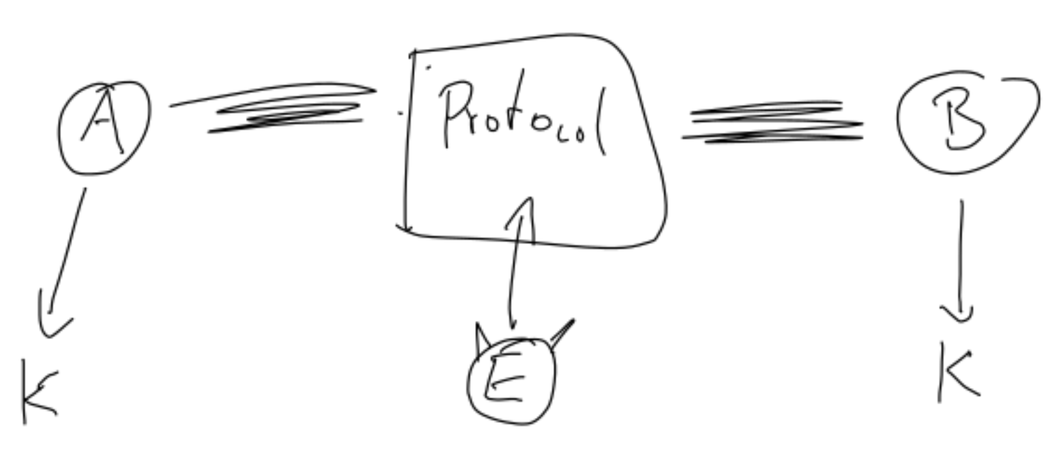
Lecture QC, April 7

Quantum Key Distribution



Want: Same K
Eve does not learn K

Classically?

G (think e.g. nums mod p), generator g

A picks a $\xrightarrow{g^a}$ B picks b

A $\xleftarrow{g^b}$ B

$(g^b)^a = g^{ab}$ $\qquad$ $(g^a)^b = g^{ab}$

Attacker that sees g^a, g^b cannot compute g^{ab} (under reasonable assm)

Drawbacks:

- Can be broken using Q computer
- Not secure against comp. unlimited adv.
  - ↳ Needs to rely on unproven assms.
  - ↳ This holds for all classical key exch. proto

Can a QKD proto avoid these limitations?

Yes!

QKD (BB84, Bennett, Brassard 1984)

(A) $|0\rangle\ |1\rangle\ |+\rangle\ |-\rangle$ (rand. chosen) → (B)
(q. channel)

(+ + × ×)

B guesses bases
Measure all

Eve: measures some qubits. With some prob: E measures in wrong basis ⇒ bit disturbed

"+" "+" "×" "×" →
(authenticated channel, after B received qubits)

Problems
- B knows ~$\frac{1}{2}$ of A's bits
- B does not know which

K = those bits that B meas. right ← ✓ no ✓ no (auth. channel) K := those bits that B measured right

"Fact:" If E measures a lot
⇒ A's key data ≠ B's key data

"Fact:" If E measures a little
⇒ E knows at most a few bits of K.

Need to add:
- A&B compare part of K over auth. channel.
- A&B do "privacy" amplification
  = postprocessing that transforms partially known data into unknown data.

How to define security?

~~Gen-t~~ General:
- "some event has small prob" → E.g. Pr[E guesses K] ≤ ε
- indistinguishability: E.g. Adv cannot distinguish two inputs
- real/ideal indistinguishability → Adv cannot dist. between A, B getting the key from QKD, or AB just getting a secret key from outside

---

Security def

Notation: For some adv E, for honest A, B, have:
- ρ^{real}_{ABE}: final joint state of A, B, E
- Pr[success]: prob. that A&B do not abort

Ideal scenario: What do we want ρ^{real}_{ABE} to look like?
- A&B have same key (random)
- E knows nothing

$E = \{|k\rangle \otimes |k\rangle, 2^{-n}\}_k$

$$\rho^{ideal}_{ABE} = \Big(\sum_{k\in\{0,1\}^n} 2^{-n} |k\rangle\langle k| \otimes |k\rangle\langle k|\Big) \otimes \rho_E \quad \text{(for some } \rho_E)$$

Bad: ~~$\sum_k |k\rangle\langle k| \otimes |k\rangle\langle k| \otimes |k\rangle\langle k|$~~

$$S_{ideal} = \Big\{ \sum_k 2^{-n} |k\rangle\langle k| \otimes |k\rangle\langle k| \otimes \rho_E \ : \ \rho_E \text{ density op} \Big\}$$

Def: (1. try) $\forall E : \exists \rho^{ideal}_{ABE} \in S_{ideal}$:

$$TD\left(\rho^{real}_{ABE}, \rho^{ideal}_{ABE}\right) \leq \varepsilon$$

Example: Say E manages the following:
- With prob. 2^{-1000}, they guess K
- With prob. $1-2^{-1000}$, they notice that attack failed and make proto abort.

↓

$$\rho^{real}_{ABE} = \sum_k |k\rangle\langle k| \otimes |k\rangle\langle k| \otimes |k\rangle\langle k|$$

⇒ ρ^{real}_{ABE} not close to S_{ideal}

⇒ Proto not secure according to def.

Want this proto to be considered secure

Def: The proto ε-secure iff $\forall E\ \exists \rho^{ideal}_{ABE} \in S_{ideal}$:

$$TD(\rho^{real}_{ABE}, \rho^{ideal}_{ABE}) \cdot Pr[success] \leq \varepsilon$$

Overview

Step 1: Exchange quantum data (insecure) (Bell pairs $\underbrace{\tfrac{1}{\sqrt2}|00\rangle + \tfrac{1}{\sqrt2}|11\rangle}_{|\beta_{00}\rangle}$)

Step 2: Test Bell pairs
⇒ $|\beta_{00}\rangle^{\otimes n}$ up to t errors
(Implications: A&B have almost same key, E know little)

If A, B have $|\beta_{00}\rangle^{\otimes n}$ means: state $|\beta_{00}\rangle\langle\beta_{00}| \otimes \rho_E$
↓ measure ⊗ I
$(|00\rangle\langle 00|\frac{1}{2} + |11\rangle\langle 11|\frac{1}{2}) \otimes \rho_E$

Step 3: Measure $|\beta_{00}\rangle^{\otimes n}$ in comp. basis

Step 4: Error correction (now A&B same key)

Step 5: Privacy amplification
⇒ E knows nothing

Notation: Bell states:

$$|\beta_{00}\rangle = \tfrac{1}{\sqrt2}|00\rangle + \tfrac{1}{\sqrt2}|11\rangle$$
$$|\beta_{01}\rangle = \tfrac{1}{\sqrt2}|01\rangle + \tfrac{1}{\sqrt2}|10\rangle$$
$$|\beta_{10}\rangle = \tfrac{1}{\sqrt2}|00\rangle - \tfrac{1}{\sqrt2}|11\rangle$$
$$|\beta_{11}\rangle = \tfrac{1}{\sqrt2}|01\rangle - \tfrac{1}{\sqrt2}|10\rangle$$

Those form a ONbasis of $\mathbb{C}^2 \otimes \mathbb{C}^2$

If we measure $|\beta_{00}\rangle$ in comp. basis: get equal random bits

$\mathcal{E}_{meas}(\rho)$:= measure & forget ρ $\quad \left(\mathcal{E}_{meas}(\rho) = \sum_x |x\rangle\langle x|\rho|x\rangle\langle x|\right)$

$$\mathcal{E}_{meas}(|\beta_{00}\rangle\langle\beta_{00}|) = \tfrac{1}{2}|00\rangle\langle 00| + \tfrac{1}{2}|11\rangle\langle 11|$$

$$\mathcal{E}_{meas}(|\beta_{00}\rangle\langle\beta_{00}|^{\otimes n}) = (\ \text{——} + \text{——}\ )^{\otimes n} = \sum_{x\in\{0,1\}^n} 2^{-n} |x\rangle\langle x| \otimes |x\rangle\langle x|$$

Notation: $|\widetilde{xy}\rangle := |\beta_{x_1 y_1}\rangle \otimes |\beta_{x_2 y_2}\rangle \otimes |\beta_{x_3 y_3}\rangle \otimes \dots$
$(x, y \in \{0,1\}^n)$

Note: $|\widetilde{xy}\rangle$ form an ONB of $\mathbb{C}^{2n}$

Step 1: Exchange Bell pairs

(A) Prepare $|\widetilde{00}\rangle$ —second halves→ (B)
↑ Eve

State after step 1?

If honest: $\rho_1 = |\widetilde{00}\rangle\langle\widetilde{00}|_{AB} \otimes \rho_E$

In general: ρ_1 is anything