# Quantum Cryptography

Tuesday, October 10, 2023 5:42 PM

## Recall: Cryptography

Cryptography (Today)

- Symmetric
  - one key (shared)
  - e.g. DES, AES
  - Can do: enryption / decryption
- Asymmetric
  - 2 keys: public and private
  - e.g: RSA, Diffie-Helman
  - Can do: encryption / decryption
    - key exchange
    - digital sigature (Authentication)

1] Cryptography in the Quantum Era.

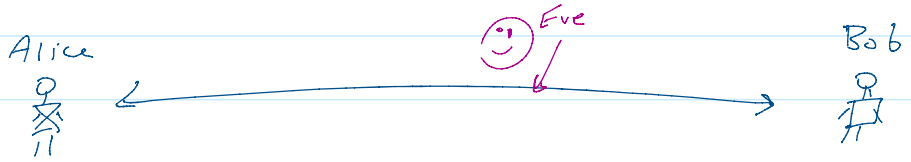
- Symmetric
  - is ok (with a larger key)
  - e.g. AES-256
- Asymmetric
  - e.g. RSA will be broken by Shor algorith

2] Solution?

- Quantum Cryptography
  - quantum mechanics
  - e.g. key-exchange
- post-quantum Cryptography (PQC)
  - e.g. Lattice-based
  - hash-based

3] Quantum key-exhange (QKE) (§ 9.1)

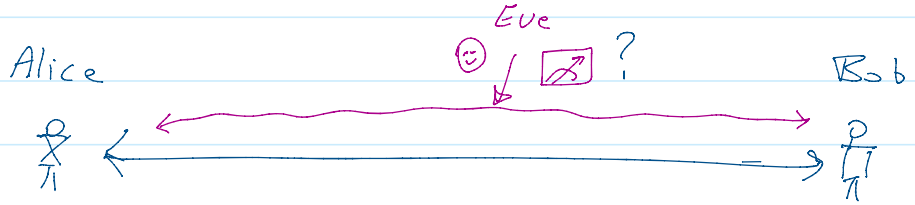
1. classical channel




Assume: ① Eve can listen to the channel "stealthy"
② She can copy all exchanged information
(ciphertext, keys, plaintext)

e.g. ⇒ Diffie-Hellman KE protocol use DLog problem to secure the key.

2. Quantum Channel:




Assumptions: ① Measuring the qubit stream alters it.
② No-cloning theorem: Eve cannot copy the qubit-stream.

---

Next Week

| | | |
|---|---|---|
| HW 2 | — due | 18 oct. |
| Quiz B2 | on | 18 — 19 oct |
| Quiz 2 | on | 20 oct. |
| Midterm | on | 21 oct. |