Quantum Crypto

Lecture | Practice

Lo Raul-Martin

- Zulip
- Homework: Required: 50% of points
- Grade: From final exam
- Materials:
  - Lecture notes
  - Book: Quantum Computation & Information Nielsen/Chuang (Chap. 1, 2, 4, 8)
  - Video
  - Whiteboard pics

Background: No physics background needed; don't fear lin. algebra

What is Q crypto?

post-quantum crypto

- crypto running on regular comp.
- secure against quantum attacks

quantum protocols

- protocols that actively use q. communication

Post Q-crypto

- Why can Q computers be more powerful?

Superposition: system can be in several states simult.

Eg. qubit could be 60% "0" + 40% "1"

10 qubits: 1024 states simult.

1000 qubits: 2^{1000} states

Operating in parallel on 2^{1000} states → massive parallelism

But: cannot read all results.

⇒ In many cases Q parallelism useless.

But: Sometimes we can combine those results, get speedup.

Q-algos

Grover:

Say $f: \{0,1\}^n \to \{0,1\}$

Goal: Find x with $f(x)=1$

Classically: Need 2^n tries

Q: $\sqrt{2^n} = 2^{n/2}$

Shor:

RSA, ElGamal, ECC

Factors large integers
- Classical: $2^{\sqrt[3]{\log n}}$
- Quantum: $\log^3$

Computing discrete logs
- Class: exp, Q: poly

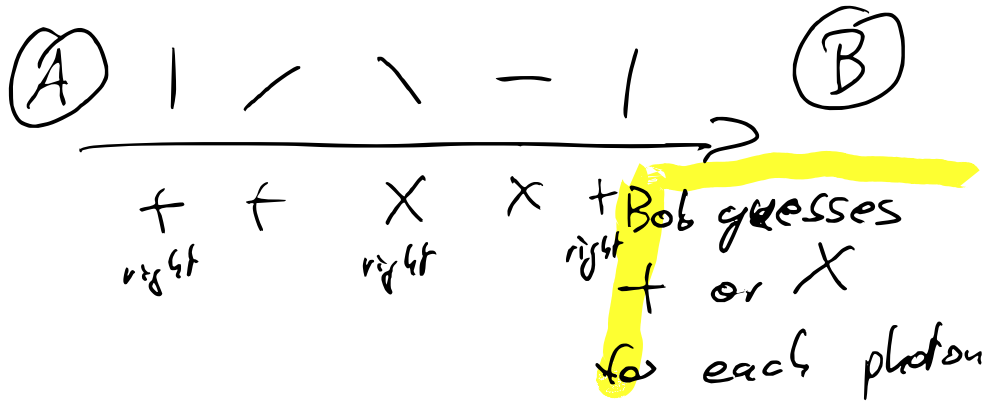
Q protocols

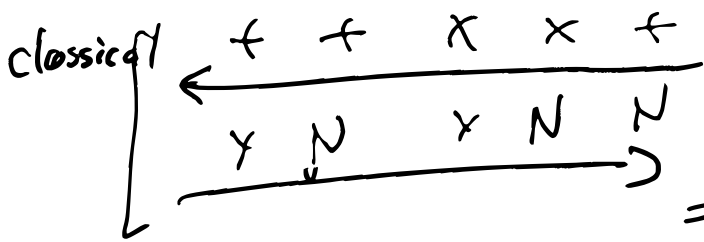
Q key distribution (1984)

Situation: A & B want to share key

- quantum channel (eg. pol. photons)
- authenticated class. channel
- do not want to rely on computational assums

Class: Impossible!





⇒ A & B both know with bits

B knows

⇓

K

⇓

K

Attack?

Eve measures qubit 3 with pr $\frac{1}{2}$: uses +

⇒ changes qubit 3 into ~ or 1

⇒ with pr $\frac{1}{2}$: A & B get diff bits

In postprocessing:

ARB check for discrepancies.

If E attached:

ARB find those & abort

Quantum mechanics

(for Q information)

Quantum system

- Characterized by N "class. possibilities".
- Eg: Qubit has 0, 1 (N=2)
- Eg: 5 qubit system

  00000, 00001, 00010,

  ...., 11110, 11111 (N=32)

Quantum states

Vector containing numbers for each class. poss.

~~$\mathbb{R}^N$~~ complex numbers

$\mathbb{C}^N$

E.g.: qubit states:

$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \hat{=}$ the system is in class. state "0"

$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \hat{=}$ class. state "1"

$\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \hat{=}$ system is equally in "0" and "1".

Entries are called "amplitudes",

|square (amplitude)| $\hat{=}$ probability

$\begin{pmatrix} \sqrt{2/3} \\ \sqrt{1/3} \end{pmatrix} \hat{=}$ prob $2/3$ of "0"
prob $1/3$ of "1".

Def: A quantum state is a vector ψ in $\mathbb{C}^N$ s.t. $\|\psi\| = 1$ ($\overset{\text{i.e.}}{\sum} |\psi_i|^2 = 1$)