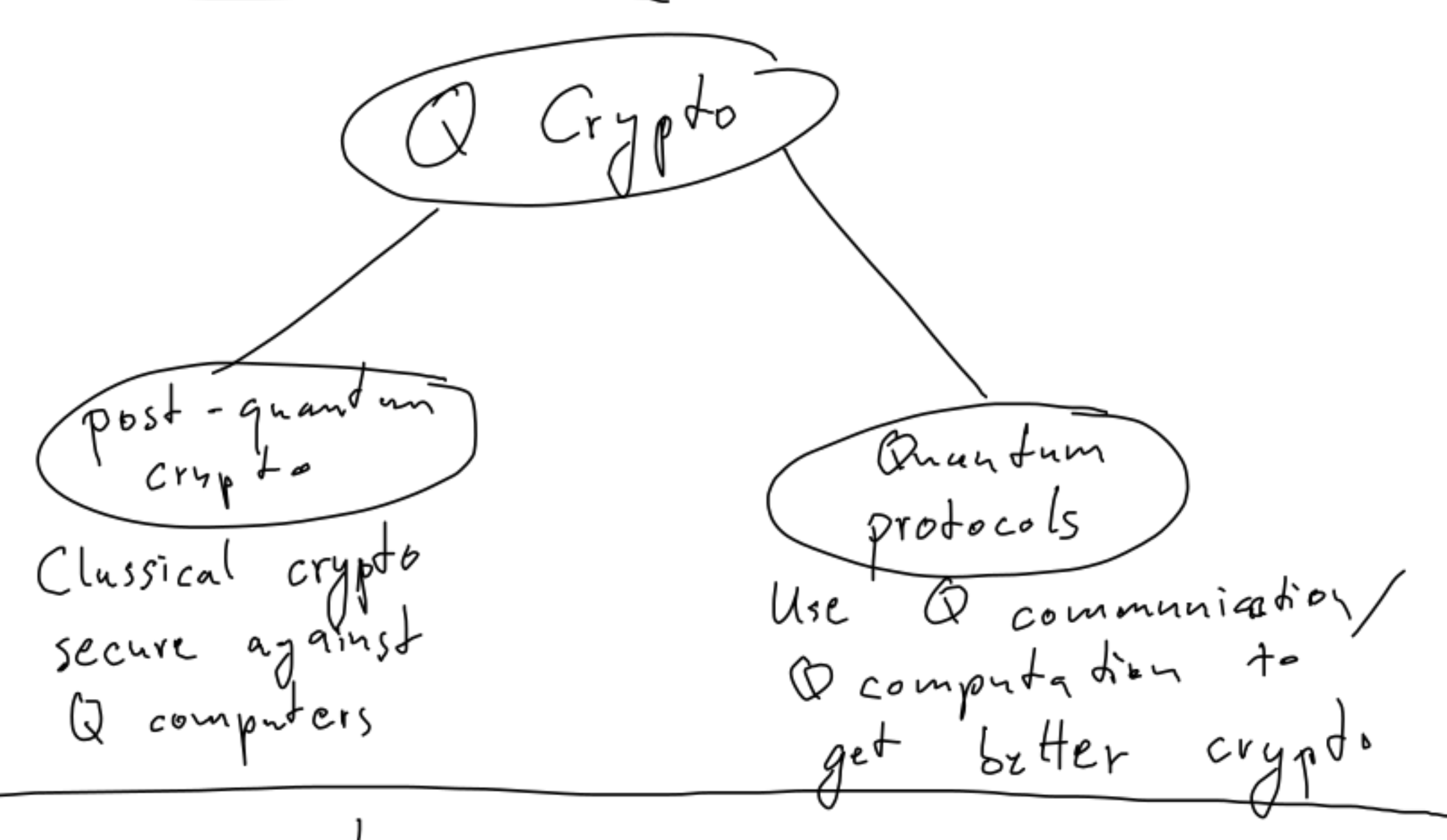
Lecture / Practice
↳ Raul-Martin

- Slack
- Homeworks: Required: 50% of points to qualify for exam
- Materials:
  - Lecture notes
  - Book: Quantum Computation & Info, Nielsen/Chuang (Chap 1 2 4 8)
  - Video
  - Whiteboard pics

Scope / background

- No physics background needed
- Math: No fear of linear algebra

What is Q crypto?



Post Q-crypto

What is a Q computer?

Superposition → system can be in several states simultaneously

Eg.: a bit could be 60% "0", 40% "1".

Eg: 10 bits could be in superpos of up to 1024 values.

Eg: 1000 bits: 2^{1000} values simult.

Can do: apply function f to all values simult.

$$\sum_x |x\rangle \longrightarrow \sum_x |x, f(x)\rangle$$

→ massive parallelism.

Caveat: If we observe the state, collapses to 1 value.

Still: Interesting algo possible

Grover: Say we have $f: \{0,1\}^m \to \{0,1\}$

Want x s.t. $f(x) = 1$

Classically: $\sim 2^m$ steps

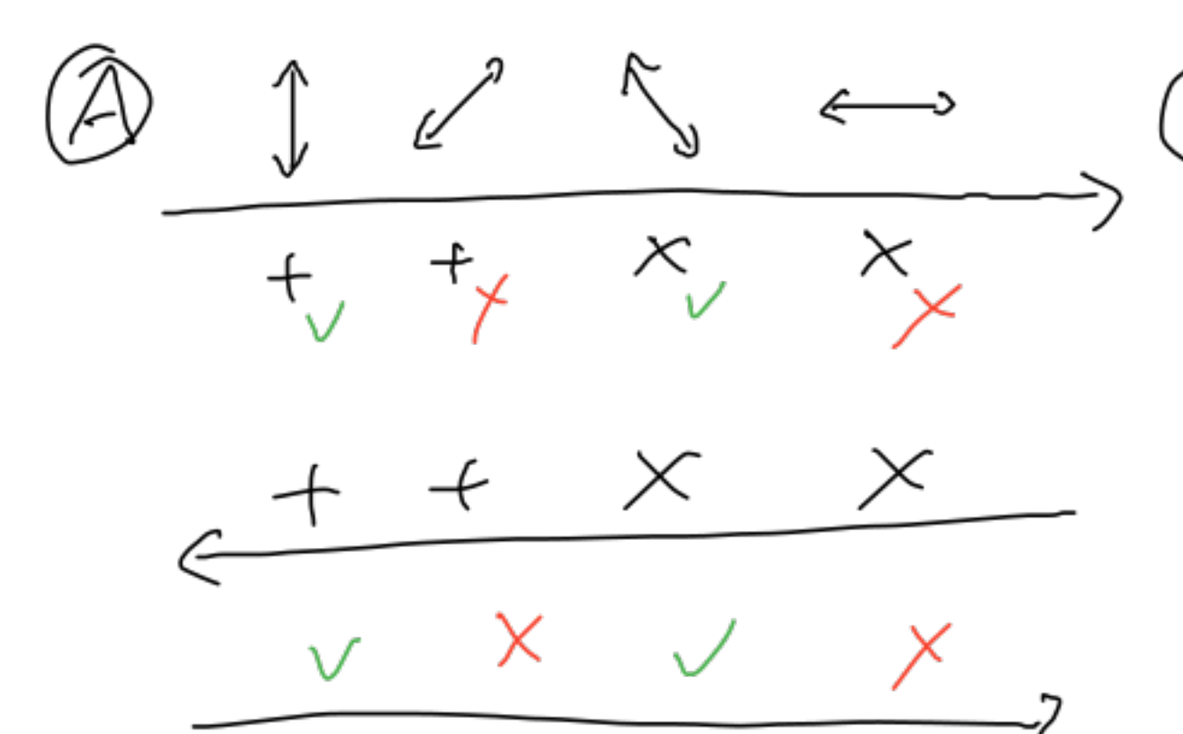
Quantumly: $\sim 2^{m/2}$ steps $= \sqrt{2^m}$

Shor: Factor large integers, Compute discrete logs } ⇒ Break most public key crypto (RSA, ElGamal, ECC)

Q protocols

Q key distribution

A&B want secret key



Bob guess for each bit: + or ×

Key := those bits where B measured right

What if E measures photons, too?

→ Photons are disturbed
→ Bob gets wrong bits
→ A&B will notice attack

Quantum Mechanics (for Q information)

Quantum system: Characterized by N different class. possibilities

E.g.: 0, 1 N=2 (qubit) E.g. left, middle, right (pos. of photon) N=3

E.g: 5 qubits: 00000, 00001, 00010, ..., 11111 $N = 2^5 = 32$

System can be in "superpos" of all class. possibilities.

E.g: All 0 → $\begin{pmatrix}1\\0\end{pmatrix}$ "0" "1"

All 1 → $\begin{pmatrix}0\\1\end{pmatrix}$ "0" "1"

50/50 → $\begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}$ "0" "1"

$\begin{pmatrix}\sqrt{2/3}\\ \frac{1}{\sqrt{3}}\end{pmatrix}$

Any vector with N complex coefficients is a valid Q-state and the squared-coeff. (abs. value) add to 1

$\begin{pmatrix}i\\0\end{pmatrix}$ $\begin{pmatrix}i/\sqrt{2}\\-i/\sqrt{2}\end{pmatrix}$

"Probabilty" := $|\text{Amplitude}|^2$

Eg: Not Q state: $\begin{pmatrix}1/2\\1/2\end{pmatrix}$ $\begin{pmatrix}1\\1\end{pmatrix}$ $\begin{pmatrix}2\\0\end{pmatrix}$

Summary: A Q-state is a vector $|\psi\rangle \in \mathbb{C}^N$ s.t. $\| |\psi\rangle \| = 1$

ket $= \begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_N\end{pmatrix}$ $= \sqrt{\sum_i |\alpha_i|^2}$

α_i called "amplitude" ("probability ampl.")
$|\alpha_i|^2$ are intuitively probabilities.

What Operations on Q systems are poss.?

- Should be func $U: \mathbb{C}^N \to \mathbb{C}^N$
- Linear! $U(|\psi\rangle + |\phi\rangle) = U|\psi\rangle + U|\phi\rangle$
  $U\gamma|\psi\rangle = \gamma U|\psi\rangle$
- If $|\psi\rangle$ is Q state, then $U|\psi\rangle$ is Q state

$\forall|\psi\rangle: \| |\psi\rangle \| = 1 \implies \| U|\psi\rangle \| = 1$

$\forall|\psi\rangle: \| U|\psi\rangle \| = \| |\psi\rangle \|$ "U is length-preserving"

aka "U unitary" / "U isometry" (same thing if $N<\infty$)

aka $U^\dagger U = I$

Summary: An operation on a Q system is a unitary matrix $(U^\dagger U = I)$

Examples: Bit flip: $\begin{pmatrix}1\\0\end{pmatrix} \to \begin{pmatrix}0\\1\end{pmatrix}$, $\begin{pmatrix}0\\1\end{pmatrix} \to \begin{pmatrix}1\\0\end{pmatrix}$ $X = \begin{pmatrix}0&1\\1&0\end{pmatrix}$

$X^\dagger X = \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} = \begin{pmatrix}1&\\&1\end{pmatrix}$ ✓

⇒ X is unitary

Mapping to "↗" = $\begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}$ $M = \begin{pmatrix}1/\sqrt{2}&1/\sqrt{2}\\1/\sqrt{2}&1/\sqrt{2}\end{pmatrix}$

$M^\dagger M = \begin{pmatrix}1/\sqrt{2}&1/\sqrt{2}\\1/\sqrt{2}&1/\sqrt{2}\end{pmatrix}\begin{pmatrix}1/\sqrt{2}&1/\sqrt{2}\\1/\sqrt{2}&1/\sqrt{2}\end{pmatrix} = \begin{pmatrix}1&1\\1&1\end{pmatrix} \neq I$

⇒ not unitary