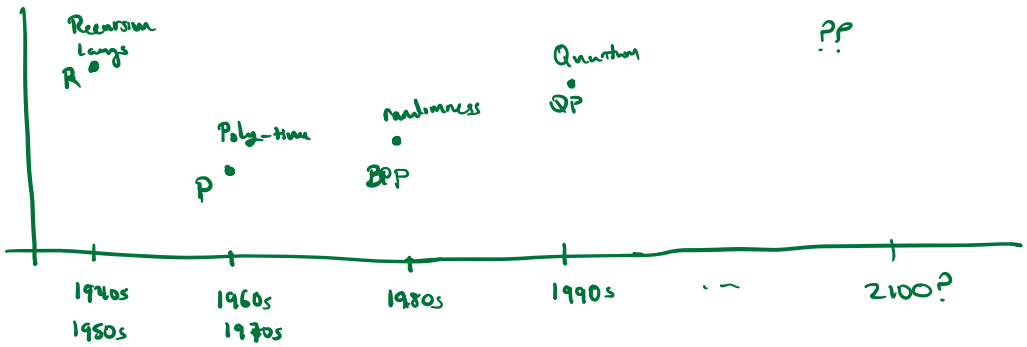
Quantum Computing and Cryptography

Models of Practical Computation



Quantum computing

Classical particle:

quantum particle:

Particle is pos. x w/ prob. $p(x)$

The state of a particle is char. by

func. $\Psi : \mathbb{R} \to \mathbb{C}$

interp. $p(x) = |\Psi(x)|^2$

so $\int_{\mathbb{R}} |\Psi(x)|^2 \, dx = 1$

Discrete version (qbit)

elec. can have top spin (0) or bottom spin (1)

$$\Psi = \Psi_0 \cdot |0\rangle + \Psi_1 \cdot |1\rangle$$

where $\Psi_0, \Psi_1 \in \mathbb{C}$ s.t. $|\Psi_0|^2 + |\Psi_1|^2 = 1$.

Let $\Omega = \text{span}_{\mathbb{C}} \{ |0\rangle, |1\rangle \}$

$\dim(\Omega) = 2$.

Quantum state: point $\Psi \in \Omega$

$$\Psi = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$$

Quantum state change via linear transform: U on Ω

$$\Psi \longrightarrow \Psi_{new} := U \cdot \Psi$$

if $\|\Psi\|_2 = 1$: $\|U \cdot \Psi\|_2 := 1$ (U must preserve norm — unitary)

$(U^T)^* U = I$

n-particles (n qbits)

$|000\ldots0\rangle, |000\ldots01\rangle, |111\ldots1\rangle$

2^n states $\Rightarrow$ Ω lin. space of dim 2^n

$\dim(\Omega) = 2^n$, $\Psi \in \Omega$ s.t. $\|\Psi\|_2 = \sum_{x \in \{0,1\}^n} |\Psi(x)|^2 = 1$

High-level desc. of quantum computer

1. Start sys in state $\Psi_0 \in \Omega$
2. Apply basic transforms $U_1 \ldots U_n$

   state of system: $\Psi_n = U_n \cdots U_2 U_1 \cdot \Psi_0$
3. Observe system:

   Observe state $x \in \{0,1\}^n$ w/ prob $|\Psi_n(x)|^2$

Goal: most of prob in $|\Psi_n|^2$ should be on "correct" answer

Problem: noise from environment: $\hat{\Psi}_n = \Psi_n +$ noise

Shor's Algorithm (1994)

Let $f_1 : \mathbb{Z} \to G$ be periodic fn

$\exists \pi \in \mathbb{Z}$ s.t. $\forall x \in \mathbb{Z}: f_1(x) = f_1(x+\pi)$

Let $f_2 : \mathbb{Z}^2 \to G$ be a periodic fn

$\exists u, v \in \mathbb{Z}^2$ s.t. $\forall x \in \mathbb{Z}^2: f_2(x) = f_2(x+u) = f_2(x+v)$

Shor: give an oracle for f_1, there is a quantum alg. that outputs a random short period $\pi' = a \cdot \pi$ of f_1 for some small $a \in \mathbb{Z}$ in time $O(\log|\pi|)$

Same for f_2.

Application #1: factoring ints

$n = p \cdot q$: breaks RSA

Let $g \in \mathbb{Z}_n^*$. $f_1(x) = g^x \in \mathbb{Z}_n^*$

$f_1 : \mathbb{Z} \to \mathbb{Z}_n^*$

$g^{\varphi(n)} \equiv 1$ in $\mathbb{Z}_n$ $\Rightarrow f_1$ has period $\varphi(n) = (p-1)(q-1)$

Shor: $a \cdot \varphi(n)$ in time $O(\log n)$

$\Rightarrow$ HW3 #1: breaks RSA

Can even be used to factor n.

finding periods of $f_2 : \mathbb{Z}_2 \to G$

$\Rightarrow$ compute Dlog in G for all G

$\Rightarrow$ breaks DH!!

takes a long time

What to do about this?

RSA, Schnorr, DH all broken!

← break 2048 bit RSA: 20M qbits, 8hr
break 256-bit ECC: 13M qbits, 24hr
currently: 100 qbits systems

Move to classical cryptosystems that are secure against quantum algs

$\Rightarrow$ Lattice systems, coding systems, isogeny systems

(very slow currently)