Shor's algorithm

The elementary version

J Avron

October 14, 2020

What classical computers cant do

Factoring

- Factoring: $35 = \underbrace{5 \times 7}_{primes}$
- Try $35/2 = ?, 35/3 = ? \ldots$
- # trials: $\sqrt{N}$
- Best known: $O\left(e^{n^{1/3}\cdots}\right), \; n = \log N$

$\#$ with 230 digits

2000 years on 2.2 GHz processor

RSA cryptosystem

It's not a bug, it's a feature

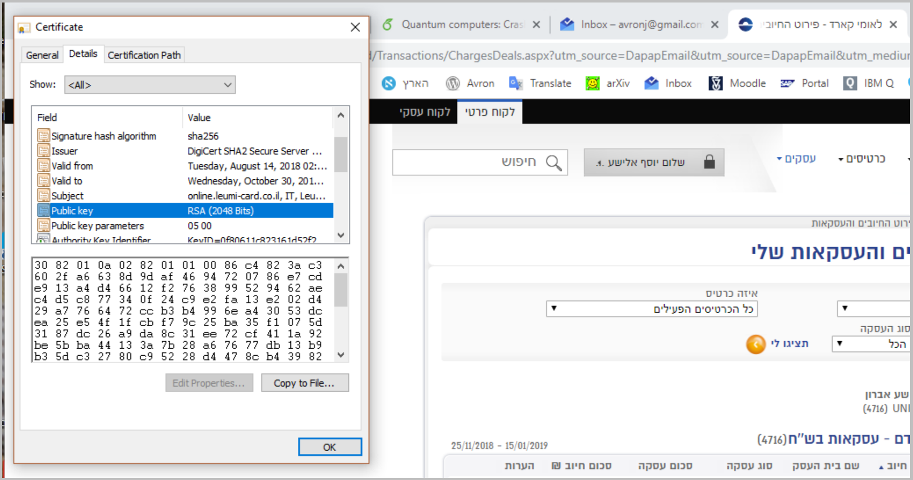
- $\underbrace{N}_{public} = \underbrace{p \times q}_{secret}$
- $Ecryption = f(Message, N)$
- $Message = g(Encryption, p, q)$

RSA security

- f, g are known functions.
- Security rests on the presumed difficulty of factoring

Everybody uses RSA

All the time



The potential disaster/Benefits

If a fast factoring algorithm is found

Bad	Good
The evil guy read our mail	We read the mail of the evil guys
The internet is insecure	The darknet is insecure
Financial transaction insecure	Money laundering is difficult
State records become public	State records become public
...	...

The quantum threat
Shor algorithm

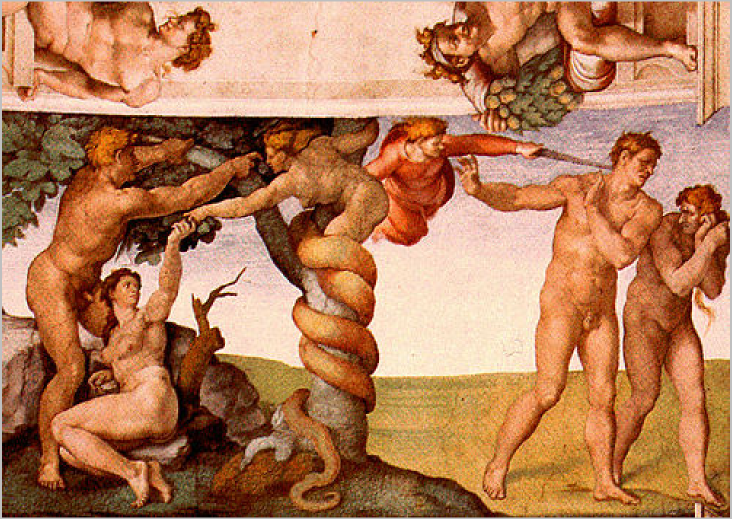
- Peter Shor 1994
- Fast factoring
- Time $= O((\#digits)^2)$
- Needs a quantum computer

Quantum computer

Allows for fast factoring

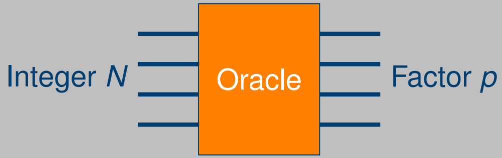
Science begets knowledge, opinion ignorance

Hippocrates



Factoring Oracle

Weak and unreliable is good enough



$$\text{Oracle}(N) = \begin{cases} \text{Error} & \text{Probability} = 1/2 \\ 1,\text{N} & \text{Porbability} = 3/10 \\ 42 & \text{Porbability} = 1/5 \\ p & \text{Probability} = 1/10 \end{cases}$$

Verify answer on a classical computer

- If incorrect, query again
- 10 trials will give p w.h.p.

poll 2

- $a^k \mod N$ is a periodic function of k
- Example with $a = 2, N = 15$ where period=4

k	1	2	3	4	5	...	15
2^k *Mod* 15	2	4	8	16=1	2	...	8

- Euler-Fermat: $a^{(p-1)(q-1)} = 1 \mod N, \quad gcd(a, N) = 1$

Factoring reduces to finding the period of $a^k \mod N$

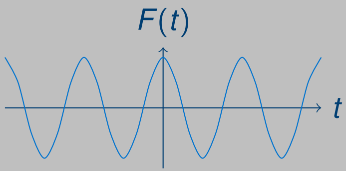
- $pq = N$
- $(p-1)(q-1) = \text{Integer} \times \text{period}\ (a^k \mod N)$

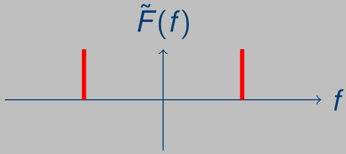
Number theory then gives p, q

More math preliminaries

Fourier transform and its Discrete cousin

- $\tilde{F}(f) = \frac{1}{\sqrt{2\pi}} \int e^{ift} F(t) dt$
- $\widetilde{e^{i\omega t}} \Longrightarrow \delta(f - \omega)$
- Unitary





Discrete Fourier: $\underbrace{\omega = e^{2\pi i/L}}_{\text{root of unity}}$

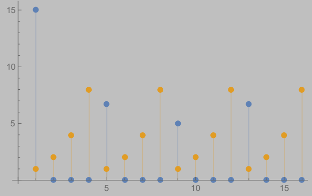
$$\tilde{F}(m) = \frac{1}{\sqrt{L}} \sum_{k=1}^{L} \omega^{km} F(k)$$

poll 3

Periodic functions

Fourier transform is sparse

$$\tilde{F}(m) = \frac{1}{\sqrt{L}} \sum_{k=1}^{L} \omega^{km} F(k)$$



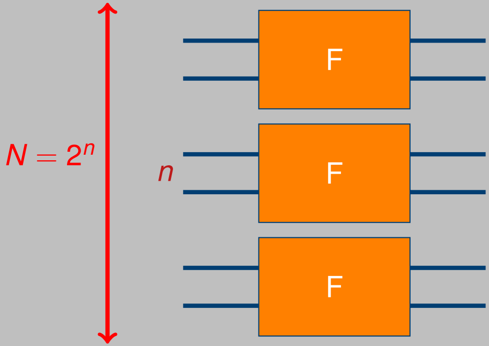
$$F(k + period) = F(k) \Longleftrightarrow \tilde{F}(m) = \underbrace{\omega^{m\,\text{period}}}_{?=1} \tilde{F}(m)$$

- Either $m \times$ period $=$ (Integer) $\times L$
- Or $\tilde{F}(m) = 0$

k	0	1	2	3	4	5	...
2^k *Mod* 15	1	2	4	8	16=1	2	...
Fourier	X	0	0	0	X	...	0

Functions contain exponential amount of information

Hard classically



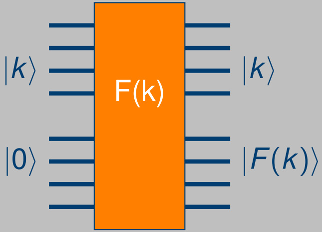
Storing $\{F\}$ needs $O(N \log N)$ bits

- n bits for one argument k
- N possible values for k

$\{F\}$ can be stored in $2n$ qubits

The superposition advantage

- n qubits encode one k
- k takes $N = 2^n$ values
- Superpositions: No extra qubits
- n qubits encode all of $\{F(k)\}$

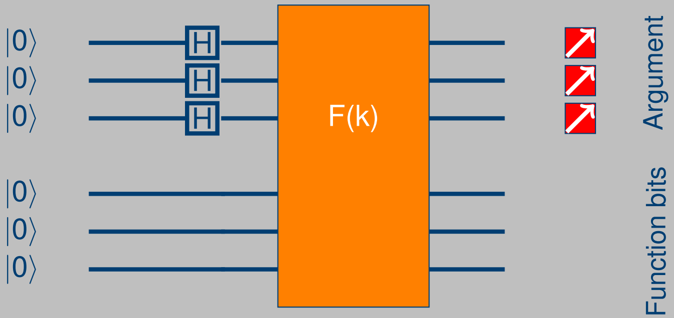


Parallel processing

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle \xrightarrow{\text{Function gate}} \frac{|0\rangle |F(0)\rangle + |1\rangle |F(1)\rangle}{\sqrt{2}}$$

No free-lunch principle

Measurement reveals one random $F(k)$



Measurement reveals

- one, random, entry k and the corresponding $F(k)$

Shor algorithm

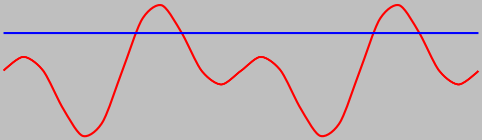
Quantum Fourier: Exponential improvement on FFT

- Under the hood: massive superposition

$$\underbrace{|0\dots0\rangle}_{\textit{argument}}\ \underbrace{|a^0\rangle}_{\textit{function}} + \cdots + |1\dots1\rangle\,|a^{L-1}\rangle$$

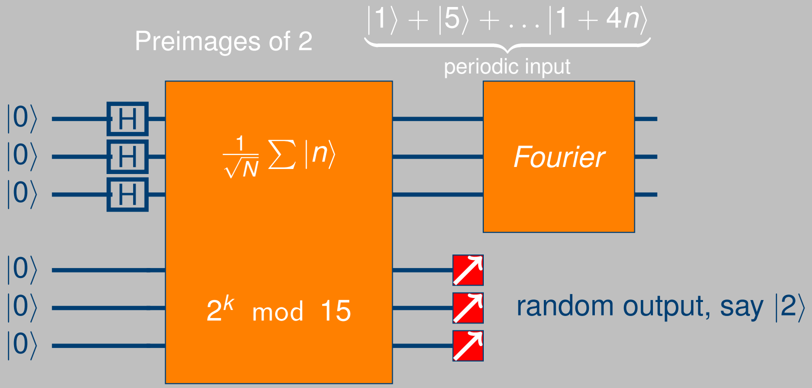
- Measure function register $|a^k\rangle$
- Get: Random integer, e.g. $|a^k\rangle = |2\rangle$
- Argument register: superposition of pre-images of $|2\rangle$

$$|1\rangle + |1+4\rangle + |1+2\times 4\rangle + |1+3\times 4\rangle\,, \quad 2^{1+4n} = 2 \mod 15$$



Entanglement gives a periodic sequence of integers

Fourier=interference extract the period

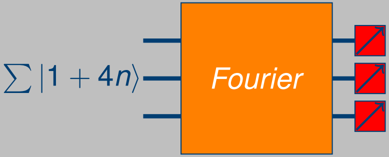


2^k *Mod* 15	1	2	4	8	1	2	...
k,m		1				5	...
Fourier	1	0	0	0	i	...	0

You also need to be lucky

1 and *N* are trivial factors

- Bad luck: Measure $|0\rangle$
- Learn nothing:
  $0 \times \textit{period} = \text{integer} \times L$



2^k *Mod* 15	1	2	4	8	1	2	...
m	0	1	2	3	4	5	...
$\lvert Fourier \rvert^2$	1	0	0	0	1	...	0

Moral: Store information in states not in amplitudes

Be wise and modest

Fourier constructively interferes the periods on few basis states

- States=Integers: Revealed in single shot
- Amplitudes=Complex numbers: Revealed in statistics
- Relevant information is best revealed in one shot
- The amplitudes are the roulette in the quantum casino