

# Shor's algorithm

## The elementary version

J Avron

October 14, 2020

# What classical computers cant do

## Factoring

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



# with 230 digits

2000 years on 2.2 GHz processor

# RSA cryptosystem

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

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



## RSA security

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

# Everybody uses RSA

All the time

The screenshot shows a Windows 'Certificate' dialog box with the 'Details' tab selected. The 'Show:' dropdown is set to '<All>'. The 'Field' and 'Value' table is as follows:

Field	Value
Signature hash algorithm	sha256
Issuer	DigiCert SHA2 Secure Server ...
Valid from	Tuesday, August 14, 2018 02:...
Valid to	Wednesday, October 30, 201...
Subject	online.leumi-card.co.il, IT, Leu...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=0FR0611r273161d52F2

Below the table is a hexadecimal representation of the public key parameters:

```
30 82 01 0a 02 82 01 01 00 86 c4 82 3a c3
60 2f a6 63 8d 9d af 46 94 72 07 86 e7 cd
e9 13 a4 d4 66 12 f2 76 38 99 52 94 62 ae
c4 d5 c8 77 34 0f 24 c9 e2 fa 13 e2 02 d4
29 a7 76 64 72 cc b3 b4 99 6e a4 30 53 dc
ea 25 e5 4f 1f cb f7 9c 25 ba 35 f1 07 5d
31 87 dc 26 a9 da 8c 31 ee 72 cf 41 1a 92
be 5b ba 44 13 3a 7b 28 a6 76 77 db 13 b9
b3 5d c3 27 80 c9 52 28 d4 47 8c b4 39 82
```

Buttons at the bottom include 'Edit Properties...', 'Copy to File...', and 'OK'.

The screenshot shows a web browser window with several tabs: 'Quantum computers: Cras...', 'Inbox - avronj@gmail.com', and 'לאומי קארד - פירוט החיוב'. The address bar shows a URL with 'utm\_source=DapapEmail'. The page content is in Hebrew and includes a search bar with the text 'חפוש' and a navigation menu with 'עסקים' and 'כרטיסים'. A large blue heading reads 'העסקאות שלי'. Below it, there are dropdown menus for 'איזה כרטיס' and 'כל הכרטיסים הפעילים'. A 'תציג לי' button is visible. At the bottom, there is a date range '25/11/2018 - 15/01/2019' and a list of items including 'הערות', 'סכום חיוב', 'סכום עסקה', 'סוג עסקה', and 'שם בית העסק'.

# The potential disaster/Benefits

If a fast factoring algorithm is found

Bad

The evil guy read our mail  
The internet is insecure  
Financial transaction insecure  
State records become public  
...

Good

We read the mail of the evil guys  
The darknet is insecure  
Money laundering is difficult  
State records become public  
...



# The quantum threat

## Shor algorithm

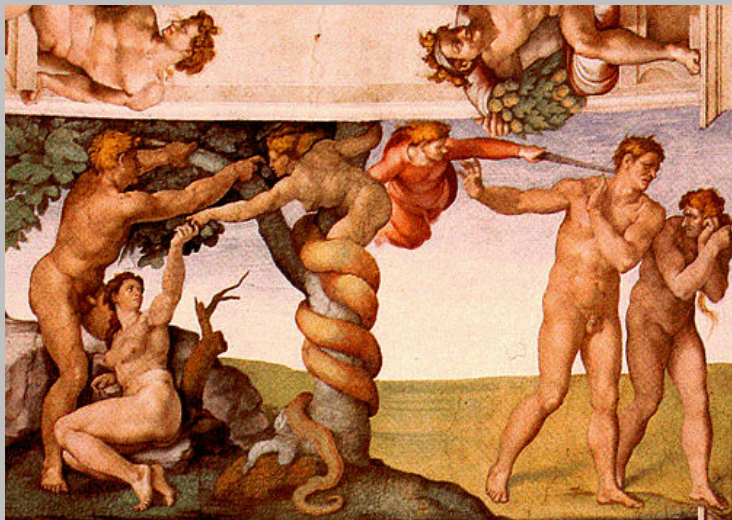
- Peter Shor 1994
- Fast factoring
- Time =  $O((\#digits)^2)$
- Needs a quantum computer



Quantum computer  
Allows for fast factoring

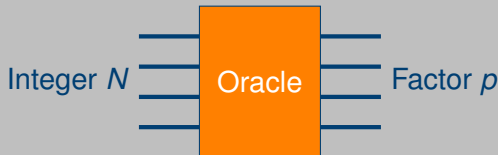
# Science begets knowledge, opinion ignorance

Hippocrates



# Factoring Oracle

Weak and unreliable is good enough



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

Verify answer on a classical computer

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



# Math Preliminaries

## Facts from number theory

poll 2

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

k	1	2	3	4	5	...	15
$2^k \bmod 15$	2	4	8	16=1	2	...	8

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

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

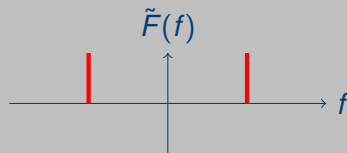
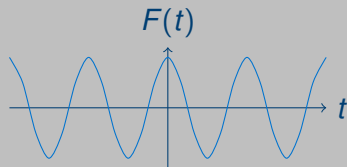
- $pq = N$
- $(p-1)(q-1) = \text{Integer} \times \text{period} (a^k \bmod N)$

Number theory then gives  $p, q$

# More math preliminaries

## Fourier transform and its Discrete cousin

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



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

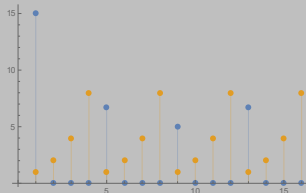
$$\tilde{F}(m) = \frac{1}{\sqrt{L}} \sum_{k=1}^L \omega^{km} F(k)$$

poll 3

# Periodic functions

Fourier transform is sparse

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



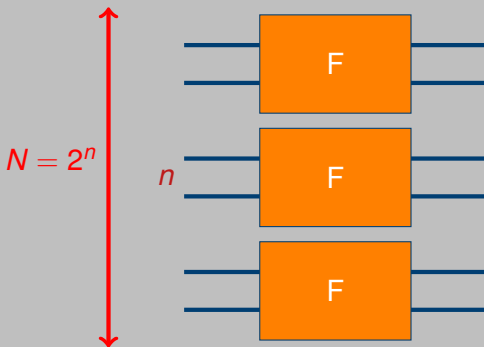
$$F(k + \text{period}) = F(k) \iff \tilde{F}(m) = \underbrace{\omega^{m \text{ period}}}_{?=1} \tilde{F}(m)$$

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

k	0	1	2	3	4	5	...
$2^k \text{ Mod } 15$	1	2	4	8	16=1	2	...
Fourier	X	0	0	0	X	...	0

# Functions contain exponential amount of information

Hard classically



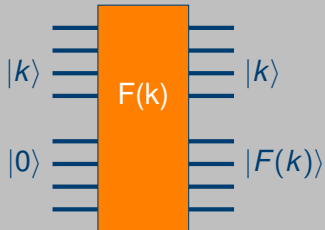
Storing  $\{F\}$  needs  $O(N \log N)$  bits

- $n$  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  $\{F(k)\}$

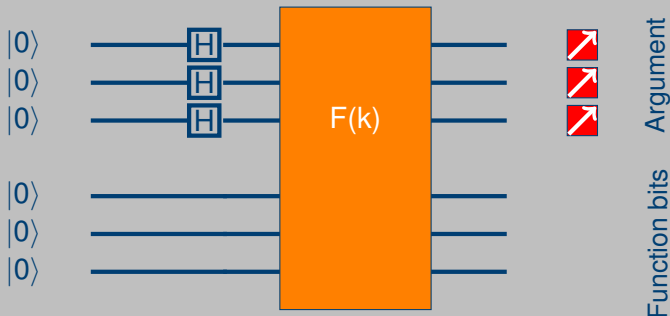


Parallel processing

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

# No free-lunch principle

Measurement reveals one random  $F(k)$



Measurement reveals

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

# Shor algorithm

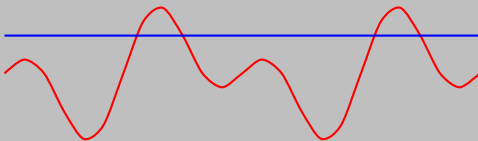
## Quantum Fourier: Exponential improvement on FFT

- Under the hood: massive superposition

$$\underbrace{|0 \dots 0\rangle}_{\text{argument}} \underbrace{|a^0\rangle}_{\text{function}} + \dots + |1 \dots 1\rangle |a^{L-1}\rangle$$

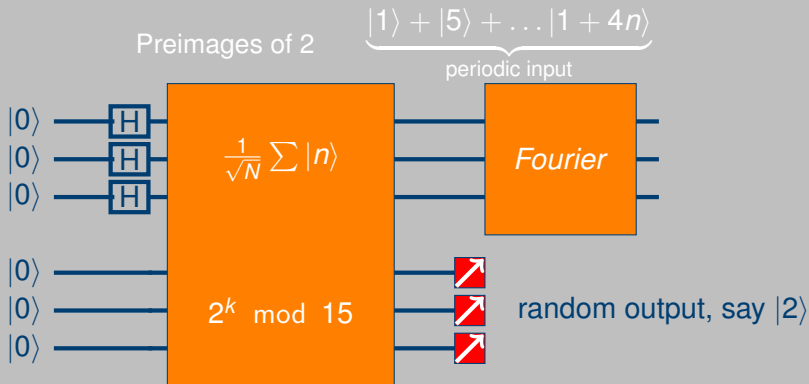
- Measure **function** register  $|a^k\rangle$
- Get: Random integer, e.g.  $|a^k\rangle = |2\rangle$
- **Argument** register: superposition of pre-images of  $|2\rangle$

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



# Entanglement gives a periodic sequence of integers

Fourier=interference extract the period



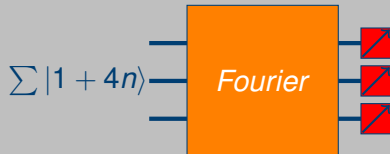
$2^k \bmod 15$	1	2	4	8	1	2	...
k,m		1				5	...
Fourier	1	0	0	0	i	...	0



# You also need to be lucky

1 and  $N$  are trivial factors

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



$2^k \text{ Mod } 15$	1	2	4	8	1	2	...
m	0	1	2	3	4	5	...
$ \textit{Fourier} ^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

