Shor's algorithm The Technion Quantum summer school 2020

J Avron

October 15, 2020

JA (Technion)

Shor's algorithm

October 15, 2020 1/17

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

What classical computers cant do

Factoring

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



with 230 digits2000 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)



イロト イヨト イヨト イヨト

RSA security

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

Everybody uses RSA

All the time

Certificate X	🗴 Quantum computers: Crasi X 🛛 🖄 Inbox – avronj@gmail.com X 🤤 א לאומי קארד - פירוט החיוביי 😜 X
General Details Certification Path	/Transactions/ChargesDeals.aspx?utm_source=DapapEmail&utm_source=DapapEmail&utm_mediur
Show: <all></all>	ארץ 🛞 Avron 🎥 Translate 🧕 arXiv প Inbox 🕅 Moodle 😅 Portal 🚺 IBM Q 🛛
Field Value ^	לקוח פרטי לקוח עסקי
Signature hash algorithm sha255 Issuer OgCert 5142 Secure Server Vaid from Tuesday, August 14, 2018 02 Vaid to Vednesday, October 30, 201 Subject online-leumi-card.col, IT, Leu	🖌 כרטיסים - עסקים - שלום יוסף אלישע א
Public key RSA (2048 Bits) Public key parameters 05 00	ירוט החיובים והעסקאות
Authority Key Identifier KeyIT)=060611c823151d5262 Y 30 82 01 00 02 82 01 01 00 82 32 32 3 A	ים והעסקאות שלי
60 0 11 40 05 01 01 01 01 01 07 03 09 02 04 62 04 c4 d5 c6 77 34 0f 24 c9 c2 fa 13 c2 02 d4 23 a7 66 47 20 cb 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 80 11 e9 2c 41 11 a 92 be 5b ba 44 13 a7 b2 8a 67 67 7 db 13 b9 b3 5d c2 78 02 95 22 8 d4 47 8e b4 39 82 ✓	איזה כרטיס כל הכרטיסים הפעילים ▼ סוג העסקה הכל ▼ תציגו לי (€)
Copy to Fie	שע אברון נאוט נאזא) דרם - עסקאות בש"ח(נאזא) דרם - עסקאות בש"ח(נאזא)

<ロ> < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Shor's algorithm

The quantum threat

Shor algorithm

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



Quantum computer

Allows for fast factoring

poll 1

JA (Technion)

Shor's algorithm

October 15, 2020 5/17

The potential disaster/benefits

If a fast factoring algorithm is found

. . .

Bad	Good
The bastards read your email	You read the mail of the bastard
Internet insecure	Dark-net is insecure
Financial transaction insecure State records exposed	Money laundering more difficult State records exposed



. . .

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

Factoring Oracle

Weak and unreliable is good enough



Verify answer on a classical computer

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

JA (Technion)

Shor's algorithm

October 15, 2020 7/17

Math Preliminaries

Facts from number theory

poll 2

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

Factoring reduces to finding the period of a^k mod N
pq = N
(p − 1)(q − 1) = Integer × period (a^k mod N) Number theory then gives p, q

More math preliminaries

Fourier transform and its Discrete cousin

•
$$\tilde{F}(f) = \frac{1}{\sqrt{2\pi}} \int e^{ift} F(t) dt$$

• $e^{i\omega t} \Longrightarrow \delta(f - \omega)$
Discrete Fourier: $\omega = e^{2\pi i/L}$
root of unity
 $\tilde{F}(m) = \sum_{k=1}^{L} \mathcal{F}_{km} F(k), \quad \mathcal{F}_{km} = \frac{\omega^{km}}{\sqrt{L}}$
 \mathcal{F} : unitary matrix

poll 3

◆□ → ◆□ → ◆三 → ◆三 → ◆ ○ ◆ ○ ◆

Periodic functions

Fourier transform is sparse



JA (Technion)

October 15, 2020 10/17

Functions contain exponential amount of information

How many bits to store a function with $N = 2^n$ arguments?



JA (Technion)

Shor's algorithm

October 15, 2020 11/17

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

The superposition advantage

- n qubits encode one k
- k takes $N = 2^n$ values
- Superpositions: No extra qubits

• 2*n* qubits encode $\{k, F(k)\}$



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

JA (Technion)

October 15, 2020 12/17

・ロト ・ 理 ト ・ ヨ ト ・ ヨ ト … ヨ

No free-lunch principle

Measurement reveals one random F(k)



Measurement reveals

• one, random, entry k and the corresponding F(k)

JA (Technion)

October 15, 2020 13/17

Shor algorithm

Quantum Fourier: Exponential improvement on FFT

• Under the hood: massive superposition

$$\underbrace{|0\ldots0\rangle}_{argument \ function} \underbrace{|a^{0}\rangle}_{+\cdots+|1\ldots1\rangle|a^{L-1}\rangle}$$

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

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



If you look twice the cat is dead

Fourier: One look suffices



You also need to be lucky

1 and N are trivial factors

- Bad luck: Measure $|0\rangle$
- Learn nothing:
 0 × period = integer × L



2 ^k Mod 15	1	2	4	8	1	2	
m	0	1	2	3	4	5	
<i>Fourier</i> ²	1	0	0	0	1		0

October 15, 2020 16/17

Moral: Store information in states not in amplitudes

Be wise and modest

Fourier= Interference

- Computational States: Revealed in single shot
- Amplitudes: Revealed in statistics



Amplitudes: The roulette in the quantum casino

	(T				
.IA	lec	nnion	۱.		
0, 1	100		,		

Shor's algorithm

October 15, 2020 17/17

・ロト ・ 理 ト ・ ヨ ト ・ ヨ ト … ヨ