Shor's algorithm The magic of the Quantum Fourier transform

J Avron

March 2, 2022

JA (Technion)

Shor's algorithm

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >
 March 2, 2022

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

•
$$N_{public} = p \times q_{secret}$$



RSA security

- *f*, *g* are known functions
- Cipher = (Message)^e Mod N, Message = (Cipher)^d Mod N
- $e \times d = Mod(p-1)(q-1)$, e=public, d=private
- Security rests on the presumed difficulty of factoring

Shor's algorithm

Everybody uses RSA

All the time

Certificate ×	🗴 Quantum computers: Cras: 🗙 🕍 Inbox – avronj@gmail.com x
General Details Certification Path	//Transactions/ChargesDeals.aspx?utm_source=DapapEmail&utm_source=DapapEmail&utm_mediur
Show: <all></all>	ארץ 🔞 Avron 峰 Translate 🧕 arXiv 🖌 Inbox 🕅 Moodle 🜌 Portal 💽 IBM Q 🛛
Field Value ^ Signsture hash algorithm sha 256 Issuer Signsture hash algorithm puGcet 514/2 Secure Server Valid from Valid from Tuesday, August 14, 2010 02: Valid to Valid to Widersday, October 30, 201 Online Lewis cold, IT, Lew	לקוח פרטי לקוח עסקי לקוח פרטי לקוח עסקי אלושע א 🔾 חיפוש 🔒 ברטיסים - עסקים -
Public key RSA (2048 Bits) Public key parameters 05 00	ירוט החיובים והעסקאות
M Buttweity Kaus Identifier KeustTm_m060611:e32346145297 ✓ 30 82 01 0 86 48 3a c3 60 2f 65 84 9d 45 97 86 97 64 12 77 86 97 64 12 62 89 52 94 62 ae c4 55 77 34 61 42 c2 at 38 95 52 94 62 ae c4 57 77 34 61 42 c2 at 30 33 dc c4 55 64 72 c5 35 ff 107 53 36 c9 25 54 67 76 55 51 17 51 33 dc c4 13 36 28 67 77 b1 13 92 b3 54 32 27 76	ים והעסקאות שלי איזה כרטיס סוג העסקה הכל יו תציגו לי ס
Edit Properties Copy to File	שע אברון UNI (4716) דם – עסקאות בש"ח (4716) 25/11/2018 - 15/01/2019 חיוב. שם בית העסק פוג עסקה פכום עסקה פכום חיוב 18 הערות

Shor's algorithm March 2, 2022 4/17

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

The quantum threat

Shor algorithm

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



Quantum computer

Allows for fast factoring

JA (Technion)

Shor's algorithm

< □ > < @ > < E > < E > E March 2, 2022

The potential disaster/benefits

If a fast factoring algorithm is found

. . .

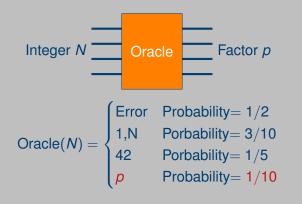
Bad	Good
The bastards read your email	You read the mail of the bastard
Internet insecure	Dark-net is insecure
Financial transaction insecure State records exposed	Money laundering more difficult State records exposed



. . .

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

March 2, 2022

< ∃ > _

Math Preliminaries

Facts from number theory

- $a^k \mod N$: A periodic function of k, assuming gcd(a, N) = 1
- Example: a = 2, N = 15 the 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 \times period
- Period gives information on the private key

More math preliminaries

Fourier transform and its Discrete cousin

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

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

$$F(t)$$

$$\widehat{F}(f)$$

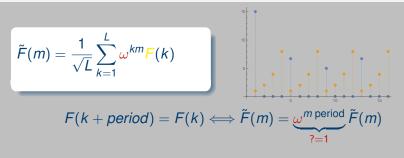
$$\widehat{F}(f)$$

$$f$$

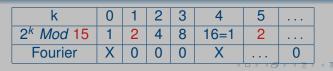
< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > 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

Periodic functions

Fourier transform is sparse



F(*m*) ≠ 0 ⇒ *m* × period = (Integer) × *L period* = (*integer*)*L*/*m*



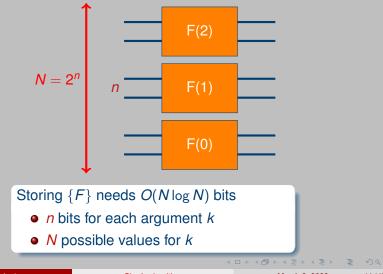
JA (Technion)

March 2, 2022

10/17

Functions contain exponential amount of information

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



JA (Technion)

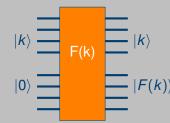
Shor's algorithm

March 2, 2022

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

The superposition advantage

- *n* bits encode one *k*
- *n* bits encode F(k)
- *n* qubits for 2^{*n*} bits in superposition
- $(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \cdots \otimes (|0\rangle + |1\rangle)$
- 2*n* qubits encode $\{k, F(k)\}$

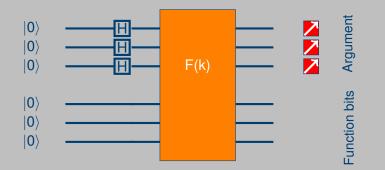


$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} |0\rangle \xrightarrow{\text{Function gate}} \frac{|0\rangle |F(0)\rangle + |1\rangle |F(1)\rangle}{\sqrt{2}}$$

・ロン ・雪 と ・ ヨ と

No free-lunch principle

The massive superposition is only in the belly of the beast



Measurement reveals

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

JA I		

・ロ・・ 日本・ ・ 日本・

Shor algorithm

Quantum Fourier: Exponential improvement on FFT

Under the hood: massive superposition



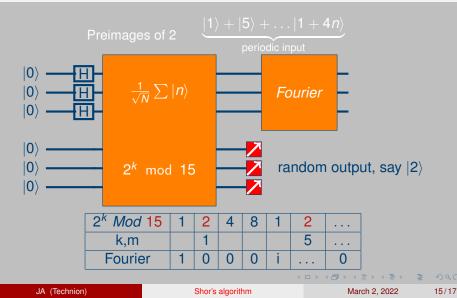
- Measure function register $|a^k\rangle$
- Get: Random outcome, e.g. $|a^k\rangle = |2\rangle$
- Argument register: superposition of pre-images of $|2\rangle$

$$\underbrace{\left(|1\rangle + |1+4\rangle + |1+2\times 4\rangle + |1+3\times 4\rangle \right)}_{\otimes |2\rangle} \otimes |2\rangle, \quad 2^{1+4n} = 2 \mod$$



If you look twice the cat is dead

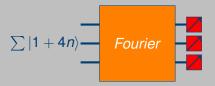
Don't query the argument: Interfere



You also need to be lucky

You may not get enough information on the period

- 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

March 2, 2022

Moral: Information in basis states exposed in one shot

Information in amplitudes is inaccessible in one shot

Fourier= Interference

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



Amplitudes: The roulette of the quantum casino

	hnion	

Shor's algorithm

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