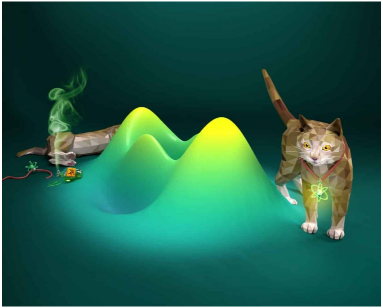
Classical cryptography
Quantum computations

Ivan Murashko

Introduction

- Quantum mechanics
- Quantum computations
- Symmetric cryptography. Grover search algorithm (GSA)
- Public-key cryptography cryptography (RSA, Diffie-Hellman, Elliptic curve) and Shor's algrorithm.

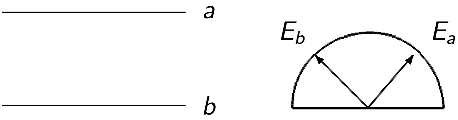
Quantum world vs Classical one



They differ. There are 2 examples

1. Schrödinger's cat, two-level atom and q-bit (quantum bit)
2. Bell experiment, negative probability and quantum logic

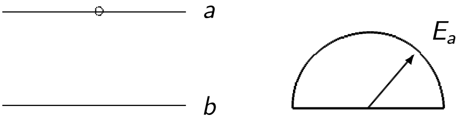
Two-level atom, q-bit



$$|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$$

Figure: Energy measurement for two-level atom. The atom is in pure state: $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Device can get either E_a or E_b.

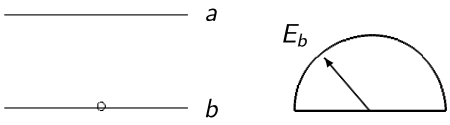
Two-level atom. E_a measurement



$$|\psi\rangle \to |a\rangle$$

Figure: Energy measurement for two-level atom. The atom is in pure state: $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Device got E_a. The following wave function collapse occurs as a result of the measurement $|\psi\rangle \to |a\rangle$

Two-level atom. E_b measurement



$$|\psi\rangle \to |b\rangle$$

Figure: Energy measurement for two-level atom. The atom is in pure state: $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Device got E_b. The following wave function collapse occurs as a result of the measurement $|\psi\rangle \to |b\rangle$

Schrödinger's cat

Classical bit vs quantum q-bit

Classical bit is either 0 or 1.
Quantum q-bit is another case. It's a state $|q\rangle = \alpha |0\rangle + \beta |1\rangle$. I.e. as Schrödinger's cat it can be 1 (die) and 0 (alive) simultaneously

Bell experiment. Classical case

$$f = \frac{1}{2}\left(ab + a'b + ab' - a'b'\right), a, a', b, b' \in \{-1, +1\}.$$

therefore $f \in \{-1, +1\}$ and $|\langle f \rangle| \leq 1$

Bell experiment. Quantum case

$$|\langle f \rangle| = \sqrt{2} > 1$$

Negative probabilities

$$\langle f \rangle = \sum_{a,a',b,b'} p(a,a',b,b') f(a,a',b,b').$$

therefore for $|\langle f \rangle| > 1$ necessary to have

$$\exists a, a', b, b' : p(a,a',b,b') < 0$$

Heisenberg inequality

$$\Delta p \Delta q \geq \frac{\hbar}{2}$$

Quantum logic

Distributive law is failed for quantum logic:

- $P \wedge (Q_1 \vee Q_2)$ can be true
- but both $P \wedge Q_1$ as well as $P \wedge Q_2$ are false

in other words

$$P \wedge (Q_1 \vee Q_2) \neq (P \wedge Q_1) \vee (P \wedge Q_2)$$

where $\wedge$ is "logical and", $\vee$ is "logical or"

Quantum logic

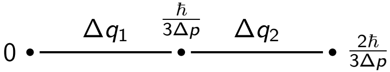


Figure: Heisenberg inequality. The event P is that momentum has uncertainty Δp Event $P \wedge Q_1$ is that particle's position is between 0 and $\frac{\hbar}{3\Delta p}$. Event $P \wedge Q_2$ is that particle's position is between $\frac{\hbar}{3\Delta p}$ and $\frac{2\hbar}{3\Delta p}$. Particle's position for event $P \wedge Q = (P \wedge Q_1) \vee (P \wedge Q_2)$ is between 0 and $\frac{2\hbar}{3\Delta p}$. The events $P \wedge Q_1$ and $P \wedge Q_2$ are forbidden by the Heisenberg inequality. From other side the event $P \wedge Q = (P \wedge Q_1) \vee (P \wedge Q_2)$ is possible

Classical computation

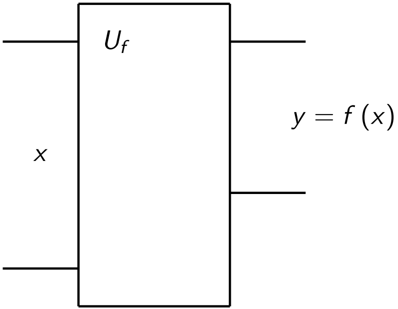


Figure: Classical computation. Input has a number x that consists of n bits. Output $y = f(x)$ is the result that consists of m bits

Quantum computations

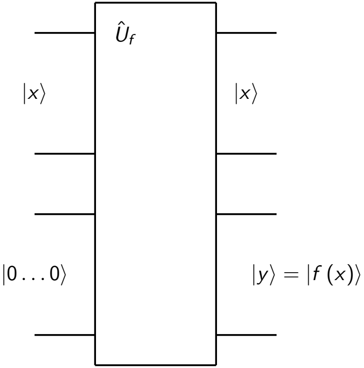


Figure: Quantum computations should be reversible. We have a number x as input. The number consists of n q-bits. We also require to have a seed of 0 states (m q-bits). Output also have two parts: the result $|y\rangle = |f(x)\rangle$ is described by m q-bits and initial state $|x\rangle$ (n q-bits)

Quantum computations

Classical case

$$x \to f(x)$$

Quantum case

$$\begin{gathered}|0\rangle\,|0\rangle + |1\rangle\,|0\rangle + |2\rangle\,|0\rangle + \dots + |x\rangle\,|0\rangle + \dots \to \\ \to |0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle + |2\rangle\,|f(2)\rangle + \dots + |x\rangle\,|f(x)\rangle + \dots\end{gathered}$$

Needle in a haystack task

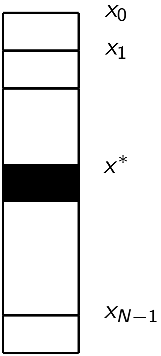


Figure: Search in unstructured data array (search "a needle in a haystack"). Classical complexity is $O(N)$

Grover search algorithm. Scheme

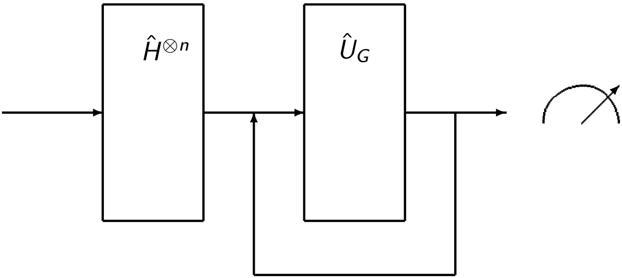


Figure: Grover search algorithm. Complexity is $O(\sqrt{N})$

Grover search algorithm. Repeating element scheme

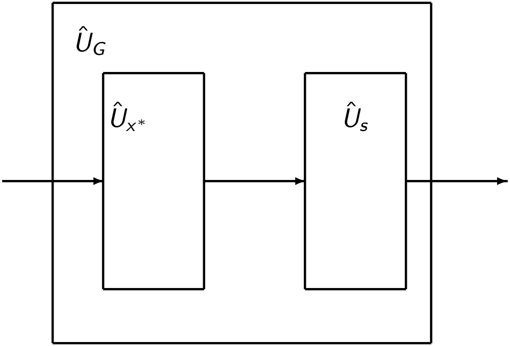


Figure: Grover search algorithm. Grover iteration

Grover search algorithm. Main principle

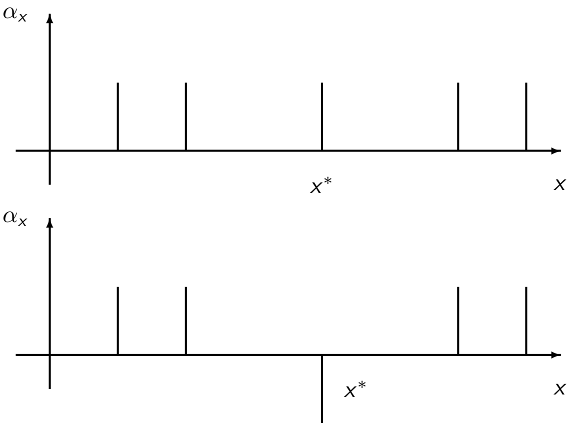


Figure: Grover search algorithm. Phase inversion aka conditional inversion

Grover search algorithm. Main principle

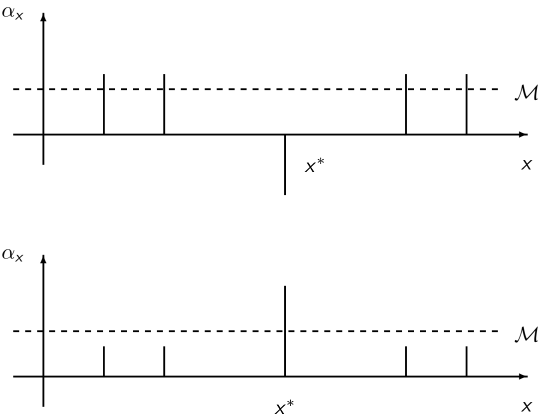


Figure: Grover search algorithm. Grover diffusion operator

Impact on classical cryptography

$O(N) \to O(\sqrt{N})$ leads to the following recommendation
$AES_{128} \to AES_{256}$

Public key cryptography

- RSA and factorisation problem
- Diffie-Hellman and discrete logarithm
- Elliptic curve and discrete logarithm

RSA and period-finding problem

$$N = p \cdot q$$

$$f(x, a) = a^x \mod N.$$

The period of the function is $T = 2r$, i.e.

$$\begin{aligned} a^{x+2r} \mod N = a^x \mod N, \\ a^{2r} \equiv 1 \mod N, \\ (a^r + 1)(a^r - 1) \equiv 0 \mod N \end{aligned}$$

Shor's algorithm

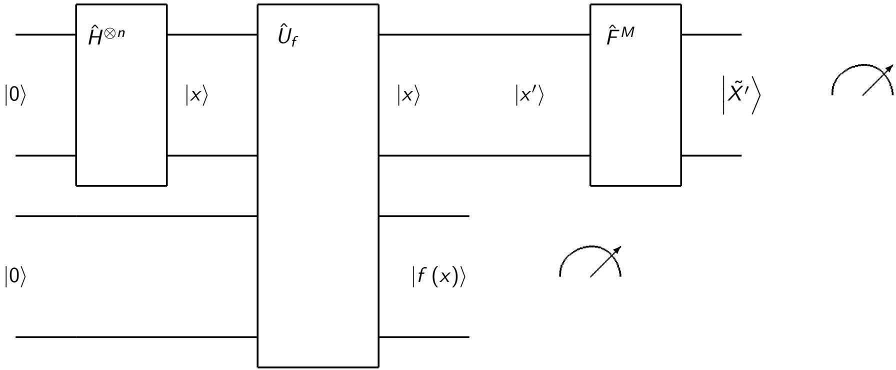


Figure: Period finding problem and quantum Fourier's transform

Shor's algorithm. Period funding problem for $f(x,a) = a^x \mod N$

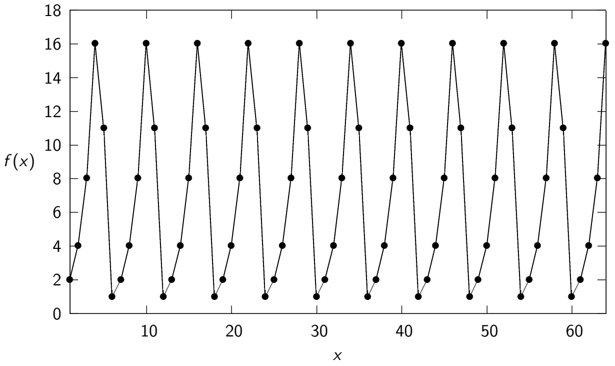


Figure: Shor's algorithm. Period funding problem for $f(x,a) = a^x \mod N$, $a = 2,\ N = 21$.

Shor's algorithm. Period funding problem for $f(x,a) = a^x \mod N$

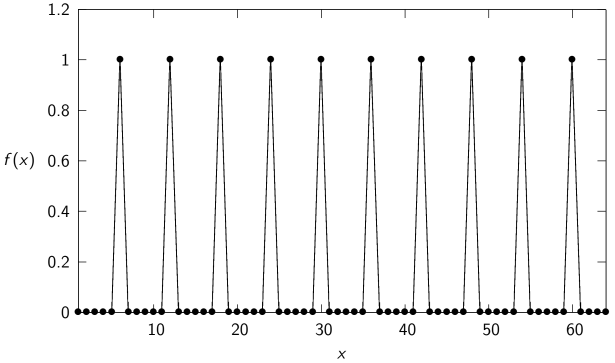


Figure: Shor's algorithm. Period funding problem for $f(x,a) = a^x \mod N$, $a = 2$, Value 1 is repeated with period of $T = 6$.

Shor's algorithm. Period funding problem for $f(x,a) = a^x \mod N$

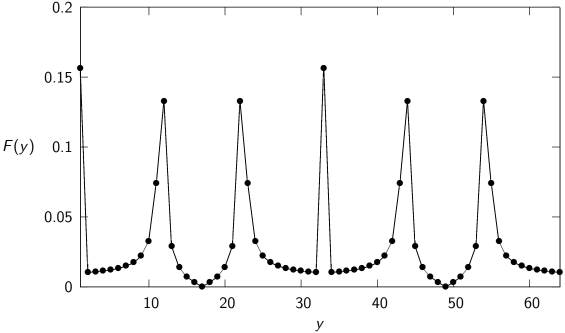


Figure: Shor's algorithm. Period funding problem for $f(x,a) = a^x \mod N$, $a = 2$. Local maxima of Fourier transform are repeated with period $\frac{M}{r} \approx 10.67$ ($M = 64$ is the number of samples for Fourier transform). This gives us $T \approx 6$

Shor's algorithm. Period funding problem for $f(x,a) = a^x \mod N$

Local maxima of Fourier transform are repeated with period $\frac{M}{r} \approx 10.67$ ($M = 64$ is the number of samples for Fourier transform). This gives us $T \approx 6$ and as therefore $r = \frac{T}{2} = 3$.
As result (in our case) $(a^r - 1) = 7$ and $(a^r + 1) = 9$ have common divisors with $N = 21$: 7 and 3.

Public key cryptography. Recommendations for key length

All key sizes are provided in bits. These are the minimal sizes for security.
Click on a value to compare it with other methods.

Year	Symmetric	Factoring (modulus)		Discrete Logarithm		Elliptic Curve	Hash
		Optimistic	Conservative	Key	Group		
2015	78	1245	1350	156	1245	156	156
2016	79	1273	1392	158	1273	158	158
2017	**80**	**1300**	**1435**	**159**	**1300**	**159**	**159**
2018	80	1329	1478	160	1329	160	160
2019	81	1358	1523	162	1358	162	162

To resist until year 2017, you may consider using a minimum of 80-bit key for symmetric systems (e.g. AES-128) and a minimum of 1440-bit key for asymmetric systems (e.g. RSA).

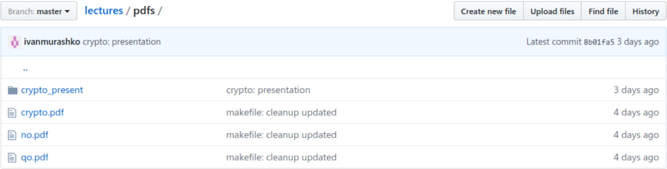
Impact on public-key cryptography

- RSA: 4096
- DH: 2048/256
- Elliptic curve: 512/256 (bitcoin)

NSA doesn't recommend elliptic curve cryptography for internal usage.

Additional info

https://github.com/ivanmurashko/lectures/tree/master/pdfs



Questions


SHRODINGER VS. HEISENBERG
CAT-DEAD OR ALIVE?
WHAT DO YOU THINK?
I DON'T KNOW
cloudcomics.blogspot.com
Cloud Comics © 2012