

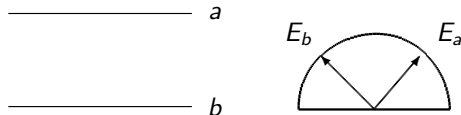
Classical cryptography Quantum computations

Ivan Murashko

Introduction

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

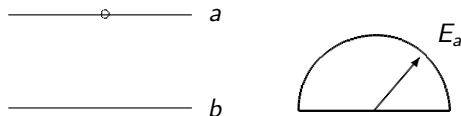
Two-level atom



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

Рис.: 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 .

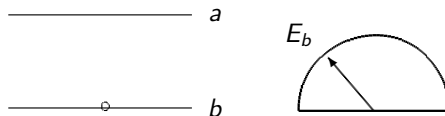
Two-level atom. E_a measurement



$$|\psi\rangle \rightarrow |a\rangle$$

Рис.: 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 $|\psi\rangle \rightarrow |a\rangle$

Two-level atom. E_b measurement



$$|\psi\rangle \rightarrow |b\rangle$$

Рис.: 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 $|\psi\rangle \rightarrow |b\rangle$

Schrödinger's cat



Эксперимент Белла. Классический случай

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

следовательно $f \in \{-1, +1\}$ и $|\langle f \rangle| \leq 1$

Эксперимент Белла. Квантовый случай

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

Отрицательные вероятности

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

следовательно для $|\langle f \rangle| > 1$ необходимо

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

Классические вычисления

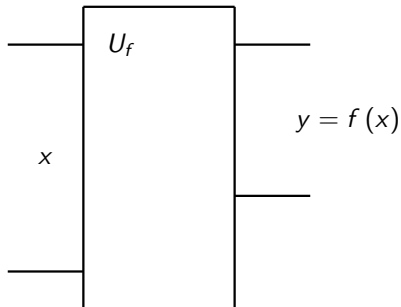


Рис.: Классические вычисления. На вход подается число x состоящее из n бит, а на выходе имеем результат $y = f(x)$ описываемый m битами

Квантовые вычисления

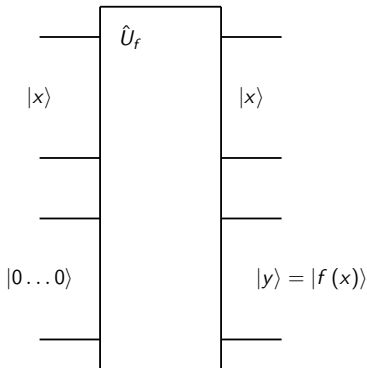


Рис.: Квантовые обратимые вычисления. На вход подается число $|x\rangle$ состоящее из n кубит и затравка из нулевых состояний (m кубит), а на выходе имеем результат $|y\rangle = |f(x)\rangle$ описываемый m кубитами и исходное состояние $|x\rangle$

Квантовые вычисления

Классический случай

$$x \rightarrow f(x)$$

Квантовый случай

$$\begin{aligned} &|0\rangle |0\rangle + |1\rangle |0\rangle + |2\rangle |0\rangle + \dots + |x\rangle |0\rangle + \dots \rightarrow \\ &\rightarrow |0\rangle |f(0)\rangle + |1\rangle |f(1)\rangle + |2\rangle |f(2)\rangle + \dots + |x\rangle |f(x)\rangle + \dots \end{aligned}$$

Задача о поиске иголки в стоге сена

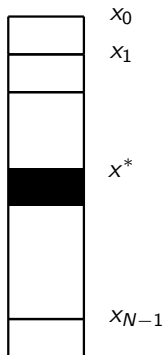


Рис.: Поиск в неструктурированном объеме данных (поиск "иголки в стоге сена"). Классическая сложность $O(N)$

Алгоритм Гровера. Схема

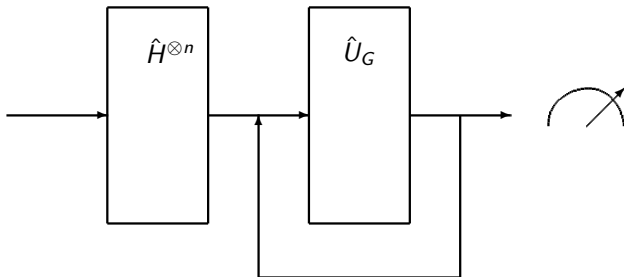


Рис.: Алгоритм Гровера. Сложность $O(\sqrt{N})$

Алгоритм Гровера. Схема повторяющегося элемента

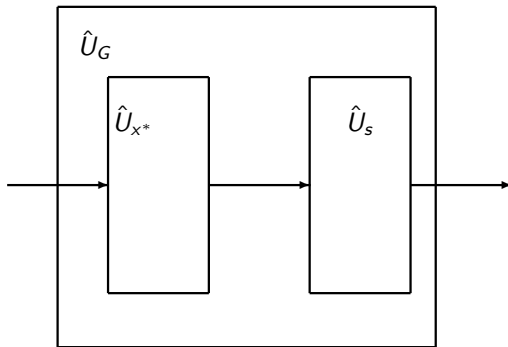


Рис.: Алгоритм Гровера. Повторяющийся элемент

Алгоритм Гровера. Принцип работы

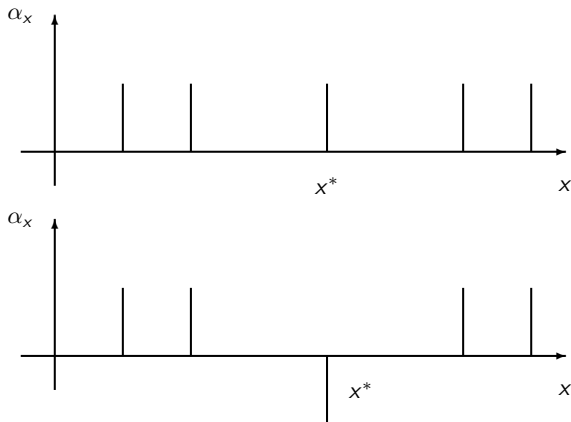


Рис.: Алгоритм Гровера. Инверсия фазы

Алгоритм Гровера. Принцип работы

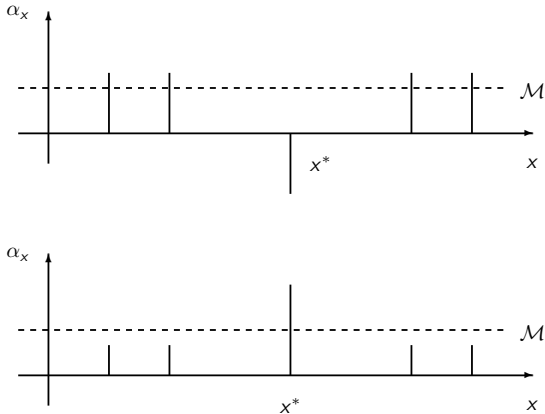


Рис.: Алгоритм Гровера. Обращение относительно среднего.

Влияние на рекомендации к использованию

$O(N) \rightarrow O(\sqrt{N})$ ведет например к следующей рекомендации
 $AES_{128} \rightarrow AES_{256}$

Несимметричное шифрование

- RSA и задача факторизации чисел
- Diffie-Hellman и дискретный логарифм
- Elliptic curve и дискретный логарифм

RSA и задача о нахождении периода функций

$$N = p \cdot q$$

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

Период функции $T = 2r$, т.е.

$$a^{x+2r} \mod N = a^x \mod N,$$

$$a^{2r} \equiv 1 \mod N,$$

$$(a^r + 1)(a^r - 1) \equiv 0 \mod N$$

Алгоритм Шора

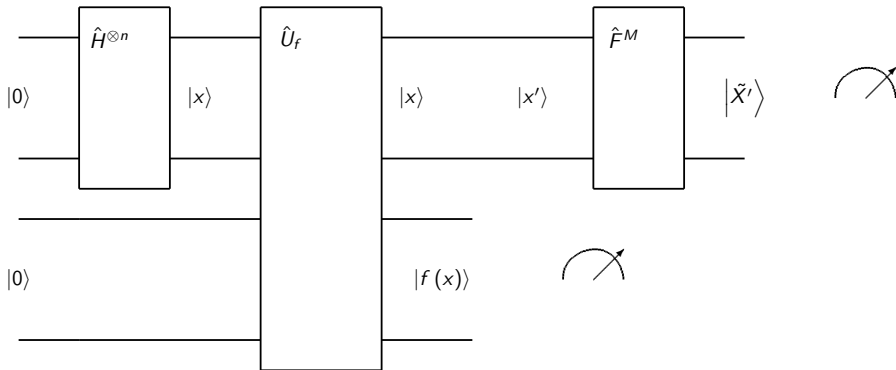


Рис.: Определение периода функций с помощью квантового преобразования Фурье

Алгоритм Шора. Нахождение периода функции $f(x, a) = a^x \bmod N$

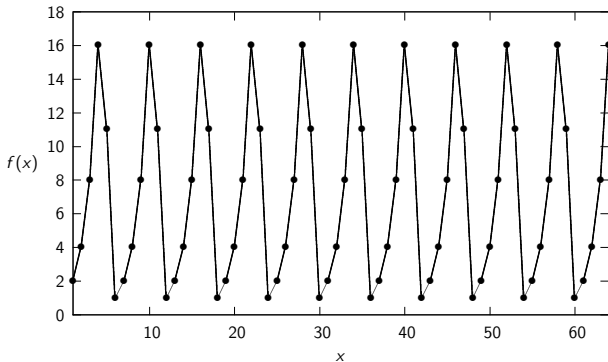


Рис.: Алгоритм Шора. Нахождение периода функции $f(x, a) = a^x \bmod N$ при $a = 2$, $N = 21$.

Алгоритм Шора. Нахождение периода функции $f(x, a) = a^x \bmod N$

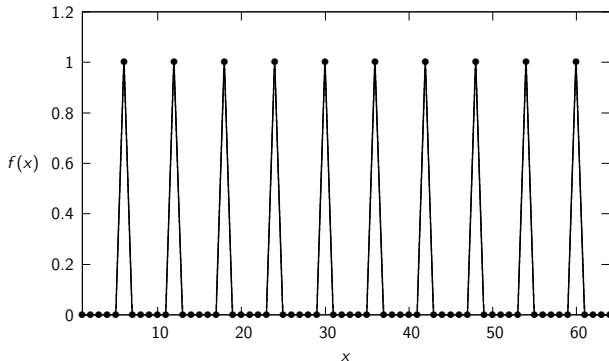


Рис.: Алгоритм Шора. Нахождение периода функции $f(x, a) = a^x \bmod N$ при $a = 2$, Значение функции 1 повторяется с периодом $r = 6$.

Алгоритм Шора. Нахождение периода функции $f(x, a) = a^x \bmod N$

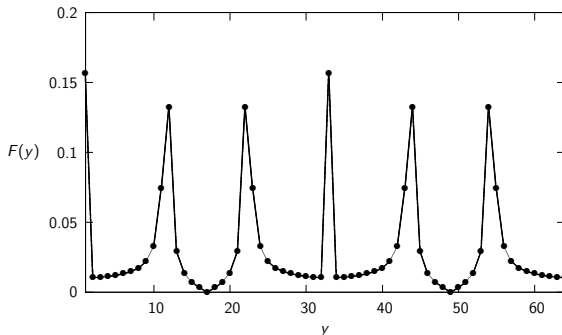


Рис.: Алгоритм Шора. Нахождение периода функции $f(x, a) = a^x \bmod N$ при $a = 2$. Локальные максимумы преобразования Фурье идут с периодом $\frac{M}{r} \approx 10.67$ ($M = 64$ - число отсчетов для преобразования Фурье)

Рекомендованные значения для длины ключа

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).

Влияние на рекомендации к использованию

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

NSA не рекомендует использование алгоритмов на эллиптических кривых для внутреннего использования.

Что дальше?

- Линейная алгебра (Матрицы)
- Дискретная математика (Операции с остатком)

Что дальше?

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

Branch: master ▾


lectures / pdfs /

Create new file

Upload files

Find file


History

 ivanmurashko

crypto: presentation


Latest commit 8b01fa5 3 days ago

..

 crypto_present


crypto: presentation

3 days ago

 crypto.pdf


makefile: cleanup updated

4 days ago

 no.pdf

makefile: cleanup updated

4 days ago

 qo.pdf

makefile: cleanup updated

4 days ago

Вопросы

SHRODINGER VS. HEISENBERG



CAT-DEAD OR ALIVE?
WHAT DO YOU THINK?

I DON'T KNOW

cloudcomics.blogspot.com

Cloud Comics © 2012