Классическая криптография
Квантовые вычисления

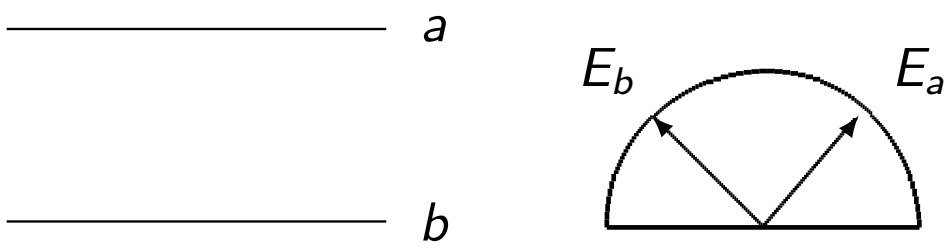
Мурашко И. В.

Санкт Петербургский Государственный Политехнический Университет

Введение

- Квантовая механика
- Квантовые вычисления
- Методы симметричного шифрования и алгоритм Гровера
- Методы несимметричного шифрования (RSA, Diffie-Hellman, Elliptic curve) и алгоритм Шора.

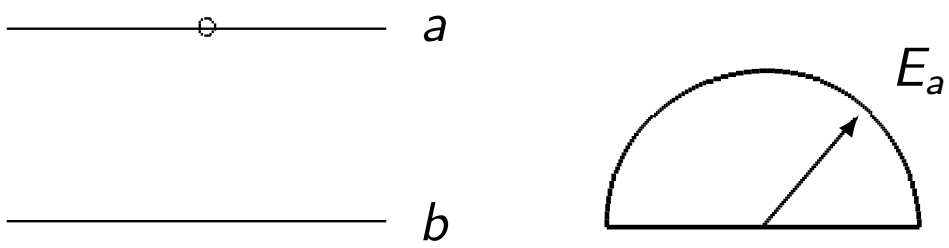
Двухуровневый атом



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

Рис.: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Прибором регистрируется значение энергии E_a или E_b.

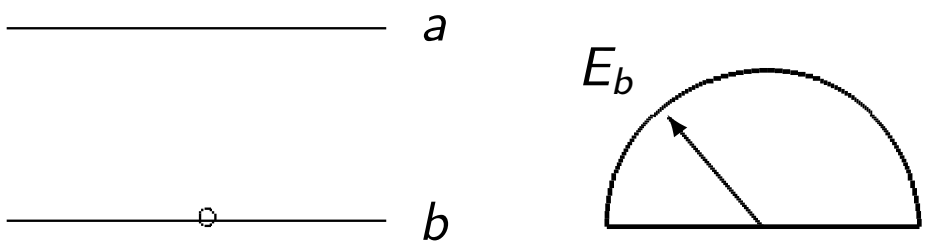
Двухуровневый атом. Измерение E_a



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

Рис.: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Прибором регистрируется значение энергии E_a. При измерении происходит следующая редукция $|\psi\rangle \to |a\rangle$

Двухуровневый атом. Измерение E_b



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

Рис.: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Прибором регистрируется значение энергии E_b. При измерении происходит следующая редукция $|\psi\rangle \to |b\rangle$

Кот Шредингера

Эксперимент Белла. Классический случай

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

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

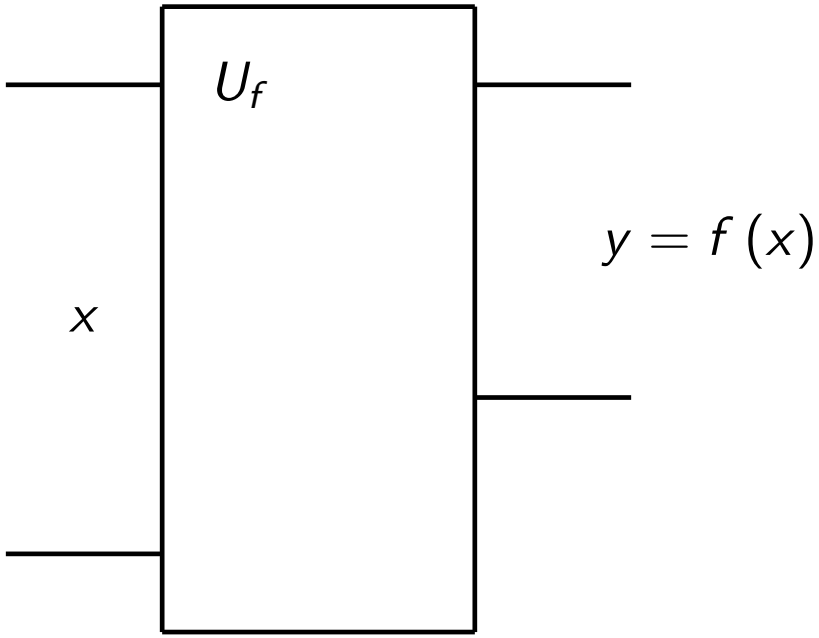


Рис.: Классические вычисления. На вход подается число x состоящее из n бит, а на выходе имеем результат $y = f(x)$ описываемый m битами

Квантовые вычисления

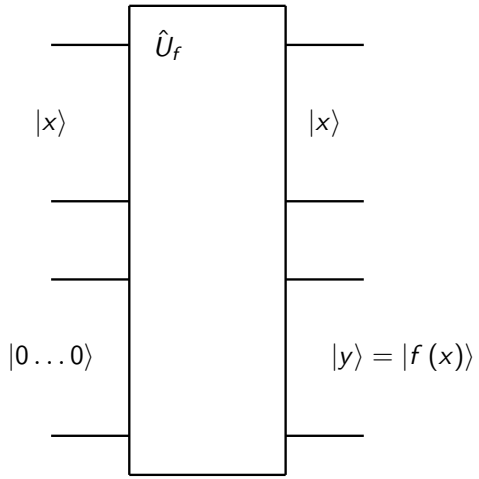


Рис.: Квантовые обратимые вычисления. На вход подается число $|x\rangle$ состоящее из n кубит и затравка из нулевых состояний (m кубит), а на выходе имеем результат $|y\rangle = |f(x)\rangle$ описываемый m кубитами и исходное состояние $|x\rangle$

Квантовые вычисления

Классический случай

$$x \to f(x)$$

Квантовый случай

$$|0\rangle|0\rangle + |1\rangle|0\rangle + |2\rangle|0\rangle + \cdots + |x\rangle|0\rangle + \cdots \to$$
$$\to |0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle + |2\rangle|f(2)\rangle + \cdots + |x\rangle|f(x)\rangle + \ldots$$

Задача о поиске иголки в стоге сена

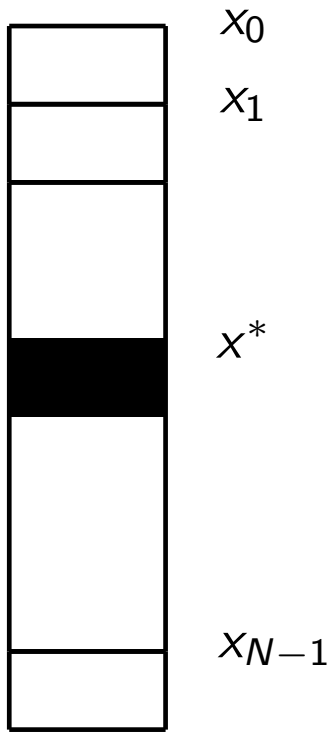


Рис.: Поиск в неструктурированном объеме данных (поиск "иголки в стоге сена"). Классическая сложность $O(N)$

Алгоритм Гровера. Схема

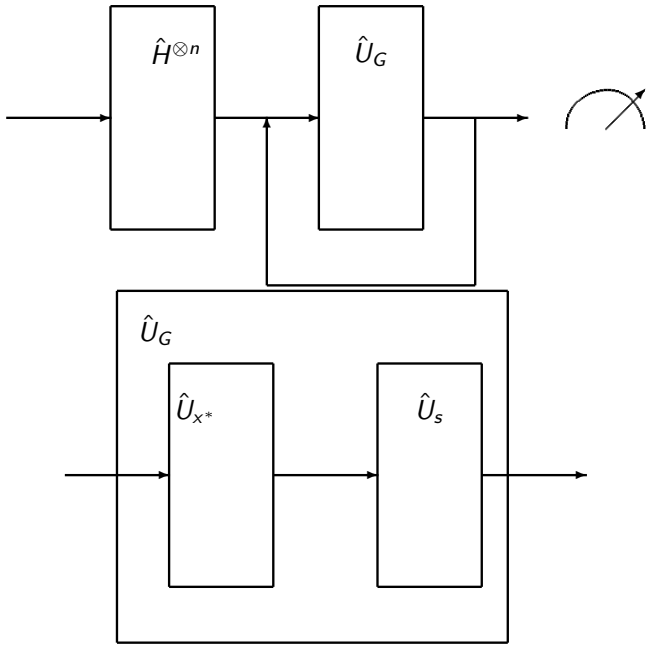


Рис.: Алгоритм Гровера. Сложность $O(\sqrt{N})$

Алгоритм Гровера. Принцип работы

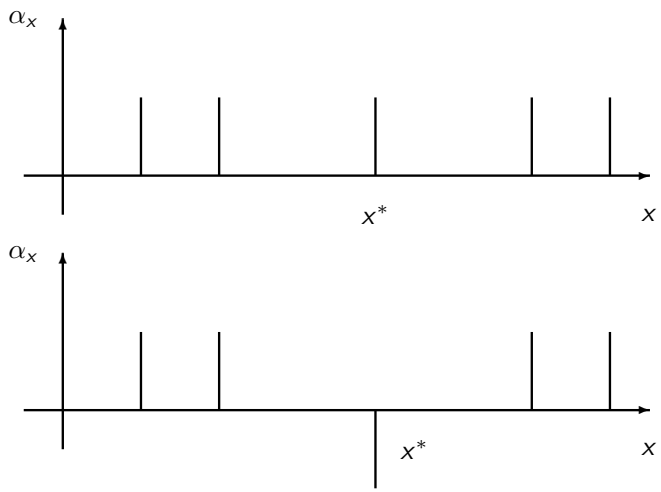


Рис.: Алгоритм Гровера. Инверсия фазы

Алгоритм Гровера. Принцип работы

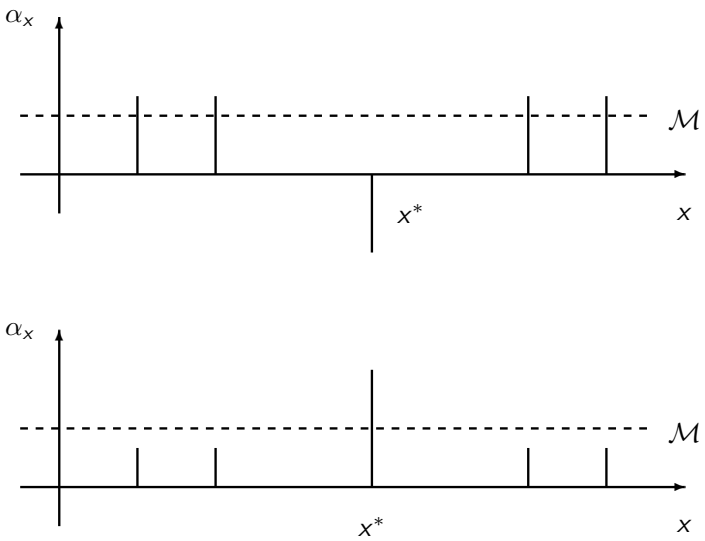


Рис.: Алгоритм Гровера. Обращение относительно среднего.

Влияние на рекомендации к использованию

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

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

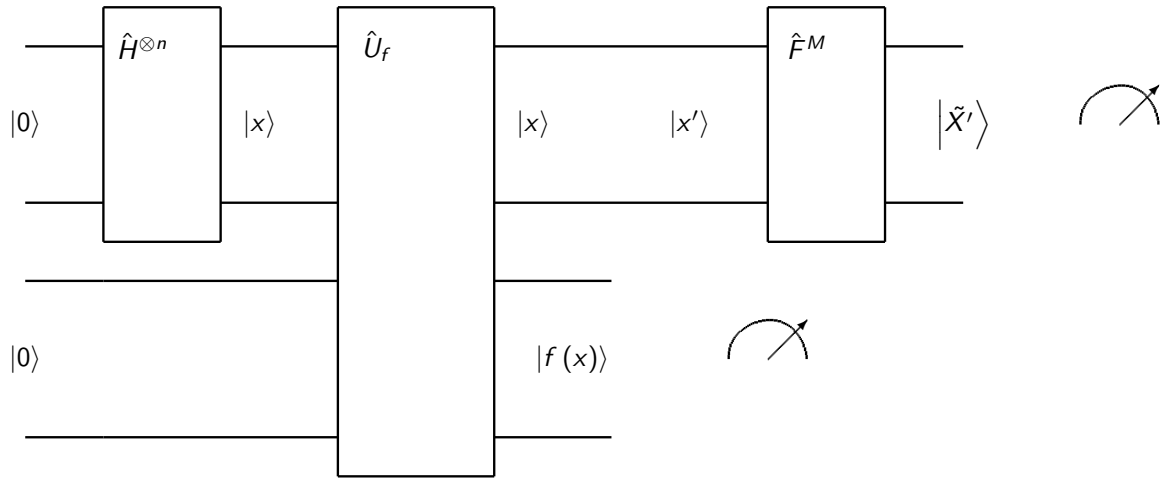


Рис.: Определение периода функций с помощью квантового преобразования Фурье

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

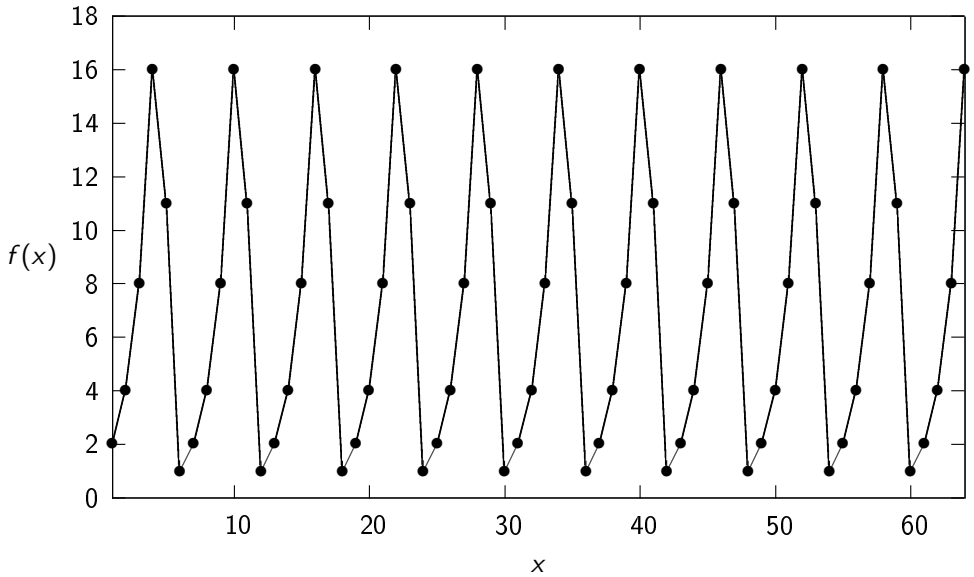


Рис.: Алгоритм Шора. Нахождение периода функции $f(x, a) = a^x \mod N$ при $a = 2$, $N = 21$.

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

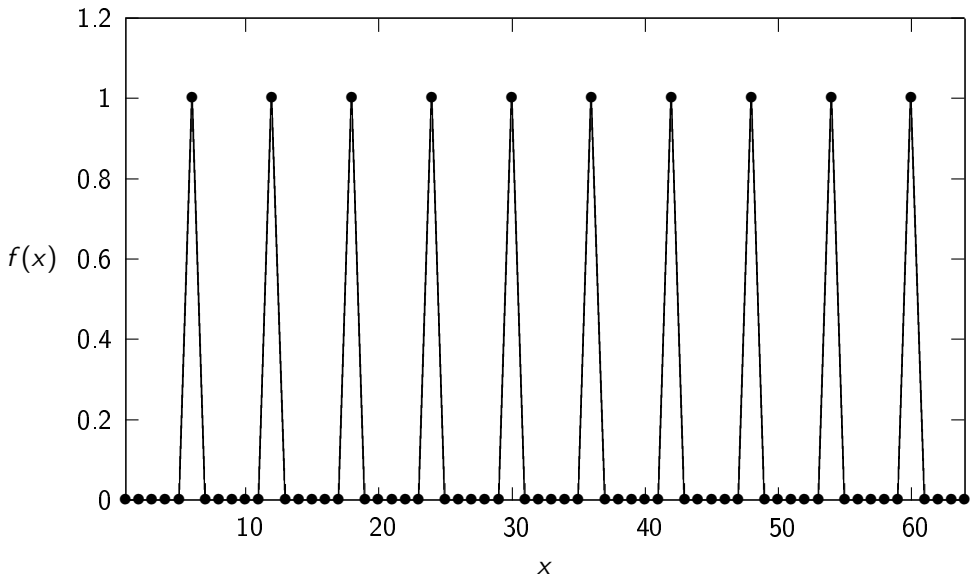


Рис.: Алгоритм Шора. Нахождение периода функции $f(x, a) = a^x \mod N$ при $a = 2$, Значение функции 1 повторяется с периодом $r = 6$.

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

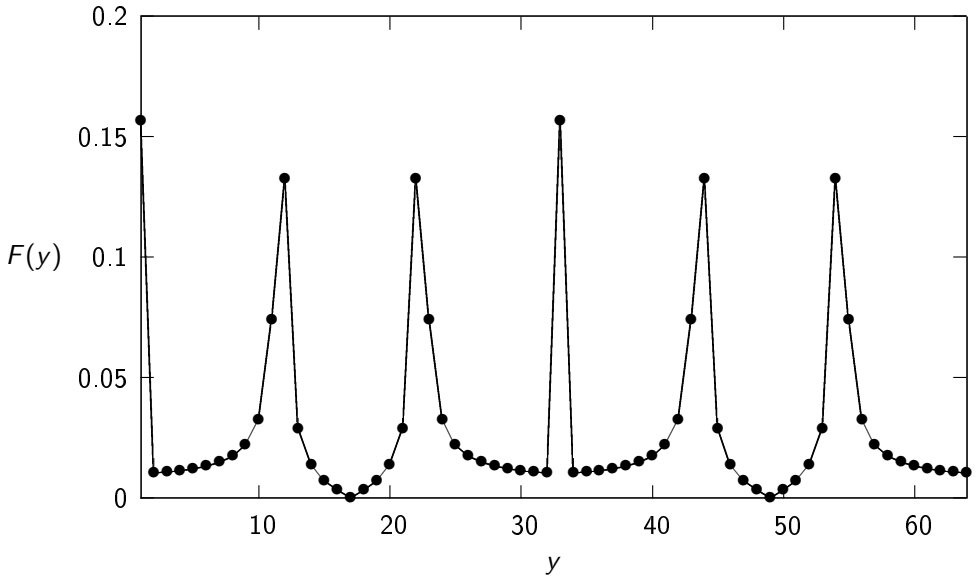


Рис.: Алгоритм Шора. Нахождение периода функции $f(x, a) = a^x \mod N$ при $a = 2$. Локальные максимумы преобразования Фурье идут с периодом $\frac{M}{r} \approx 10.67$ (M - число отсчетов для преобразования Фурье)

Влияние на рекомендации к использованию

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

Что дальше?

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

Вопросы


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