



AGH UNIVERSITY OF SCIENCE
AND TECHNOLOGY

Selected Topics in Cryptography

Quantum cryptanalysis

Szymon Szozda

Department of Telecommunications

04.12.2017

Quantum crypanalysis

Agenda

1. Bra-ket notation
2. Quantum gates
3. Grover's Database Search
4. Shore's factorization algorithm
 - Fast modular exponentiation
 - Quantum Fourier Transform
5. Implementation of quantum computer
 - Cold, Confined Atomic Ions
 - Cold, Confined Atoms
 - Quantum Dots
 - Superconducting Devices
 - NMR

Bra-ket notation

Definition

Bra-ket notation, also known as Dirac notation: $\langle x|y\rangle$ is a standard notation for describing quantum states. It can also be used to denote abstract vectors, linear functionals and scalar product in mathematics.

The left part: $\langle x|$, called the bra, is a row vector.

The right part: $|y\rangle$, called the ket, is a column vector.

A pure qubit state is a linear superposition of the basis states. This means that the qubit can be represented as a linear combination of $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

When we measure this qubit in the standard basis, the probability of outcome $|0\rangle$ is $|\alpha|^2$ and the probability of outcome $|1\rangle$ is $|\beta|^2$.





Because the absolute squares of the amplitudes equate to probabilities, it follows that α and β must be constrained by the equation

$$|\alpha|^2 + |\beta|^2 = 1$$

In quantum computing and specifically the quantum circuit model of computation, a quantum gate (or quantum logic gate) is a basic quantum circuit operating on a small number of qubits.

Gates

Example

Gate	Notation	Matrix
NOT (Pauli- X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli- Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
CNOT (Controlled NOT)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Unitary Transformation

Definition

Unitary transformation is transformation that preserves the inner product (isometry).

It is a bijective function:

$$U : H_1 \rightarrow H_2$$

where H_1 and H_2 are Hilbert spaces, such that:

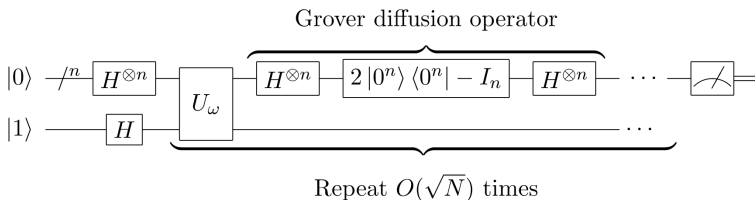
$$\langle Ux, Uy \rangle_{H_2} = \langle x, y \rangle_{H_1}$$

Grover's database search

Grover's database search uses ability of quantum computing to parallel process of qubits. The algorithm allows us to find selected element in unsorted set with complexity \sqrt{n} .

Grover's database search

Scheme



Group Theory

Abelian group

In abstract algebra, an abelian group, also called a commutative group, is a group in which the result of applying the group operation to two group elements does not depend on the order in which they are written.

Group theory

Multiplicative group of integers modulo n

Multiplicative group of integers modulo n is an abelian group.
The set of classes relatively prime to n is closed under multiplication:

$$\gcd(a, n) = 1 \wedge \gcd(b, n) = 1 \rightarrow \gcd(ab, n) = 1$$

1. Pick a random number $a < N$ and compute $\gcd(a, N)$.
2. If $\gcd(a, N) \neq 1$, then this number is a nontrivial factor of N , so we are done.
3. Otherwise, use the period-finding subroutine (below) to find r , the period of the following function:

$$f(x) = a^x \bmod N$$

i.e. the order r of a in $(\mathbb{Z}_N)^\times$, which is the smallest positive integer r for which $f(x+r) = f(x)$, or

$$f(x+r) = a^{x+r} \bmod N \equiv a^x \bmod N$$

4. If r is odd, go back to step 1.
5. If $a^{\frac{r}{2}} \equiv -1 \bmod N$, go back to step 1.
6. $\gcd(a^{\frac{r}{2}} + 1, N)$ and $\gcd(a^{\frac{r}{2}} - 1, N)$ are nontrivial factors of N .

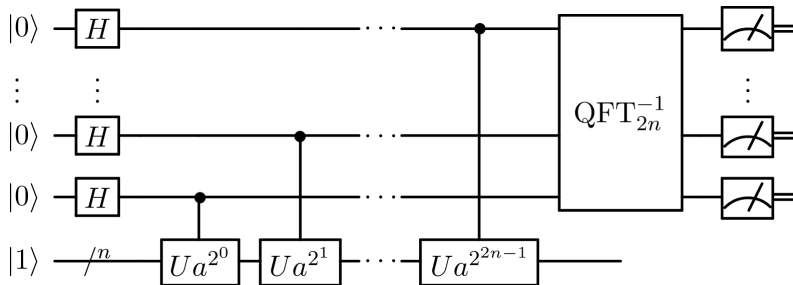
Fast exponentiation

We can calculate $A^B \bmod (C)$ quickly, using modular multiplication rules:

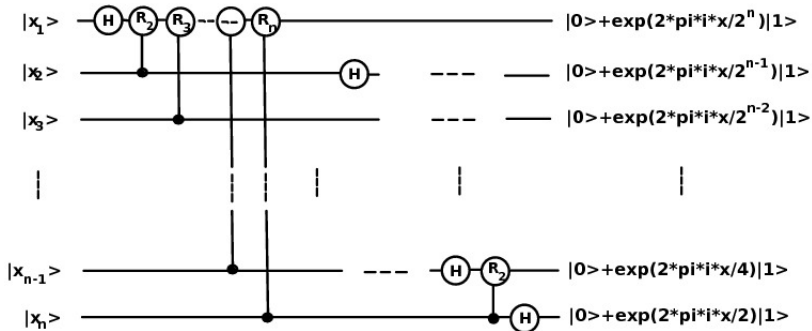
$$A^2 \bmod (C) = (A * A) \bmod (C) = ((A \bmod (C)) * (A \bmod (C))) \bmod (C)$$

Shor

Scheme



Quantum fourier transform



Cold, Confined Atomic Ions

Overview

Cold, Confined Atomic Ions technique uses laser beam to cool atomic ions, which are inside ion trap. After this process ions are organized in stable array. Qubit is represented with different levels of electron energy. We could pump ion with specific energy laser beam to change its state. Reading could be done in the same way.

Quantum Dots are a nano-scale crystals ($1^{-9}m$). As the size of QD is similar to De Broglie wave length, the structure is a kind of a trap for specific energy, free electrons. There is also possible QD design, such that it could trap electrons by spin.

Nuclear Magnetic Resonance

Overview

Nuclear Magnetic Resonance quantum computing is the most mature and established among other methods. In NMR we use the bits as nuclear spins. Spin can be changed by applying radio-frequency in resonance with nuclear spin frequency.

Time for questions

Bibliography:

- Goong Chen, David A. Church, Berthold-Georg Englert, Carsten Henkel, Bernd Rohwedder, Marlan O. Scully, M. Suhail Zubairy, "Quantum Computing Devices", Chapman Hall CRC, 2016
- Oliver Morsh "Quantum Bits and Quantum Secres", WILEY-VCH Verlag, 2008
- Wikipedia, Shor's algorithm, <https://en.wikipedia.org/>

Thank you for attention!