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
   - Linear Optic Computers
   - Superconducting Devices
   - NMR

Bra-ket notation

Definition

Bra–ket 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.

Qbit

Definition

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

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

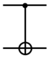
Gates
Definition

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)	$-\boxed{X}-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Z	$-\boxed{Z}-$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
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:

$$U : H_1 \to H_2$$

where $H_1 \quad \text{and} \quad H_2$ are Hilbert spaces, such that:

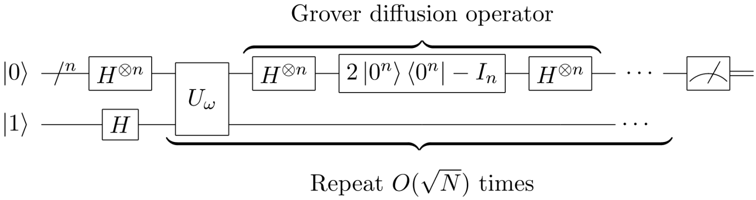
$$\langle Ux, Uy \rangle_{H_2} = \langle x, y \rangle_{H_1}$$

Grover's database search

Grover's database search uses ability of quantum computing to pararell 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

Abellian 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.

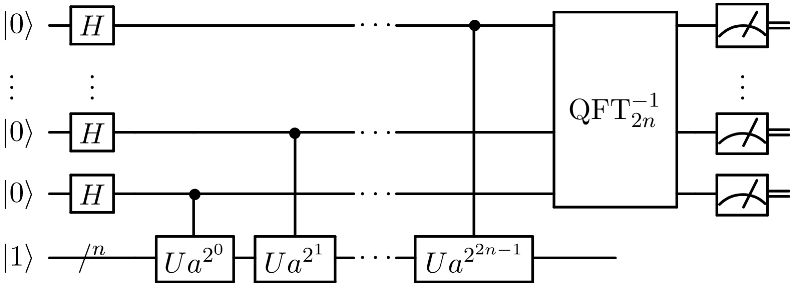
Multiplicative group of integers modulo n is an abelian group. The set of classes relatively prime to n is closed under multiplication:

$$gcd(a, n) = 1 \quad \text{and} \quad gcd(b, n) = 1 \quad => \quad gcd(ab, n) = 1$$

General Steps

Shor

Scheme



Fast exponentiation

We can calculate $A^B modC$ quickly, using modular multiplication rules:

$$A^2 modC = (A * A) modC = ((AmodC) * (AmodC)) modC$$

Quantum fourier transform

xyz

General Steps