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

Bra-ket notation

Origins

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

Origins

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

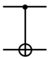
Definition

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

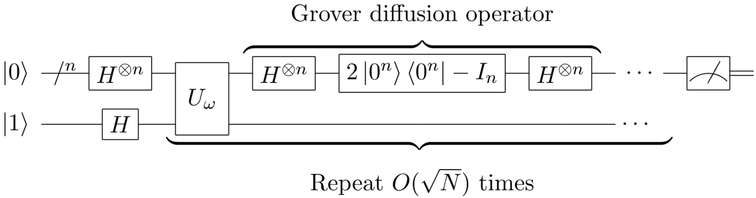
example

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)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Grover's database search

Grover's database search uses possibility to pararell process of qbit. The algorithm allows us to find selected element in unsorted set with complexity $\sqrt{n}$

Grover's database search



Fast exponentiation

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

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

Advanced Encryption Standard

3.MixColumns

Each column is represented as four-bytes vector.

Each column of State is replaced by a new column which is formed by multiplying that column by a certain matrix of elements of the field.

Together with ShiftRows, MixColumns provides *diffusion* in the cipher.

MixColumns step is used in every cycle **except** the last one cycle.

It is also possible to see this operation as polynomial multiplication where each column is represented with polynomial a(x):

$$a(x) = c(x).a(x) mod x^4 + 1 =$$
$$(03x^3 + 01x^2 + 01x + 02).(a_3x^3 + a_2x^2 + a_1x^1 + a_0) mod x^4 + 1$$

$$c(x) = \begin{bmatrix} 02 & 03 \\ 01 & 02 \end{bmatrix}$$

Advanced Encryption Standard

Key Schedule: Rcon Table

Rcon Constants			
Round	Constant(Rcon)	Round	Constant(Rcon)
1	01 00 00 00	6	20 00 00 00
2	02 00 00 00	7	40 00 00 00
3	04 00 00 00	8	80 00 00 00
4	08 00 00 00	9	1B 00 00 00
5	10 00 00 00	10	36 00 00 00

Time for questions

Advanced Encryption Standard

Bibliography

Bibliography:

- Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard", Springer, 2002.

- Joshua Holden, "The Mathematics of Cryptography", Princeton University Press, 2017

- Federal Information Processing Standards Publication 197 : the official AES standard, United States National Institute of Standards and Technology, 2001

- Wikipedia, Advanced Encryption Standard, https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Thank you for attention!