

Quantum Computing and Cryptography

Karol Gołęb
Warsaw University

June 13, 2001

Abstract

What quantum computers mean for
today's cryptography.

Lecture Overview

- Quantum computer
- Quantum cryptography
- Quantum cryptanalysis
- The future

Quantum Computer

Using properties of Quantum Mechanics for computations.

Qubit – Quantum Bit

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$$a, b \in \mathbb{C}$$

$$|a|^2 + |b|^2 = 1$$

May also be written as $\begin{bmatrix} a \\ b \end{bmatrix}$, so:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

For n qubits

$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle$$

Quantum Computer – continued

- Superposition and non-determinism
- Entanglement
- Reversible unitary evolution
- Measurement and its irreversibility
$$|\psi\rangle = a|0\rangle + b|1\rangle$$
$$P[0] = |a|^2$$
$$P[1] = |b|^2$$
- No cloning principle

Quantum Computer - an example

Quantum Cryptography

around 1970 S. J. Wiesner
quantum money

1984 C. H. Bennet, G. Brassard
key distribution scheme

1991 A. K. Ekert
EPR-based key distribution scheme

1992 C. H. Bennet
another key distribution scheme

Quantum Cryptography – BB84

1984 Charles H. Bennet, Gilles Brassard –
quantum key distribution scheme

Properties:

- Secure from any classical attack
- Secure from any quantum attack
- Efficient
- Problem with storing the key

BB84 – continued

Participants:

- Alice – sender
- Bob – receiver
- Eve – eavesdropper

Assumptions:

- quantum channel – insecure, may be modified
- public channel – classical, unjammable

BB84 – continued

The scheme uses four distinct qubit states:

$$|0\rangle, |1\rangle,$$

$$|+\rangle = \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle$$

$$\text{and } |-\rangle = \frac{\sqrt{2}}{2}|0\rangle - \frac{\sqrt{2}}{2}|1\rangle$$

Let U_H denote Hadamard's transform:

$$U_H = \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \end{bmatrix}$$

BB84 – scheme

1. Alice sends Bob a sequence of qubits, each in one of the four states.
2. For each qubit Bob decides whether to use Hadamard's transform.
3. Bob measures each qubit.
4. Bob announces for which qubits he used the transform.
5. Alice announces which choices were correct.
6. Alice and Bob discard all 'faulty' measurements.

7. Alice and Bob test whether Eve tampered the qubits
8. Alice and Bob perform error correction.
9. Alice and Bob perform privacy amplification.

BB84 – an example

BB84 – a proof?

1998 H.-K. Lo, H. F. Chau – rigorous proof

Problems:

- To handle noise in the quantum channel.
- To constrain Eve's information on the final key.
- To protect from joint attacks (Eve entangles transmitted qubits with her probe).
- To securely store the final key.

BB84 – the easy case

Eve measures qubits in transit.

The best strategy is to randomly use Hadamard's transform – then each qubit has 75 % chance of pass as valid.

By exchanging k bits (or performing k parity checks) Alice and Bob protect against such attack.

EPR-based scheme

Alice and Bob share EPR pairs. Those are generated by either of them or by a third party.

Before utilizing the BB84 scheme, Alice and Bob verify whether the pairs were not tampered with.

Alice and Bob run modified BB84 scheme. Step 1 (sending qubits) is replaced Alice performing steps 2 (choosing basis) and 3 (measurement).

The final key is used immediately after creation.

Quantum Cryptanalysis

- Use quantum computers to break classical cryptographic schemes.
- Use quantum computers to break quantum cryptographic schemes.

Breaking RSA

1994 Peter W. Shor – fast algorithms for factoring and discrete logarithms

Best known classical algorithms:

$$\exp(cL^{1/3}(\log L)^{2/3}),$$

where L is the length of the number.

Shor's algorithm:

$O(L^2 \log L \log \log L)$ quantum
and $O(L^3)$ classical.

Factorization – the idea

Let N be the number to be factored.

Let a be any number that $0 \leq a \leq N$ and $(a, N) = 1$.

Consider function $f_{a,N}(x) = a^x \pmod N$.

Let r be the period of $f_{a,N}$.

If r is even and $a^{r/2} \not\equiv -1 \pmod N$ then $(a^{r/2} - 1, N)$ divides N .

Shor's algorithm uses quantum computer to find r for randomly chosen a . Then classic computer is used to verify whether the result found is correct and search for nearby solutions.

Brute-force attacks

1996 Lev K. Grover – fast searching

Searching in any set may be performed in time $O(\sqrt{N})$, where N is the size of the set.

This implicates that the exhaustive key-space search for any classic cryptosystem may be performed in time $O(2^{n/2})$ where n is key length.

Classical brute-force attack takes time $O(2^n)$.

The Future

Quantum cryptography:

- Schemes for multiple users.
- Public key schemes?

Quantum cryptanalysis:

- Specialized algorithms for different cryptosystems.
- Quantum computers.