MAN IN THE MIDDLE AND QUANTUM PROTOCOLS

MIGUEL ÁNGEL LÓPEZ MUÑOZ
FAC C.C. MATEMÁTICAS, UCM

Quantum computation: is the study of the information processing tasks that can be accomplished with quantum mechanical systems.

Different kinds of computing machines and systems:

Abacus $\rightarrow$ System of sticks and beads
Classic computation $\rightarrow$ Electric systems
Quantum computation $\rightarrow$ Quantum mechanical systems

1994, **Shor's Algorithm**: solves in an efficient way (the computation speed increases with a polynomial pattern with respect to the input) in a quantum computer the problem of finding the prime factors of an integer number.

Classic computation $\rightarrow$ bit
Quantum computation $\rightarrow$ qubit

The **qubit** is the quantum analog of the bit. A bit can be either 0 or 1. A qubit can be 0, 1 (which is denoted by $|0\rangle$, $|1\rangle$) but also '0 and 1'.

A qubit can be written in the form

$$\alpha|0\rangle + \beta|1\rangle, \text{ with } \alpha^2 + \beta^2 = 1,$$

where α and β are complex numbers, but most of the times they can be considered real numbers. Each time we measure the qubit we obtain the value $|0\rangle$ with probability α^2 or $|1\rangle$ with probability β^2.

Shor's Algorithm could break RSA cryptosystem, so it's important the study of new cryptographic methods.

Quantum cryptography: the study of processing tasks which security is based upon quantum mechanical laws.

BB84: First quantum cryptography algorithm. It is based in Heisenberg's principle. If Alice sends qubits to Bob and an enemy (called Eve) observes them, then Eve has forced the qubits to appear in a concrete state, a fact that can be used to detect her.

We can use the tensor product to represent pairs of qubits. For example, we have

$$\frac{|01\rangle + |00\rangle}{\sqrt{2}} = |0\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

and as we can see they can be easily decomposed. However, the following pair of qubits cannot be decomposed:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

This is a Bell state of **EPR pair**. It has a useful property: if we measure the first qubit, the second qubit must take the same value.

There are a lot of protocols based in EPR pairs (but we cannot teleport information using EPR pairs, at least without sharing classical communication). These protocols are vulnerable to **Man in the Middle attack**.

The Man in the Middle Eve can do the following:

- Eve can masquerade Alice and Bob.
- Eve can stop communication between Alice and Bob.
- Eve can do nothing and let the information pass.

Algorithm in which we are working: algorithm used to detect Man in the Middle. Basic ideas:

- Alice sends qubits to Bob with two random patterns. First, she sends or not a qubit which is part of an EPR pair with probability $1/2$. Second, this qubit can be one of two non-orthogonal different qubits, also with probability $1/2$.
- If Eve gets the qubit sent and re-sends one of her own, she cannot know if is or not part of an EPR pair, and she also cannot know which qubit is (just because we cannot distinguish non-orthogonal qubits).
- As a result, she could be either automatically detected. In other case, she will change drastically the expected probability of total of measures or she won't interfere at all (which is interpreted as a success for Alice and Bob).
- Eve cannot clone the qubit she gets, because of the no-cloning theorem (we cannot 'clone' a random qubit).

References:

Nielsen and Chuang, *Quantum Information and Quantum Computation*, Cambridge University Press (2000).

D. Richard Kuhn. Vulnerabilities in Quantum Key Distribution Protocols. Preprint, math. AG/0305076.