INSTITUIÇÕES ASSOCIADAS

Quantum Security

Armando Nolasco Pinto

Nuno Silva

Quantum Cryptography

- Define and write an optical superposition state
- Design a circuit using a photon source and optical components (beam splitters, polarization beam splitters) to achieved at the end a superposition state
- What is a qubit, and its relationship with superposition
- Represent the qubit in a column vector and in its computation basis

Quantum Cryptography

- Show that the folllowing state is normalized

$$\left(\frac{1}{2}+\frac{1}{2}i\right)|0\rangle-\frac{1}{\sqrt{2}}|1\rangle$$

- Write the state for two qubits.

- What will be the collumn vector for the two qubit states?

Quantum Cryptography

- What is the quantum state for two qubits?
- Write the four entangled two-qubit states, known as Bell states
- What is the fundamental difference between the quantum state for two qubits and the Bell quantum states?
- How can we access that we have an entangled state?
- Does entanglement violate special relativity

Quantum Cryptography

- Why do we need single photons for QKD to be secure? Why not use “classical light” composed of many photons to represent 0 and 1?

- In the BB84 quantum protocol using single photons polarization, how we can attribute bits to quantum states?

- Starting from Alice bits “0” and “1” draw the decision tree at Bob detection scheme output.

Quantum Cryptography

- How many communication channels do we need to implement a QKD system?
- How the security can be guaranteed and assessed by the users of a QKD system? It is possible to attack those systems?
- Do CV-QKD systems use two single photon detectors in the receiver? Explain.
- Can the quantum key distribution systems replace the public encryption systems?

universidade de aveiro

Thank You!

(nasilva@ua.pt)

(anp@ua.pt)

instituto de telecomunicações

IQC quantum communications