Tecnologias Quânticas
Universidade de Aveiro
2018-2019

Coherent One Way (COW) QKD Protocol

João António[1], **Daniel Pereira**[2,3], **Armando N. Pinto**[2,3]

Physics Department[1],
Department of Electronics, Telecommunications and Informatics[2],
University of Aveiro, Aveiro, Portugal
Instituto de Telecomunicações,[3], Aveiro, Portugal

Quantum Key Distribution

Quantum Key Distribution (QKD) is a secure way of sharing a unique random key (composed of 0 and 1) between two parties spatially distant. They later use this random key to encrypt and decrypt messages between them.

Alice	
Message	42
Message in 8bit Binary	00101010
Key	**10101011**
(Key + 8bit mod 2) Encrypted Message	10000001

Bob	
Encrypted Message	10000001
Key	**10101011**
(Encrypted Message + Key mod 2) Decrypted Message	00101010
Message	42

To share/create the random key, they use two channels, one quantum channel and one Authenticated classic channel (can be eavesdropped but can't be modified).

COW - Protocol

Step 1 Alice produces:

$$|0\rangle = |\alpha\rangle|0\rangle$$
$$|1\rangle = |0\rangle|\alpha\rangle$$
$$|d\rangle = |\alpha\rangle|\alpha\rangle$$

where $|0\rangle$ is the vacuum state and $|\alpha\rangle$ is a coherent state of light with intensity $\mu = |\alpha|^2$.

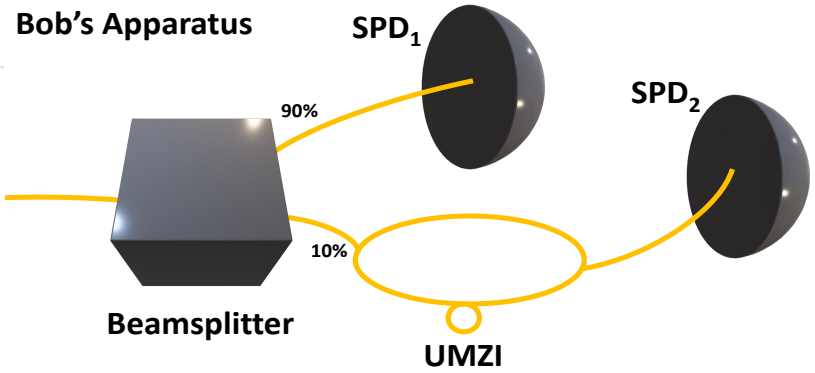
Alice produces $|d\rangle$ with probability f and the quantum signal cannot be divided bitwise (coherence of the laser).

$$|...0d10...\rangle = |... : 0\alpha : \alpha\alpha : \alpha 0 : 0\alpha...\rangle$$

COW - Protocol

Step 3 Bob uses a 90:10 beamsplitter making 90% of the photons into the SPD_1 to arrival time measurements, the remaining 10% are used to measure phase coherence.

In the UMZI (Unbalanced Mach-Zehnder Interferometer) the delayed half of each pulse is recombined in the non-delayed half the next pulse.



COW - Protocol

In the UMZI (Unbalanced Mach-Zehnder Interferometer) the delayed half of each pulse is recombined in the non-delayed half the next pulse.

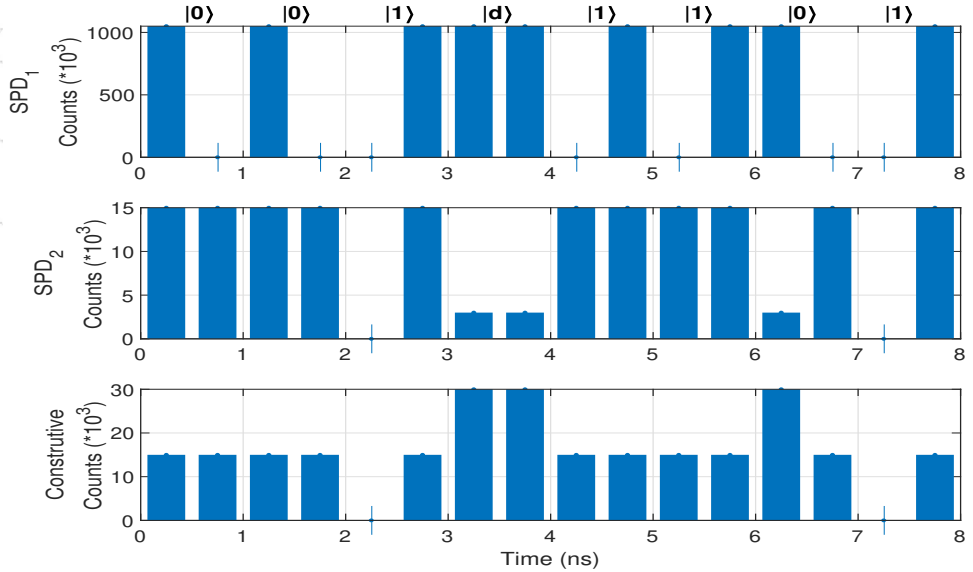


Image based on the article 2017 - Roberts - Modulator-free coherent-one-way quantum key distribution

COW - Protocol

Step 4 Alice informs Bob when she sent a decoy pulse.

Step 5 They calculate the visibility (V) and the QBER (Q) of the key.

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}$$

where the I_{max} and I_{min} are the average pulse intensities for constructive and destructive interference respectively.

They also share a small part of the key in a public channel, to see if there are errors in the message.

A loss of coherence and therefore a reduction of the visibility reveal the presence of an eavesdropper, in which case the key is simply discarded

E-mail: joaoantonio@ua.pt