Universidade de Aveiro
2018-2019

Coherent One Way (COW) QKD Protocol

João Antônio, Daniel Silva, Armando N. Pinto

Department of Electronics, Telecommunications and Informatics,
University of Aveiro, Aveiro, Portugal
Instituto de Telecomunicações, Aveiro, Portugal

INSTITUIÇÕES ASSOCIADAS:

instituto de telecomunicações

creating and sharing knowledge for telecommunications

COW - Protocol

Step 1 Alice produces:

$$|0\rangle = |\alpha\rangle_{2k}|0\rangle_{2k+1},$$
$$|1\rangle = |0\rangle_{2k}|\alpha\rangle_{2k+1}.$$
$$|d\rangle = |\alpha\rangle_{2k}|\alpha\rangle_{2k+1}.$$

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

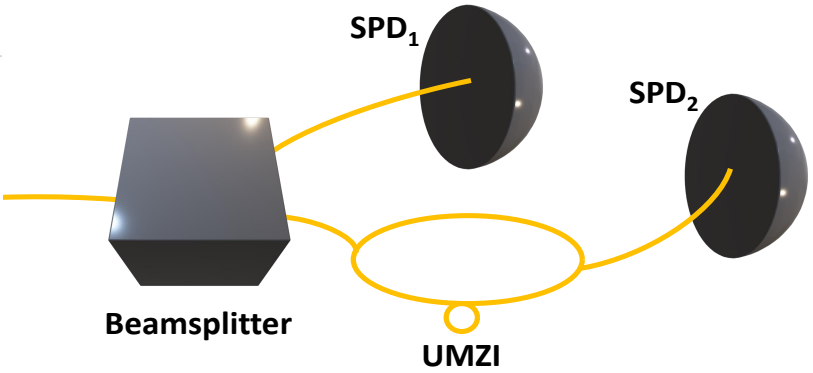
Alice produces $|d\rangle$ with probability f and the quantum signal cannot be be divided bitwise (coherence of the laser).

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

COW - Protocol

Step 2 Alice uses a attenuator to around 0.1 photons per pulse and then transmits through a quantum channel.

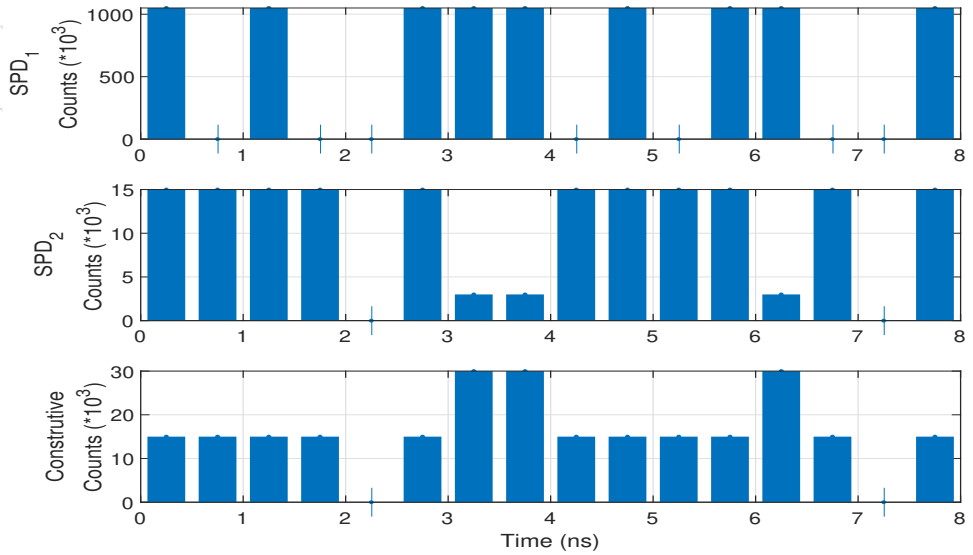
Step 3 Bob uses a 90:10 beamsplitter making 90% of the photons into the SPD_1 to arrival time measurements, the remaining 10% are used to measure phase coherence.



COW - Protocol

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

Example, for a key $|0\rangle|0\rangle|1\rangle|d\rangle|1\rangle|1\rangle|0\rangle|1\rangle$



COW - Protocol - Attacks

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

Step 5 They calculate the visibility 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.

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

COW - Protocol - Attacks

- Beam-splitting attack - Eve removes a small part from the intensity of the original message and send the rest to bob in a no-losses channel. Eve introduces additional errors to in order to make her information equal to the Bob information.
- Active beam-splitting attack - Eve removes smaller intensities of the message and can make individual measurements and block some of it.

COW - Protocol

- Unambiguous state discrimination (USD) - Alice and Bob only check the coherence in two successive pulses. So if Eve can attack while they don't check the coherence, she can do an unnoticed attack, if systematically, Alice and Bob notice that no decoy have been detected.

Name	Discriminating
USD3	$\|0\rangle\|\alpha\rangle\|0\rangle$
USD4a	$\|0\rangle\|\alpha\rangle : \|\alpha\rangle\|0\rangle$
USD4b	$\|0\rangle : \|\alpha\rangle\|\alpha\rangle : \|0\rangle$

E-mail: joaoantonio@ua.pt