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

INSTITUIÇÕES ASSOCIADAS:

INSTITUTO
SUPERIOR
TECNICO

Faculdade de Ciências
e Tecnologia da
Universidade de Coimbra

universidade
de aveiro

P T   Inovação

SIEMENS
Communications

instituto de
telecomunicações

creating and sharing knowledge for telecommunications

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).

Quantum Key Distribution

The two main types of QKD are Polirization protocols and Time Bin protocols.

The Coherent One Way (COW) protocol, uses the Time Bin properties.
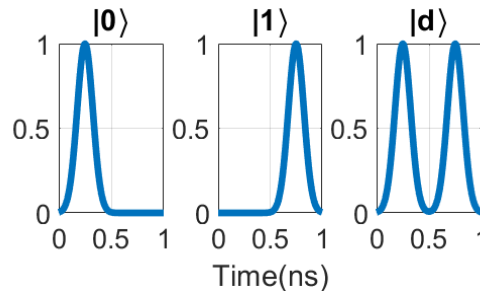
COW - Protocol

Step 1 Alice creates a random key using:

$$|0\rangle = |\alpha\rangle|0\rangle$$

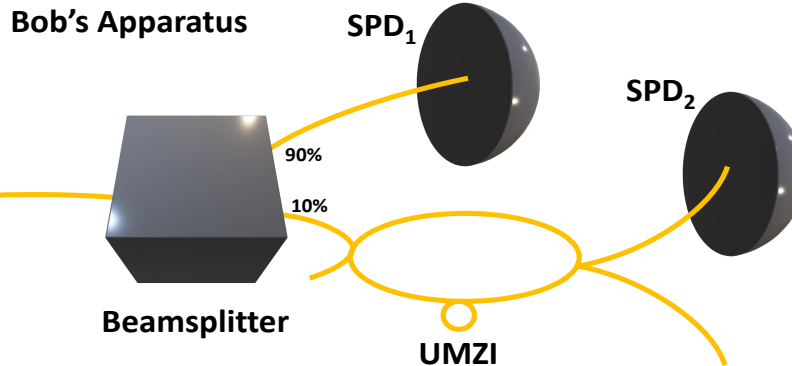$$|1\rangle = |0\rangle|\alpha\rangle$$

$$|d\rangle = |\alpha\rangle|\alpha\rangle$$

where $|0\rangle$ is the vacuum state and $|\alpha\rangle$ is a coherent state of light with intensity $\mu = |\alpha|^2$ and spreads a few random decoy states ($|d\rangle$) in random locations during the creation of the key.

COW - Protocol

Step 2 Bob uses a 90:10 beamsplitter making 90% of the photons into the SPD_1 to create the key by measuring time-bins, the remaining 10% are used to measure phase coherence.


The UMZI (Unbalanced Mach-Zehnder Interferometer) delays by 0.5 ns the photon, measuring in the SPD_2 the destructive interference.

COW - Protocol

To better study what happens in the 10% branch of the Bob Apparatus. The the top graph of the Figure is the single photons that arrive before the UZMI. The bottom one is the measures in the SPD_2, where a photon in time t can interact with a photon in time t-0.5 ns.

Time T	Time T - 0.5	SPD2
1	0	1
0	1	1
1	1	0
0	0	0
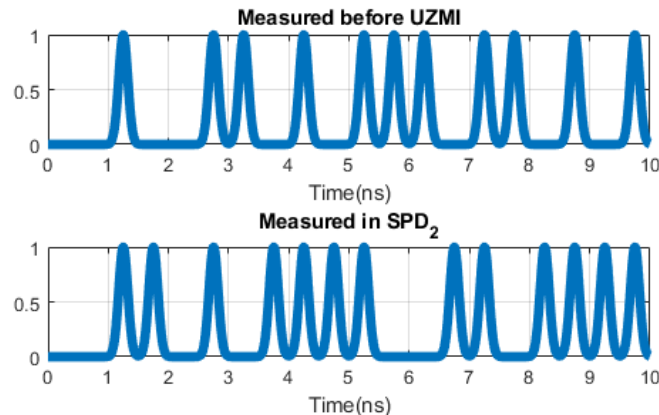
COW - Protocol

Step 3 Alice informs Bob when she sent a decoy pulse.

Step 4 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

- 2017 - Roberts - Modulator-free coherent-one-way quantum key distribution
- 2006 - Branciard - Zero-Error Attacks and Detection Statistics in the Coherent One-Way Protocol for Quantum Cryptography