Coherent One Way (COW) QKD Protocol

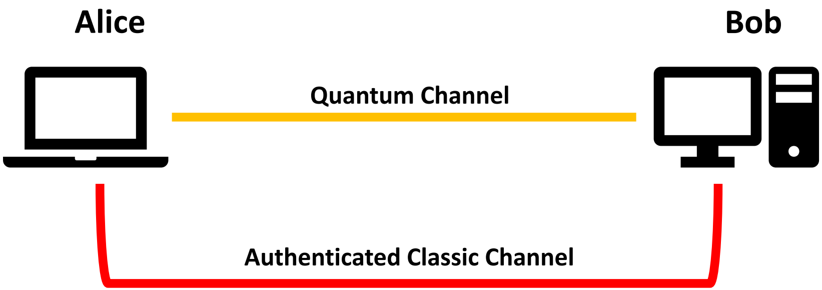
João António[1], Daniel Pereira[2,3], Armando N. Pinto[2,3]

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.

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 was elaborated by Nicolas Gisin et al in 2004. Uses time bin properties and the main principle is the **Quantum Entanglement**.

The advantage of this system are that :

- the setup is experimentally simple
- tolerant to photon numbers splitting attacks

COW - Protocol

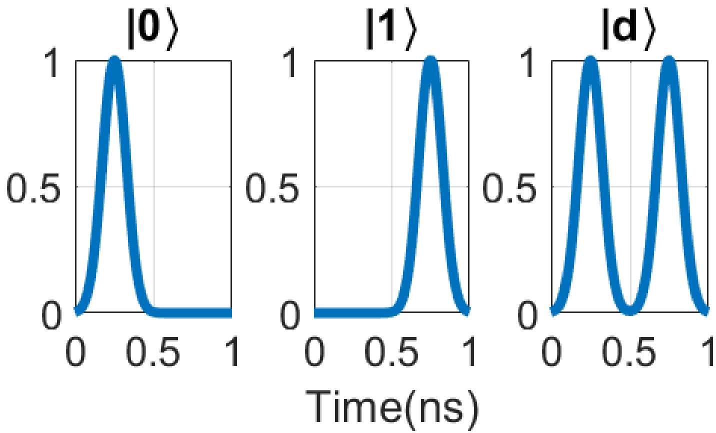
Step 1 Alice creates a random key using:

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

$$|1\rangle = |\emptyset\rangle|\alpha\rangle$$

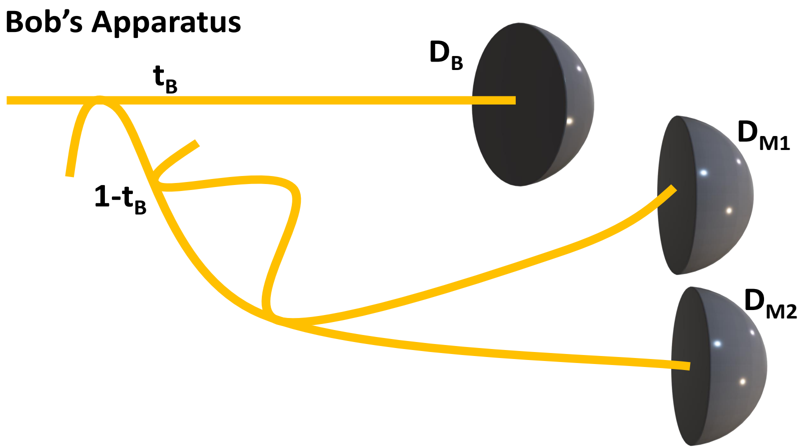
$$|d\rangle = |\alpha\rangle|\alpha\rangle$$

Where $|\emptyset\rangle$ 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. The two photons are Quantum Entanglement.



COW - Protocol

Step 2 Bob's detection is completely passive. An asymmetric coupler sends a fraction t_B of the photons into the data line. That consist of a single photon counter D_B, where the bits are discriminated by the time of arrival.



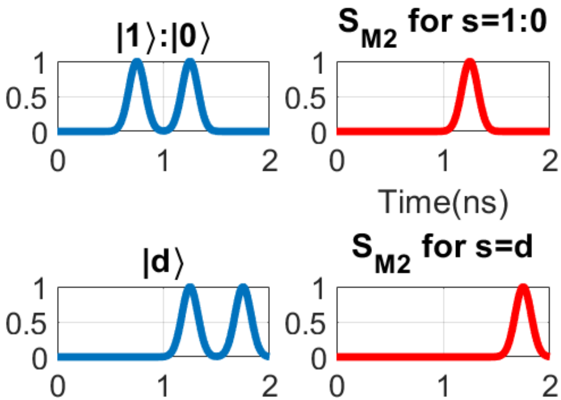
In the other line half of each pulse interacts with the half of the previous pulse (delayed by 0.5 ns).

COW - Protocol

The D_{M2} (constructive photon counter) should only click when:

- Decoy state where the coherence is within the bit sequence (s=d);
- A logical bit 1 followed by a logical bit 0 where the coherence is across the bit separation (s=1:0);

All the other photons should click the D_{M1}.



COW - Protocol

Step 3 Bob informs Alice when D_{M1} and D_{M2} clicked. Alice tell Bob which items of the data line must be discarded because they correspond to decoy sequences.

Step 4 They calculate the visibility (V) and the QBER (Q) of the key.

$$V_s = \frac{P(D_{M1}|s) - P(D_{M2}|s)}{P(D_{M1}|s) + P(D_{M2}|s)}$$

where $P(D_M|s)$ is the probability that detector D_M has clicked at a time corresponding to a s sequence. After that Bob reveals some bits of the data line to calculate the Q.

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

- 2014 - Singh - Quantum Key Distribuition Protocols A review
- 2006 - Branciard - Zero-Error Attacks and Detection Statistics in the Coherent One-Way Protocol for Quantum Cryptography
- 2017 - Kronberg - Analysis of coherent quantum cryptography protocol
- 2017 - Roberts - Modulator-free coherent-one-way quantum key distribution