UA

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

TÉCNICO LISBOA

universidade de aveiro

UNIVERSIDADE BEIRA INTERIOR

U.PORTO

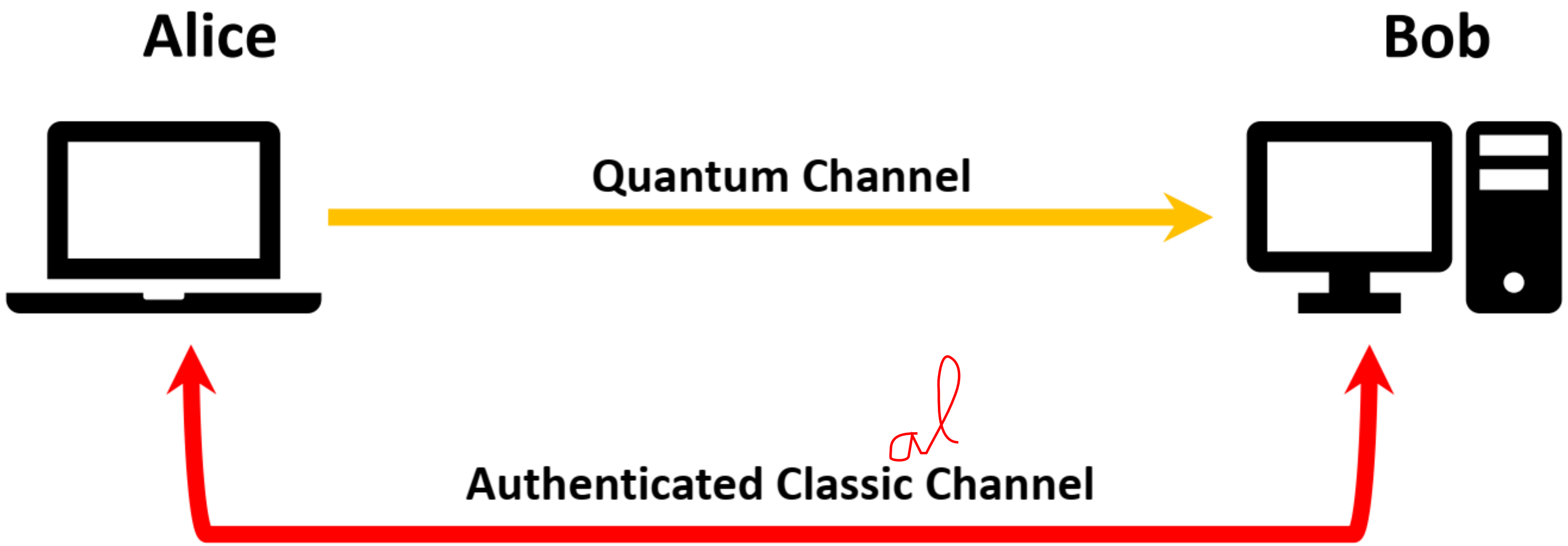
ISCTE IUL

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 symmetric key to encrypt and decrypt messages between them.

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

a



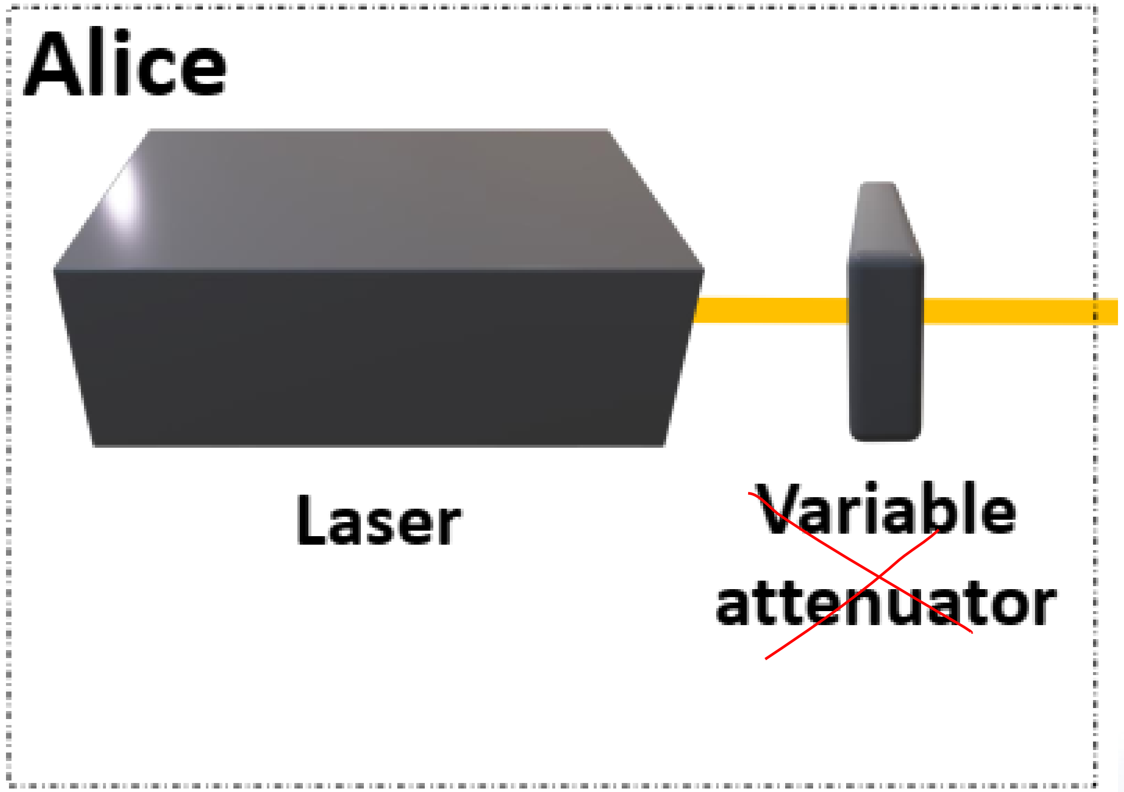
~~Quantum Key Distribution~~ Time Bin – QKD

Polarization QKD and Ti–

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

The Coherent One Way (COW) protocol was elaborated by Nicolas Gisin et al in 2004 [1]. Uses time bin properties.

It is also characterized by having a very simple experimental setup since Bob's apparatus is passive.



→ Intensity Modulator

Optical Atten

[1] Gisin, Nicolas, et al. "Towards practical and fast quantum cryptography." arXiv preprint quant-ph/0411022 (2004).

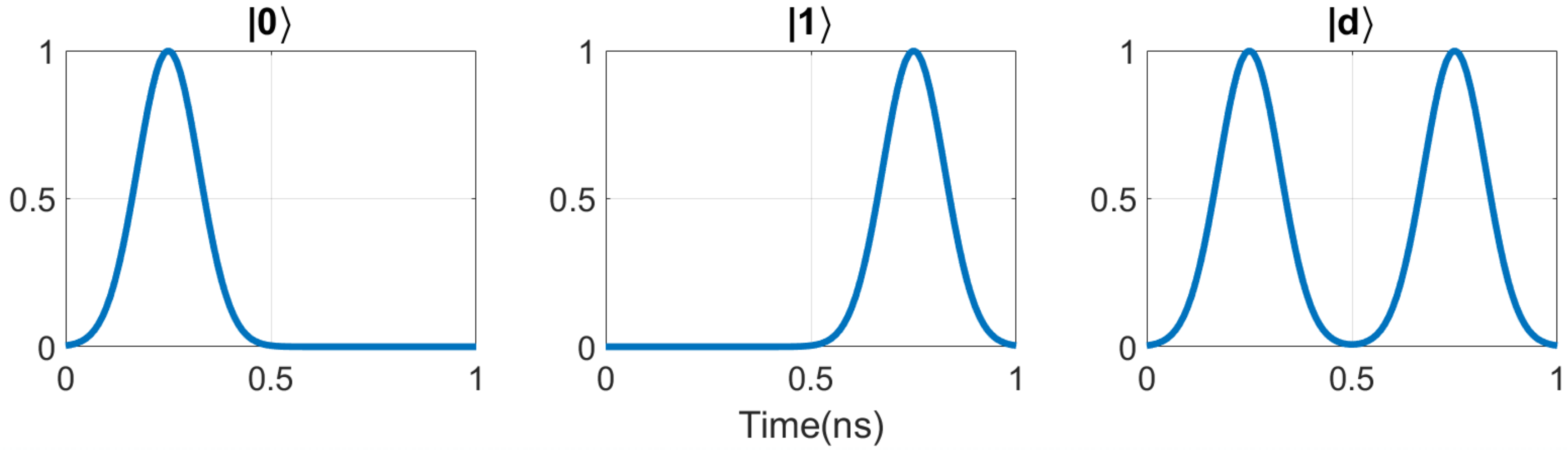
COW - Protocol

0 1 0 d 0 1 0 d d 0 1 0

Step 1 Alice creates a random key using:

$$|0\rangle = |\alpha\rangle|\emptyset\rangle$$
$$|1\rangle = |\emptyset\rangle|\alpha\rangle$$
$$|d\rangle = |\alpha\rangle|\alpha\rangle \longrightarrow \text{decoy}$$

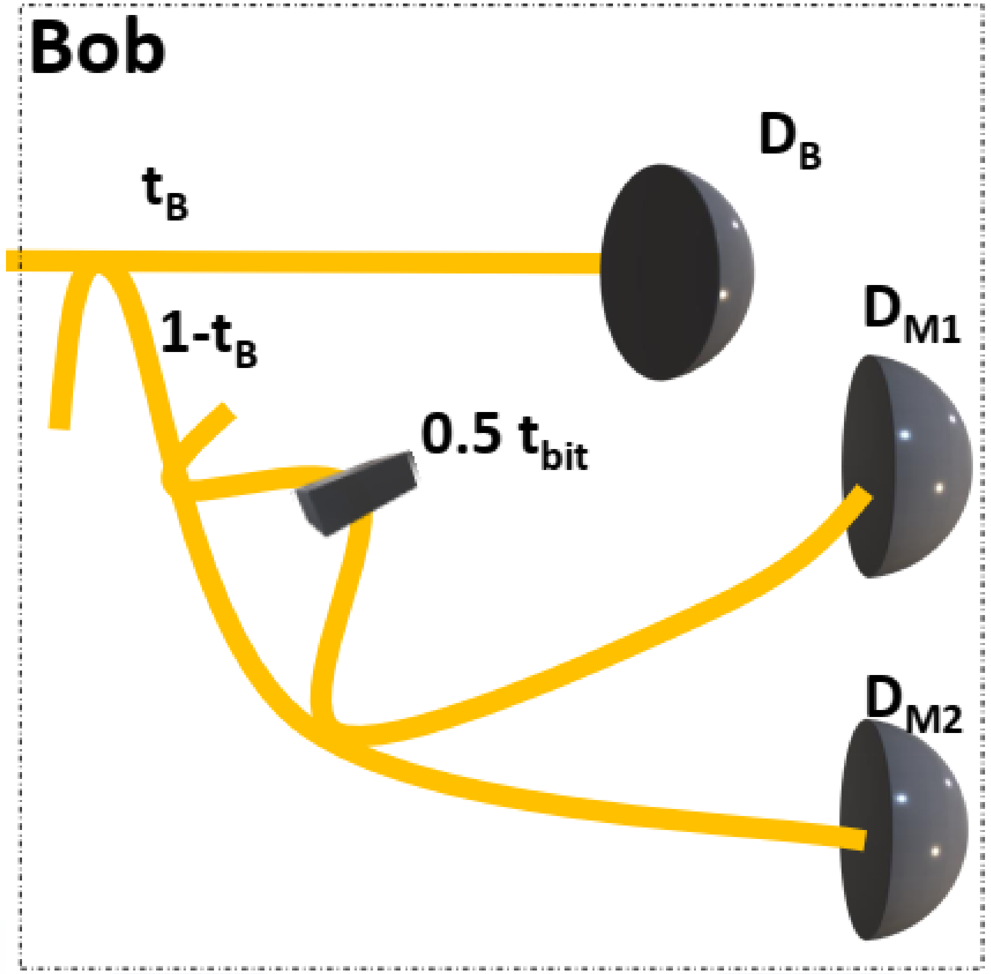
Where $|\emptyset\rangle$ is the vacuum state and $|\alpha\rangle$ is a coherent state of light with intensity $\mu = |\alpha|^2$ and spreads a few random decoy states ($|d\rangle$) in random locations during the creation of the key.

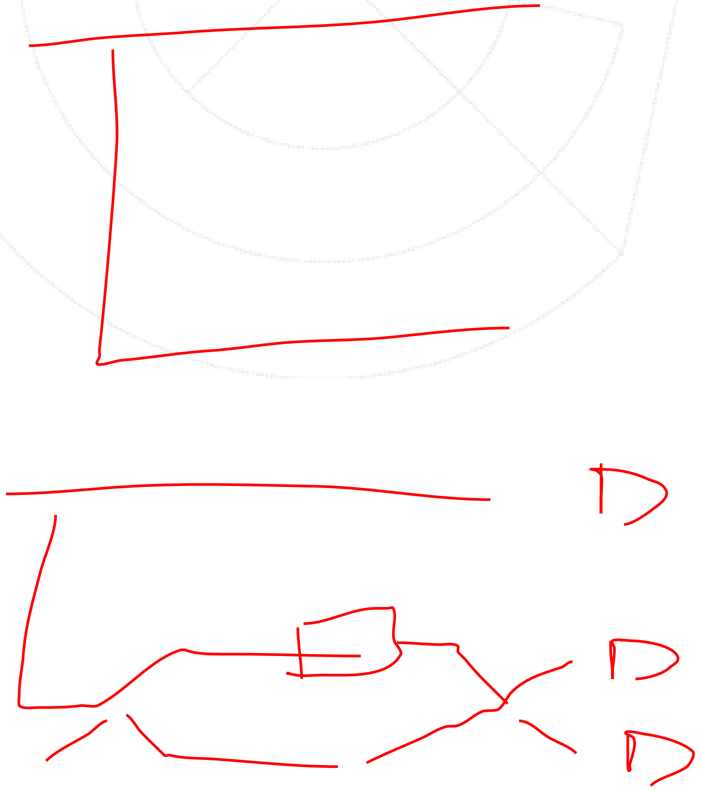


$\mu << 1$

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.





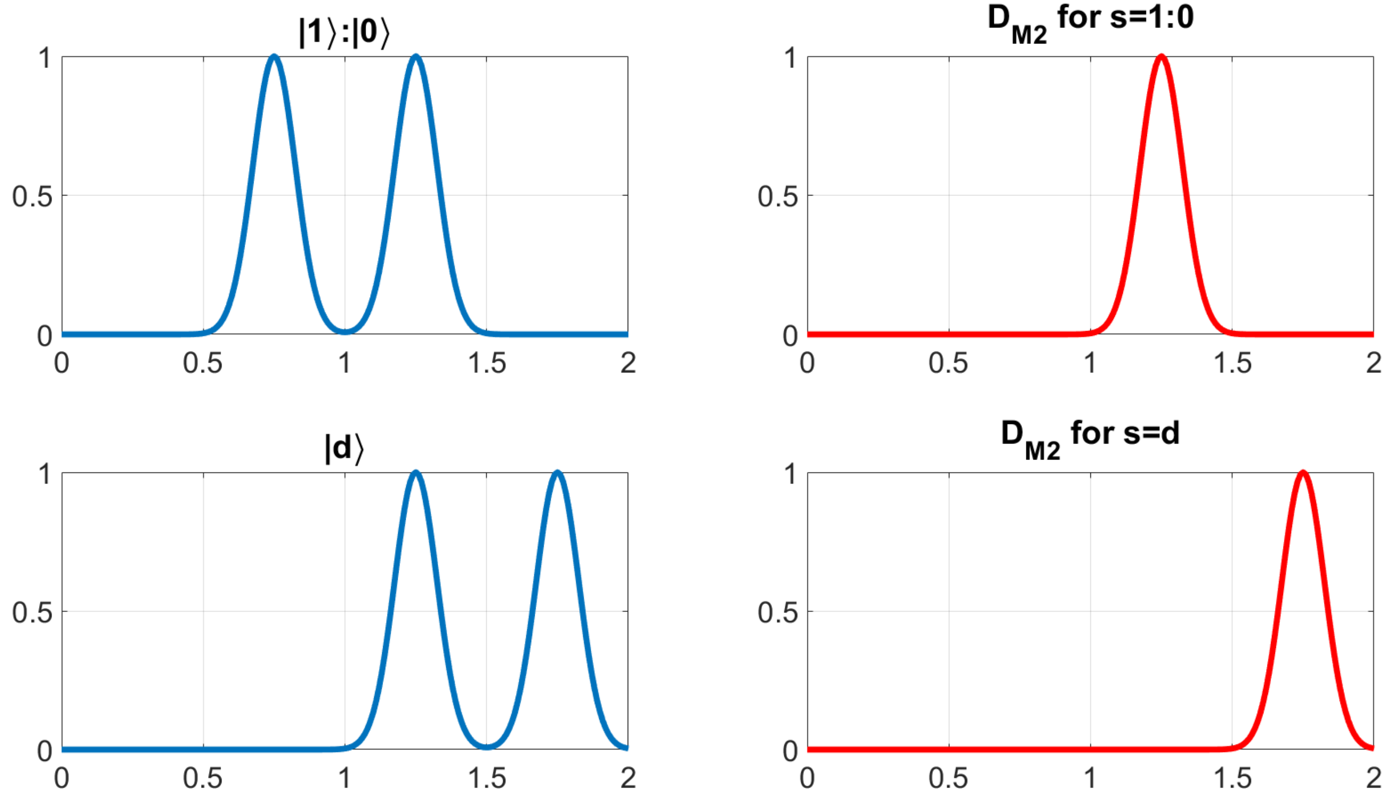
In the other line half of each pulse interacts with the half of the previous pulse (delayed by 0.5 t_{bit}).

COW - Protocol

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

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

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

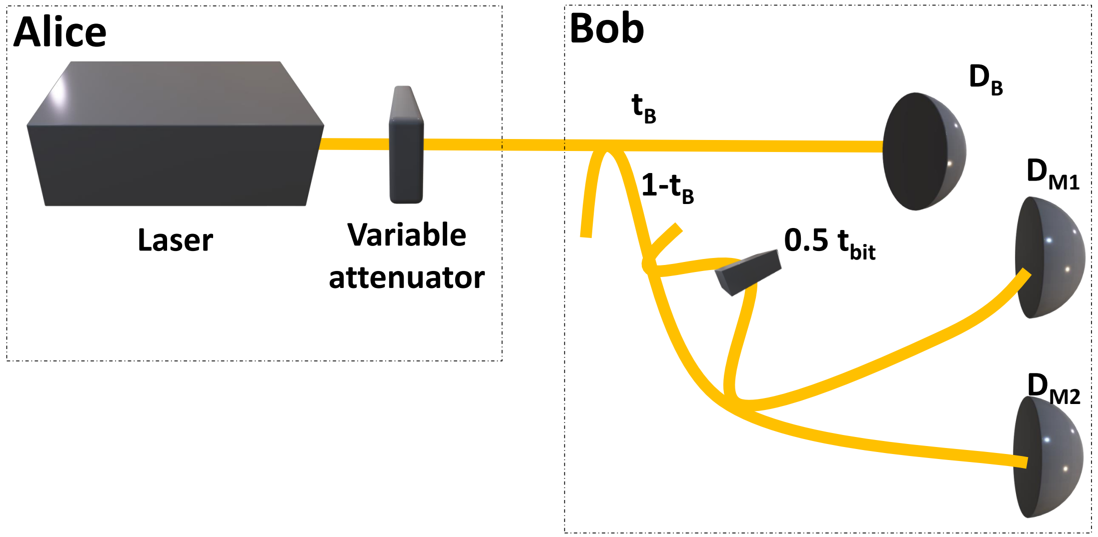


COW - Protocol

Step 3 Alice tell Bob the times of the decoy sequences ($2k_d$ & $2k_d - 1$). Bob also checks if the D_{M2} has ever fired during a $2k_d$ time. Thus they estimate the break of coherence of decoy pulses.

Step 4 Bob reveals the times that he had a detection in D_{M2}, Alice verifies if they belong to a $|1\rangle : |0\rangle$, thus, Alice and Bob estimate the break of coherence across the bit separation.

Step 5 Finally, Bob reveals the items that he has detected in the data line. Alice and Bob run error correction and privacy amplification on these bits and end up with a secret key.



E-mail: joaoantonio@ua.pt

- Gisin, Nicolas, et al. "Towards practical and fast quantum cryptography." arXiv preprint quant-ph/0411022 (2004).
- Branciard, Cyril, et al. "Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography." arXiv preprint quant-ph/0609090 (2006).
- Kronberg, Dmitry Anatol'evich, et al. "Analysis of coherent quantum cryptography protocol vulnerability to an active beam-splitting attack." Quantum Electronics 47.2 (2017): 163.
- Roberts, George L., et al. "Modulator-Free Coherent-One-Way Quantum Key Distribution." Laser & Photonics Reviews 11.4 (2017): 1700067.