

# Coherent One Way (COW) QKD Protocol

INSTITUIÇÕES ASSOCIADAS



João António<sup>1</sup>, Daniel Pereira<sup>2,3</sup>, Armando N. Pinto<sup>2,3</sup>

Physics Department<sup>1</sup>,  
Department of Electronics, Telecommunications  
and Informatics<sup>2</sup>,  
University of Aveiro, Aveiro, Portugal  
Instituto de Telecomunicações,<sup>3</sup> Aveiro, Portugal



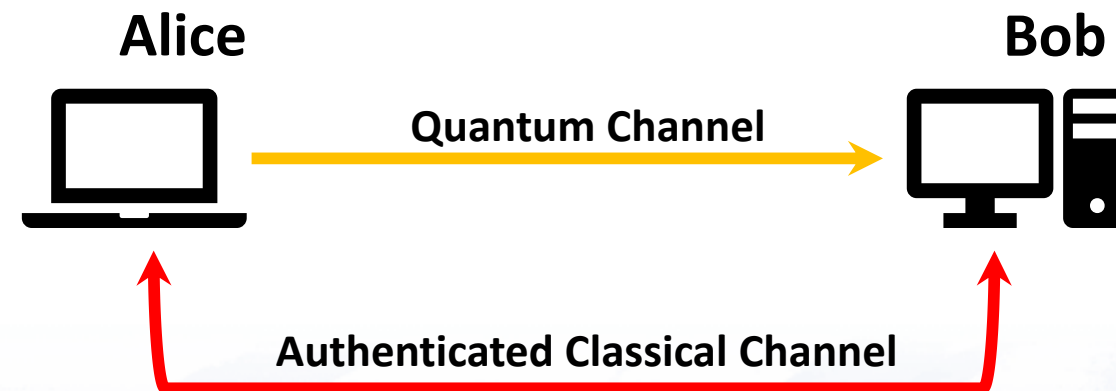
©2018, it - instituto de telecomunicações.

# Quantum Key Distribution

- Quantum Key Distribution (QKD)<sup>1</sup> is a secure way of sharing a unique random key between two parties spatially distant.
- Polarization QKD vs Time Bin QKD.

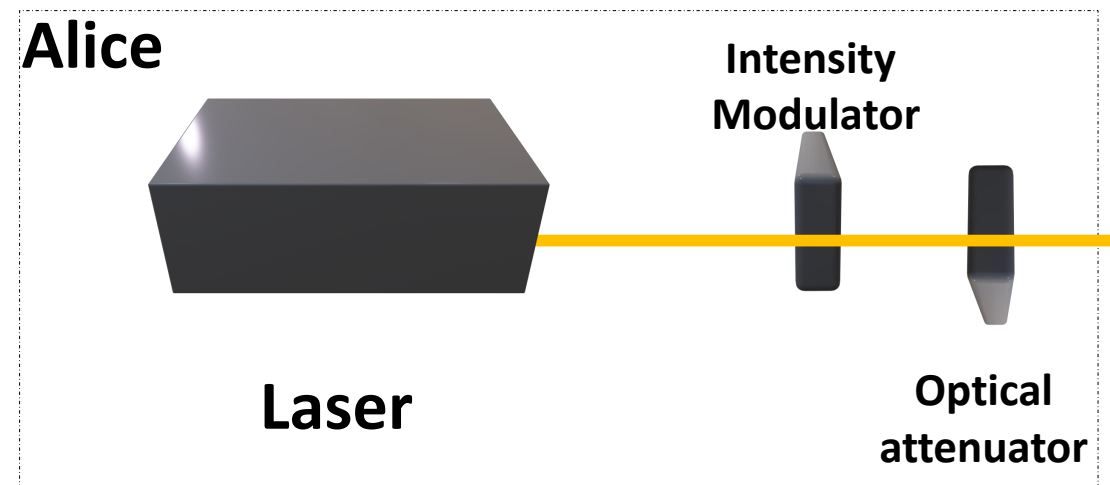
They use:

- One quantum channel (One way is this QKD)
- And one authenticated classic channel (can be eavesdropped but can't be modified).



# Time Bin QKD

- The Coherent One Way (COW) protocol was elaborated by Nicolas Gisin et al in 2004<sup>2</sup>.
- Uses time bin properties.
- It has a very simple setup (Bob's apparatus is passive).



# Alice - COW protocol

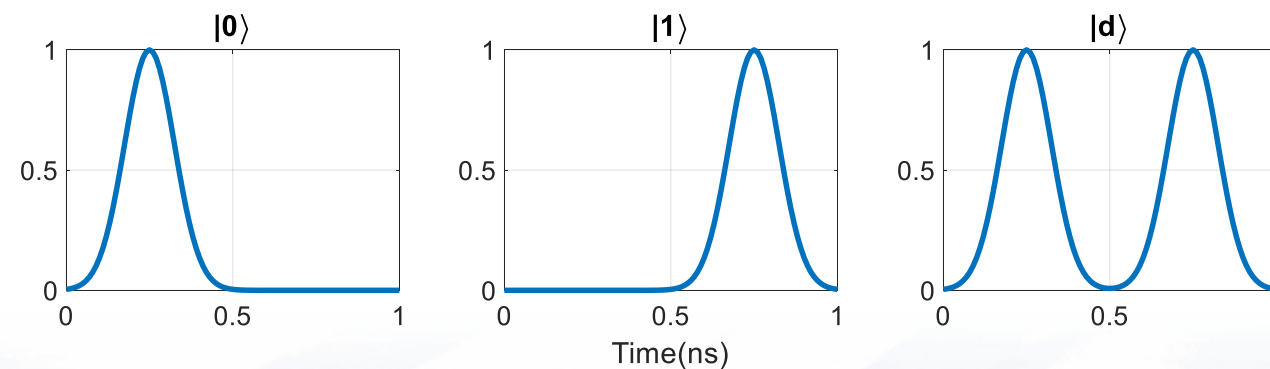
**Step 1** Alice creates a random key using:

$$|0\rangle = |\alpha\rangle|\emptyset\rangle = \textit{Logical 0}$$

$$|1\rangle = |\emptyset\rangle|\alpha\rangle = \textit{Logical 1}$$

$$|d\rangle = |\alpha\rangle|\alpha\rangle = \textit{DecoyState}$$

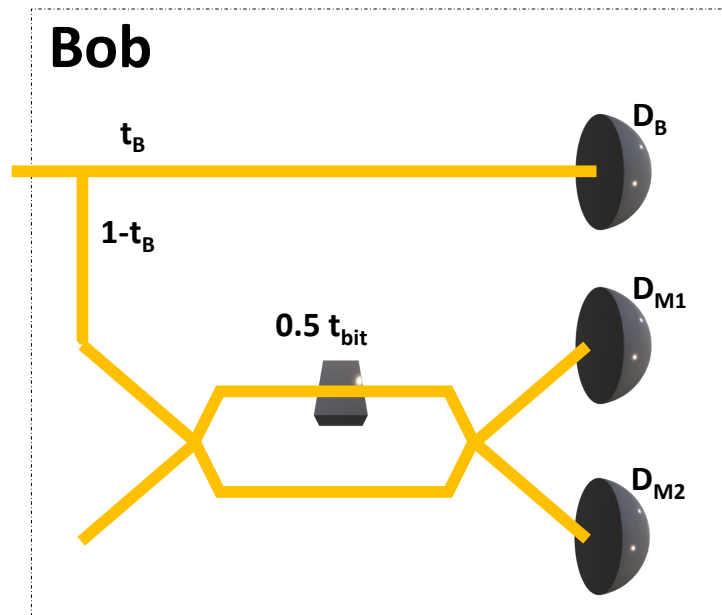
Where  $|\emptyset\rangle$  is the vacuum state and  $|\alpha\rangle$  is a coherent state of light with intensity  $\mu = |\alpha|^2 \ll 1$ .



# Bob - COW protocol

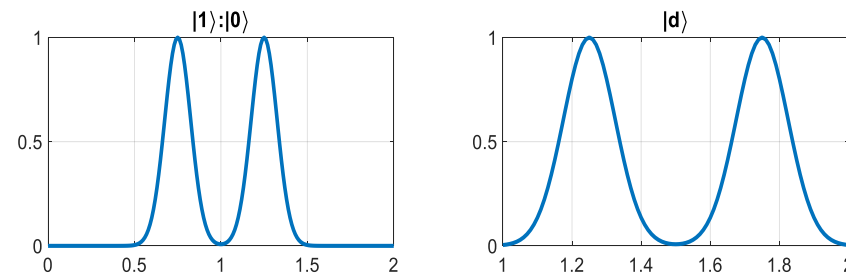
**Step 2** A fraction  $t_B$  of the photons go into the photon counter  $D_B$ , where the bits are discriminated by the time of arrival.

Half of the other photons are delayed by  $0.5 t_{bit}$  interacting with the half of non-delayed bits.

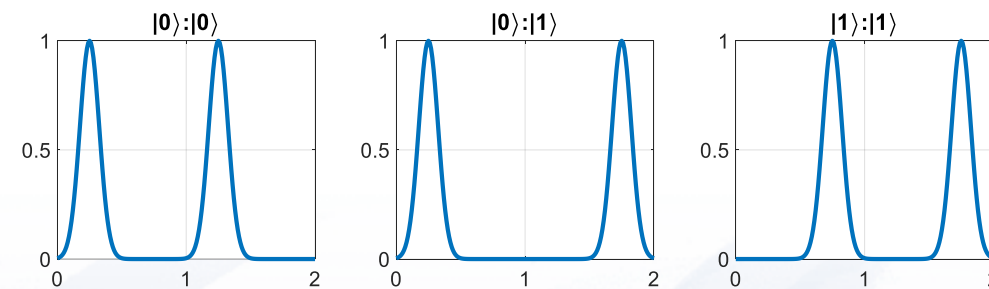


# Monitoring line - COW protocol

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



All the other combinations of photons should click the  $D_{M1}$ :



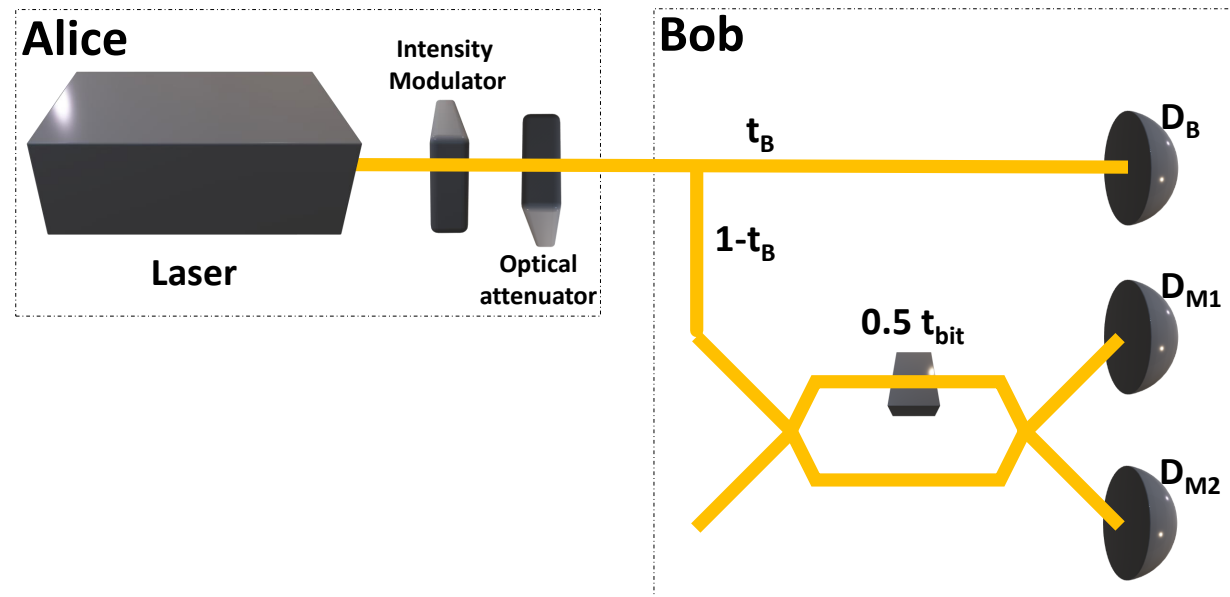


# Testing Visibility and Errors - COW protocol

**Step 3** Alice tell the times of the decoy. Bob checks if the  $D_{M2}$  has fired during a decoy time.

**Step 4** Bob reveals the other times that he had a detection in  $D_{M2}$ , Alice verifies if they belong to a  $|1\rangle : |0\rangle$ .

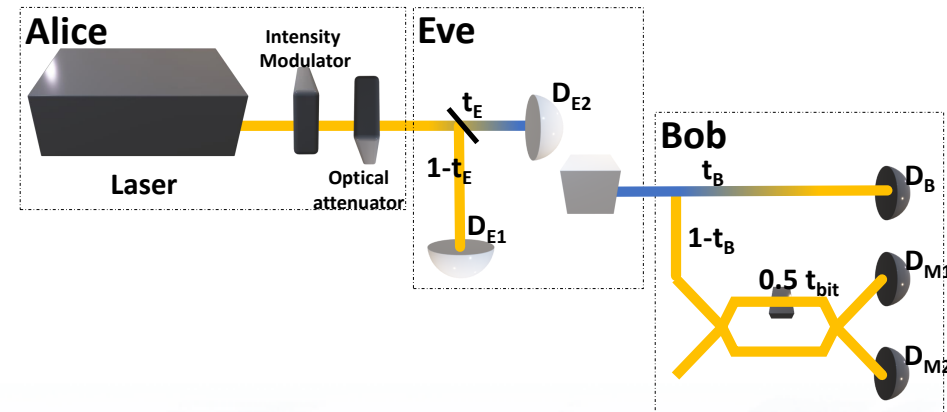
**Step 5** Bob reveals some part of the key. Alice and Bob run error correction and privacy amplification on these bits and end up with a secret key.



# Intercept-Resend Attack - COW protocol

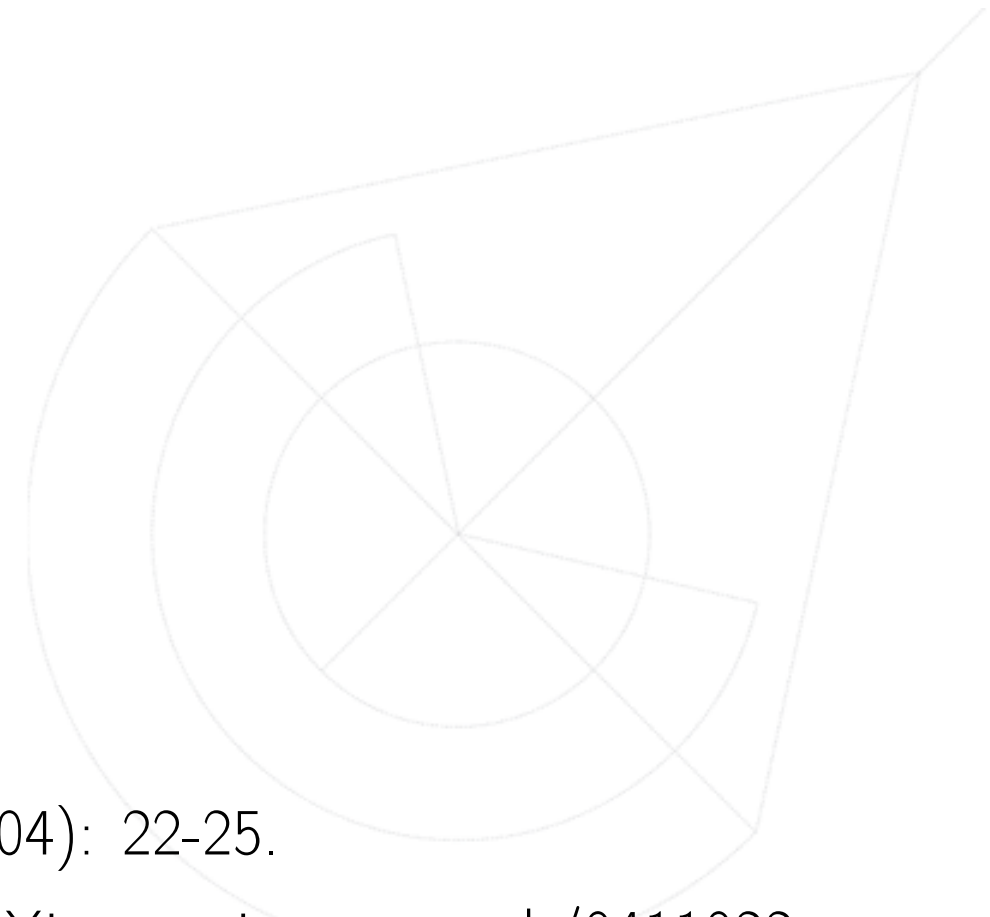
- Eve removes  $1 - t_E$ .
- The rest  $t_E$  are in a lossless channel.
- If  $D_{M2}$  fires (probability  $\mu \times t_E$ ), she prepares a single-photon in the good time-bin and forwards it.
- Eve breaks coherence everywhere with this attack. ( $V_{d|IR} = V_{10|IR} = 0$ )<sup>3</sup>

Eve	Bob
Detected	Detected
Detected	Dark Count
Not Detected	Dark Count





E-mail: joaoantonio@ua.pt



- Ouellette, Jennifer. "Quantum key distribution." Industrial Physicist 10.6 (2004): 22-25.
- 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.