universidade de aveiro
theoria poiesis praxis

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

instituto de telecomunicações

INSTITUIÇÕES ASSOCIADAS

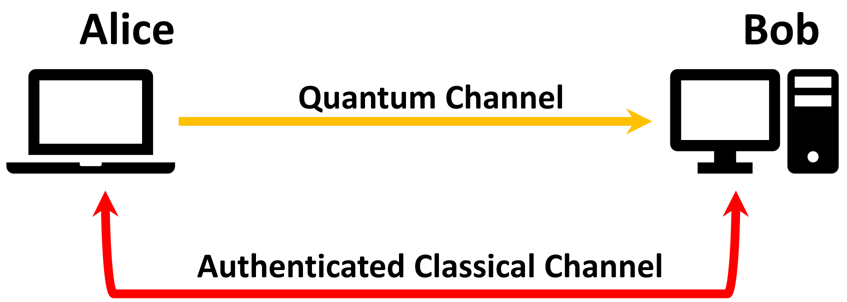
© 2018, Instituto de Telecomunicações

Quantum Key Distribution

- Quantum Key Distribution (QKD) is a secure way of create and share a unique random key between two spatially distant parties.
- Polarization QKD vs Time Bin QKD.

They use:

- One quantum channel (with one way transmission)
- And one authenticated classic channel (can be eavesdropped but can't be modified).

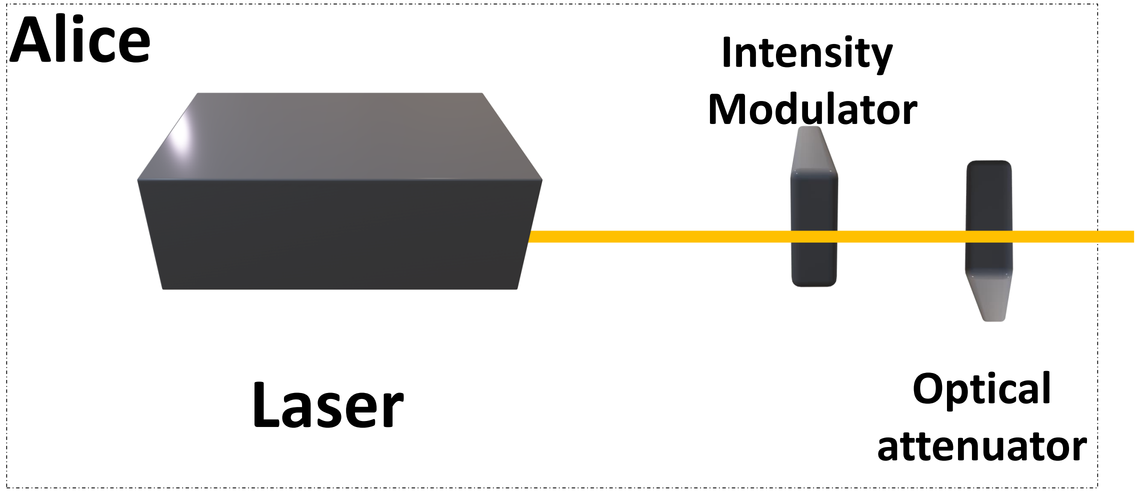


Ouellette, Jennifer. "Quantum key distribution." Industrial Physicist 10.6 (2004): 22-25.

© 2018, Instituto de Telecomunicações

Time Bin QKD

- The Coherent One Way (COW) protocol was elaborated by Nicolas Gisin et al in 2004.
- Uses time bin encoding.
- It is has a very simple setup.



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

instituto de telecomunicações
© 2018, Instituto de Telecomunicações

Alice - COW protocol

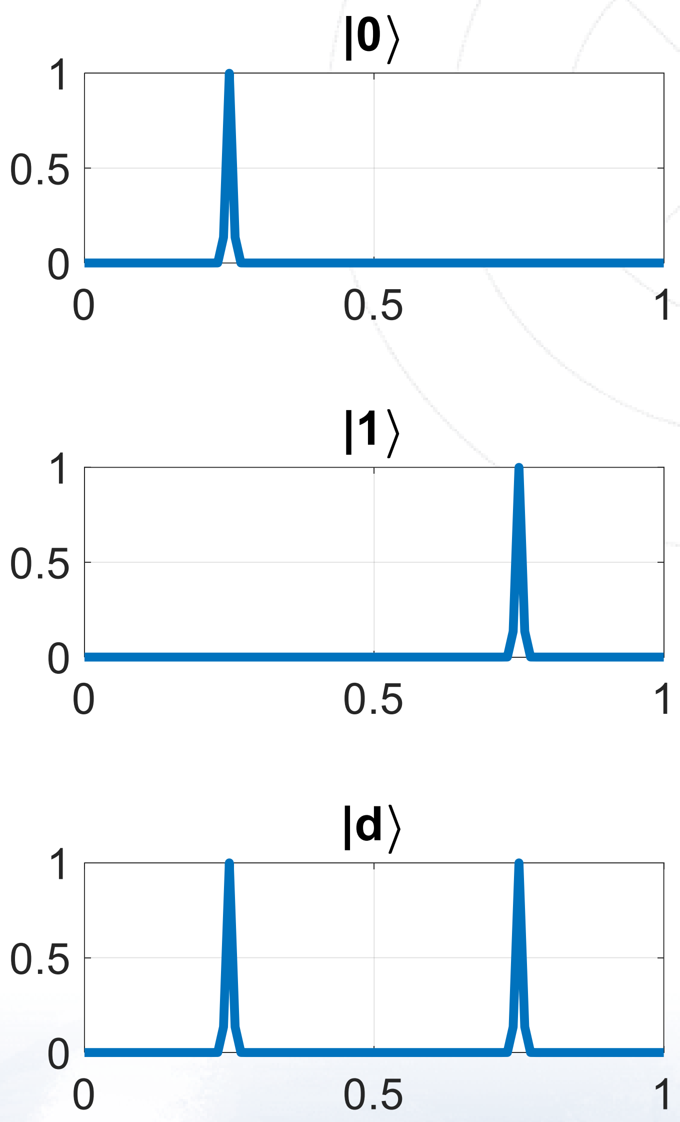
Step 1 Alice creates a random key using:

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

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

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

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

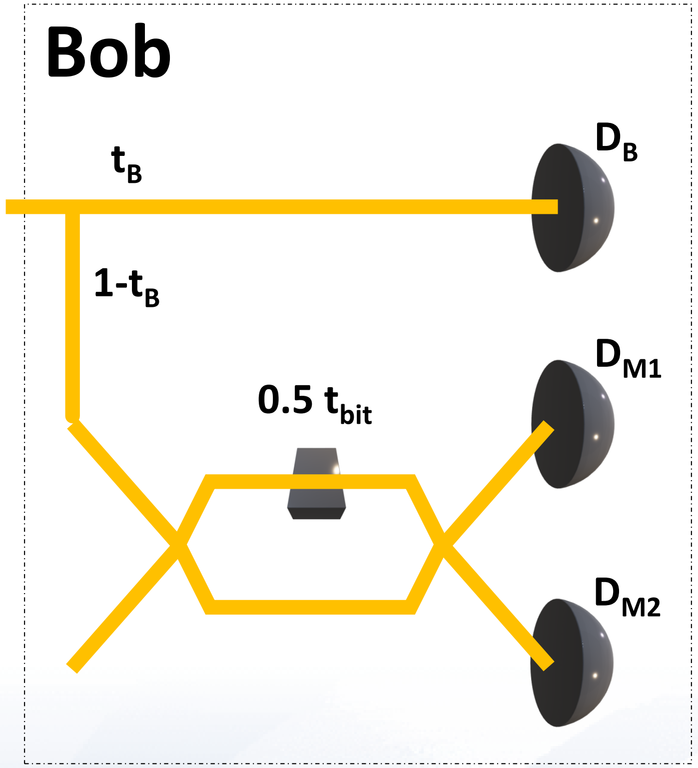


© 2018, Instituto de Telecomunicações

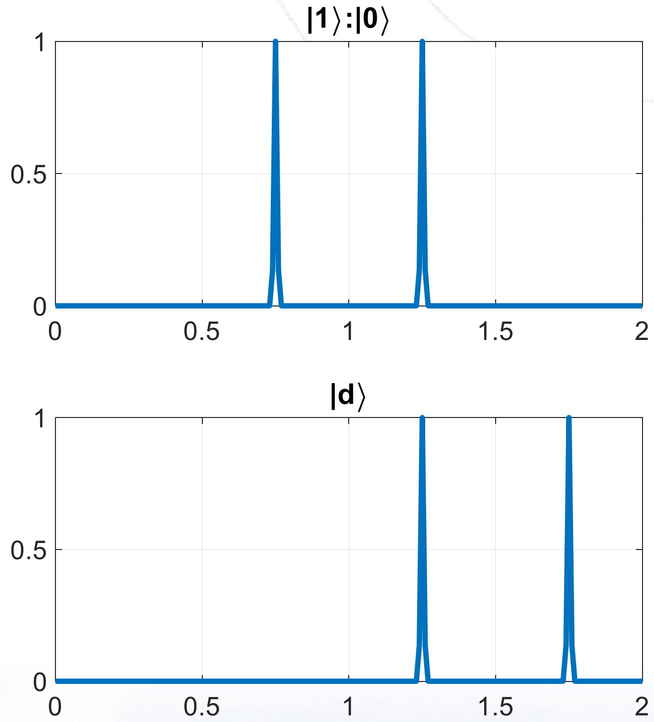
Bob - COW protocol

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.

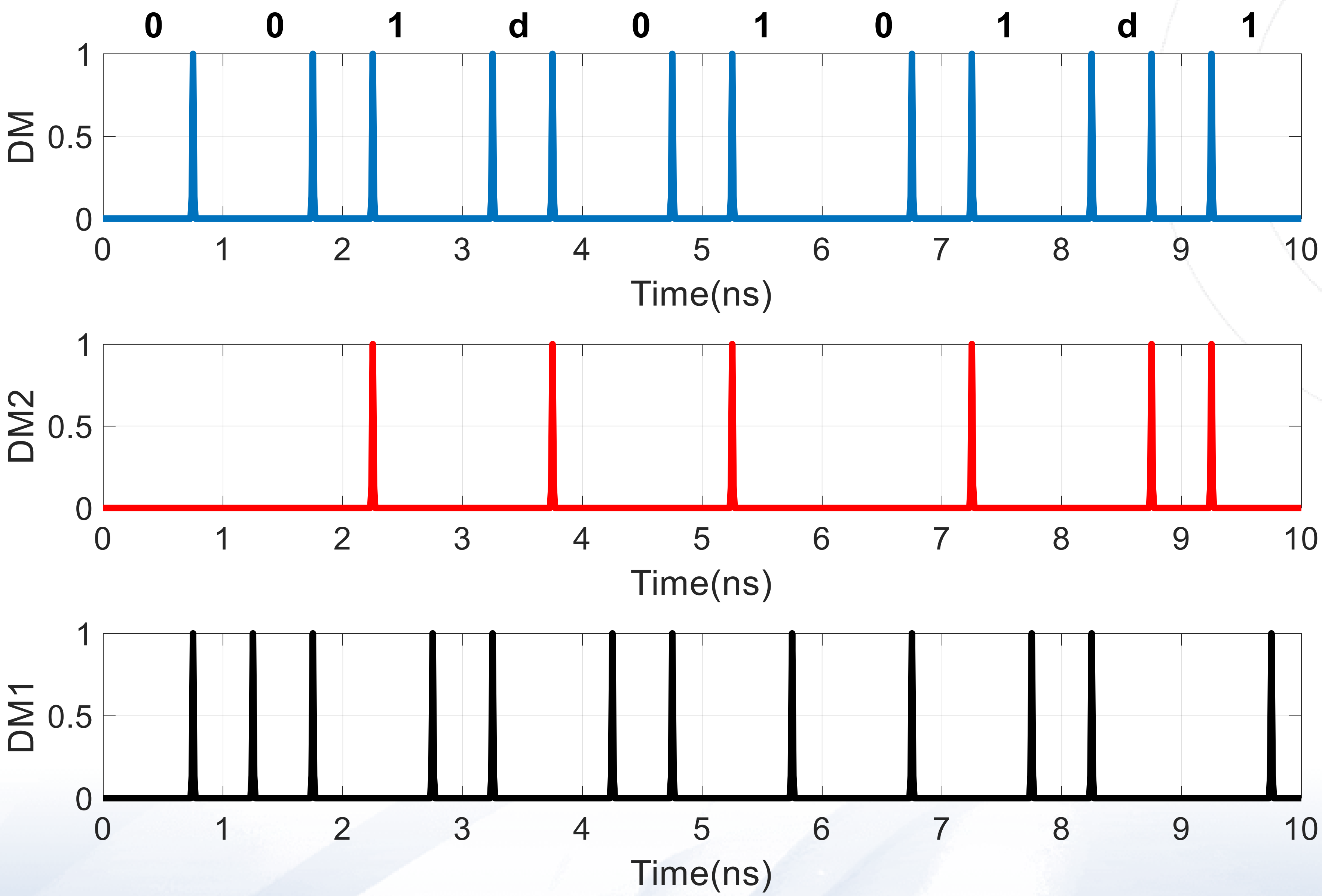


Therefore D_{M2} (constructive photon counter) should only click when:



© 2018, Instituto de Telecomunicações

Monitoring line - COW protocol



© 2018, Instituto de Telecomunicações

Testing Visibility and Errors - COW protocol

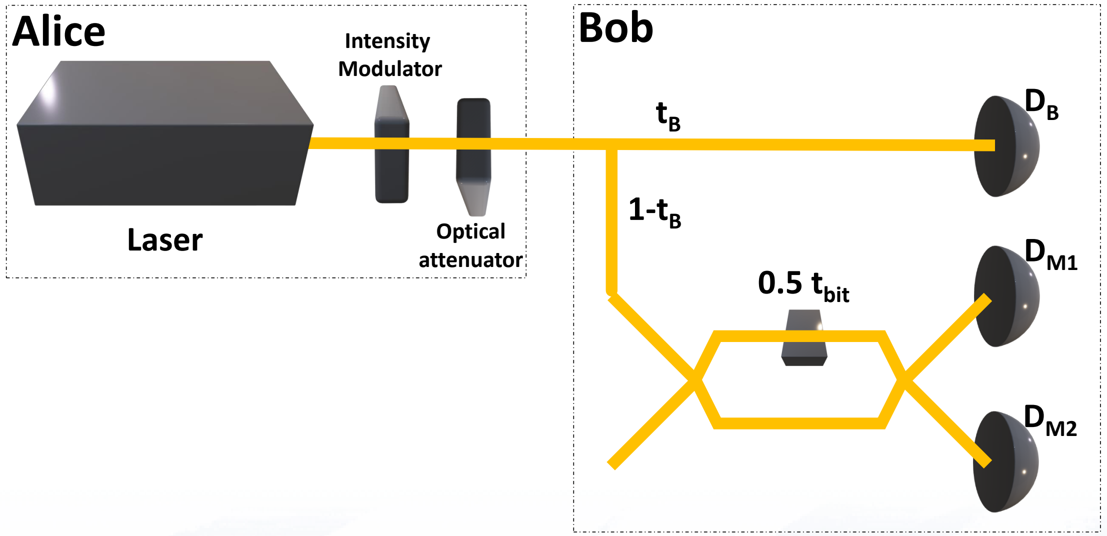
Step 3 Alice tell the decoy times. Bob checks if the D_{M2} has fired during those times.

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 the times that D_B fired, and they use those as key.

Step 6 QBER, check the number of the detections for every detector.

Step 7 run error correction and privacy amplification.



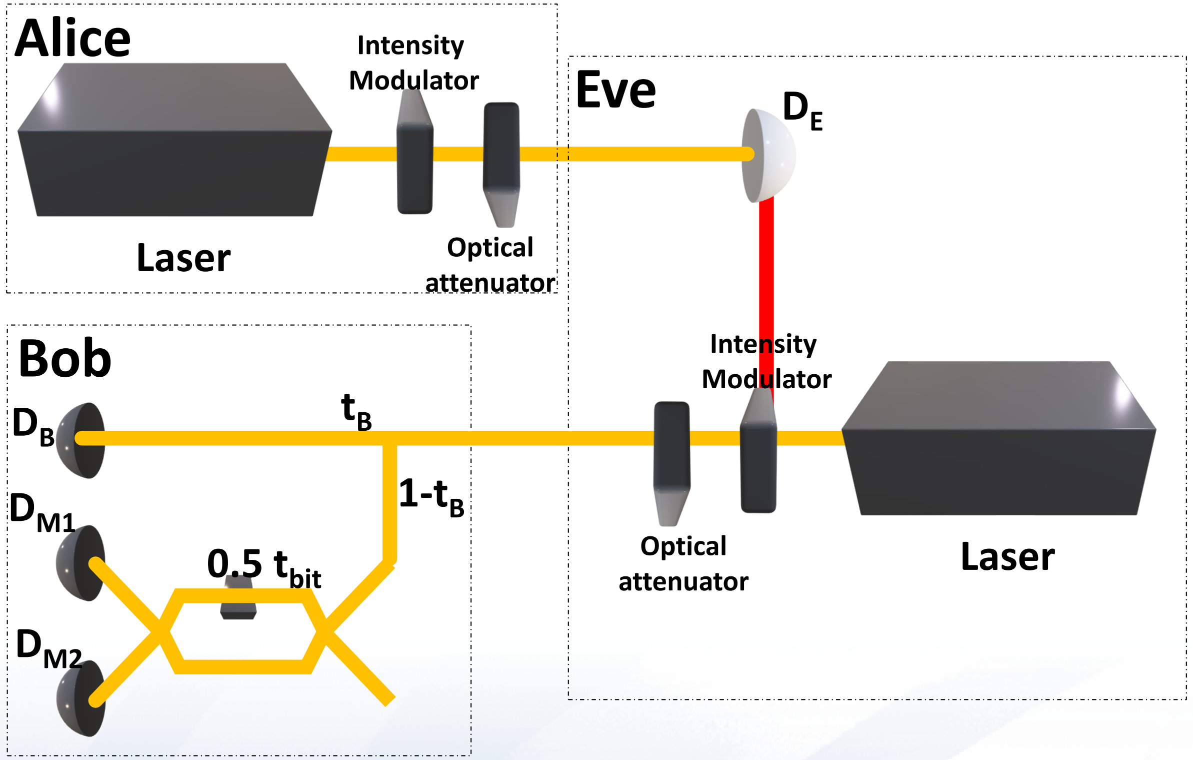
© 2018, Instituto de Telecomunicações

Security

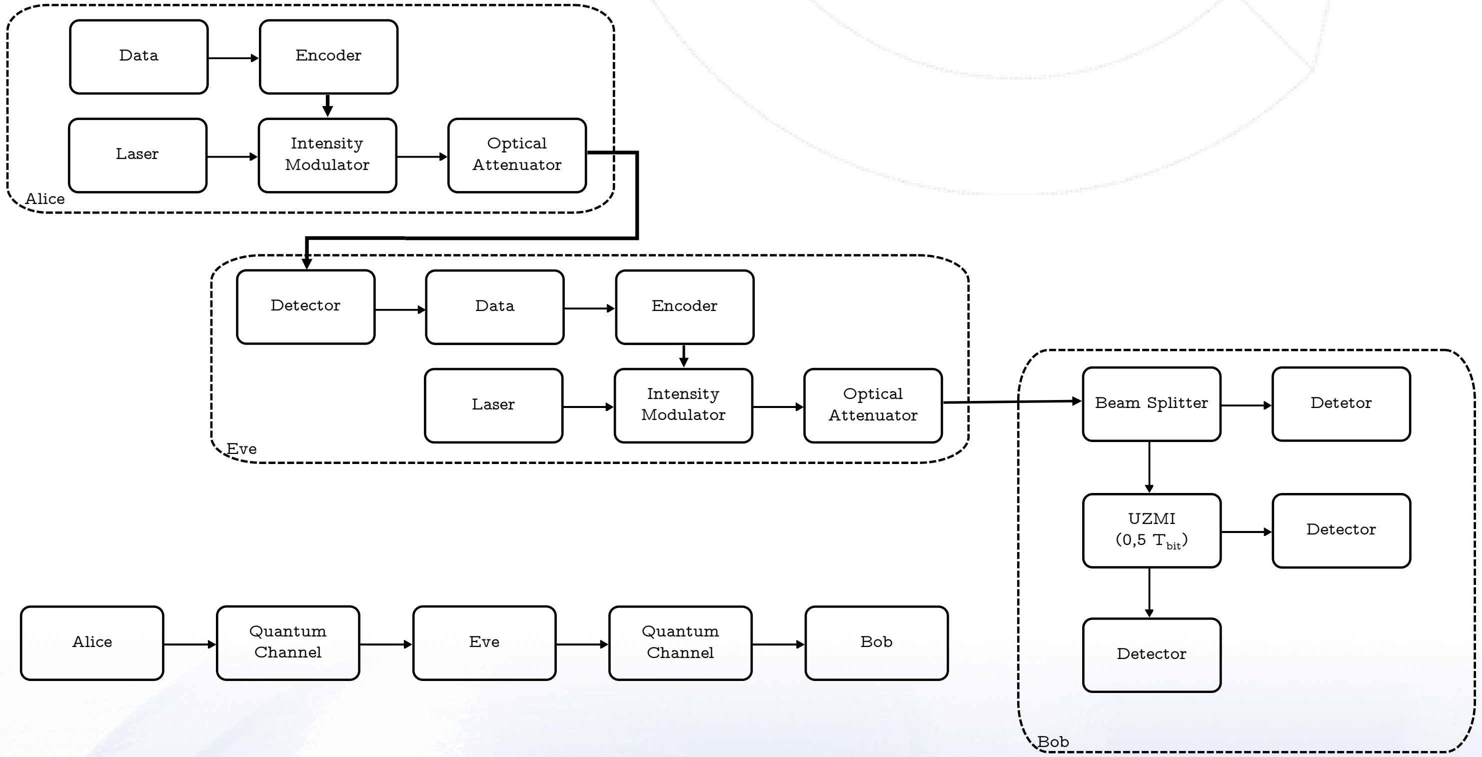
The two main security features of the model is the test of **coherence** and the **Length of the Key**.

We want to see how robust is the protocol to a **Intercept-Resend Attack**. On this attack Eve captures all the information, measures and then resend it to Bob.

Using the same representation as previously:



Using a block Diagram:



© 2018, Instituto de Telecomunicações

Simulation

For the Simulation, using a fiber without looses:

Logical Bits from Alice	10^7
Probability of Decoy	10 %
Alice Attenuation	0.1
Bob Detectors Efficiency	10 %
Bob DarkCount Probability	10^{-5}
Average Over	200 times
Percentage of the Key for QBER	50 %

Note that 10^7 logical bits in a fiber with 90% looses and with a attenuation from Alice equal to 0.1 is 1 second with the system working.

In a simulation without attack, and with this variables, the final information that Bob and Alice have is:

	Min	Averag.	Max
QBER	9.9×10^{-5}	0.0001366	0.00018906
$B_{M1} + B_{M2}$	95294	96288	97069
Key Length	422730	423898	425281

© 2018, Instituto de Telecomunicações

IR - Eve Efficiency

Using the Attenuation of Eve equal to 0.1, by changing the efficiency we get:

	Eve Efficiency = 0.1			Eve Efficiency = 0.5			Eve Efficiency = 1		
	Min	Averag.	Max	Min	Averag.	Max	Min	Averag.	Max
QBER	0.0020583	0.73014	1	0.0016881	0.22776	1	0.001729	0.0023946	0.00032631
$B_{M1}+B_{M2}$	0	1106	9261	0	4602	9383	8889	9173	9404
Key Length	85	4968	40642	91	20361	40883	40034	40438	40748

Simulation without attack again for comparison:

	Min	Averag.	Max
QBER	9.9×10^{-5}	0.0001366	0.00018906
$B_{M1}+B_{M2}$	95294	96288	97069
Key Length	422730	423898	425281

Eve presence lowers the Key length.

© 2018, Instituto de Telecomunicações

IR - Eve Attenuation

Assuming that Eve has 100 % efficiency. By altering the value of her attenuation we get:

	Eve Attenuation = 1.101			Eve Attenuation = 2		
	Min	Averag.	Max	Min	Averag.	Max
QBER	0.00011775	0.00017323	0.00022875	6.21×10^{-5}	8.93×10^{-5}	0.00011472
$B_{M1} + B_{M2}$	99146	100632	101557	181047	182217	183986
Key Length	423756	424850	426440	739744	741841	743701

Simulation without attack again for comparison:

	Min	Averag.	Max
QBER	9.9×10^{-5}	0.0001366	0.00018906
$B_{M1} + B_{M2}$	95294	96288	97069
Key Length	422730	423898	425281

Eve presence increases the sum ($B_{M1} + B_{M2}$) when the Key Length is the correct, and lowers the Key Length when the Sum ($B_{M1} + B_{M2}$) is correct.

instituto de telecomunicações © 2018, Instituto de Telecomunicações

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.

 © 2018, Instituto de Telecomunicações