

Coherent One Way (COW) QKD Protocol

INSTITUIÇÕES ASSOCIADAS



João António¹, Daniel Pereira^{2,3}, Armando N. Pinto^{2,3}

Physics Department¹,
Department of Electronics, Telecommunications
and Informatics²,
University of Aveiro, Aveiro, Portugal
Instituto de Telecomunicações,³ Aveiro, Portugal

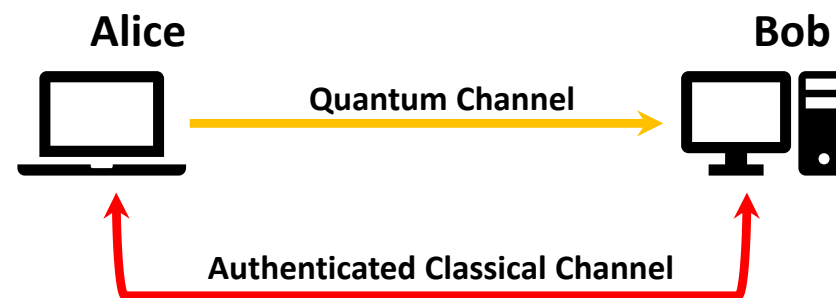


Quantum Key Distribution

- 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.

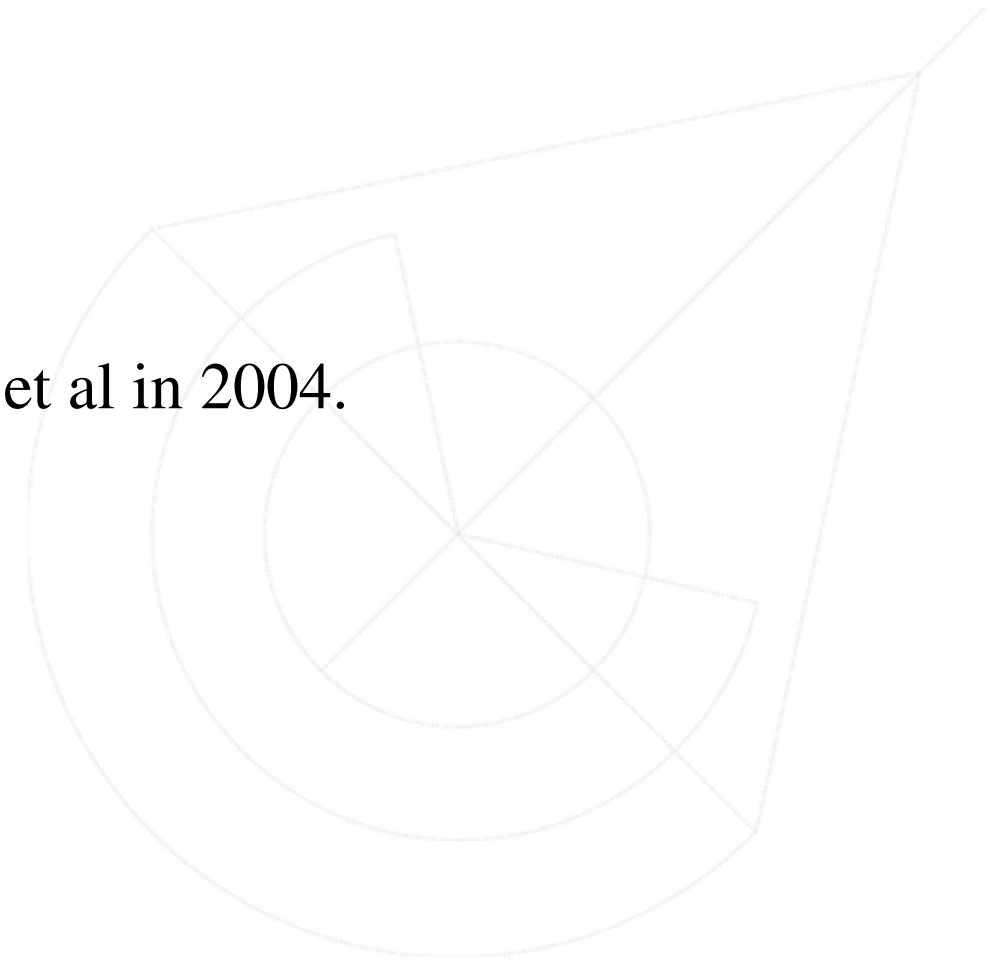
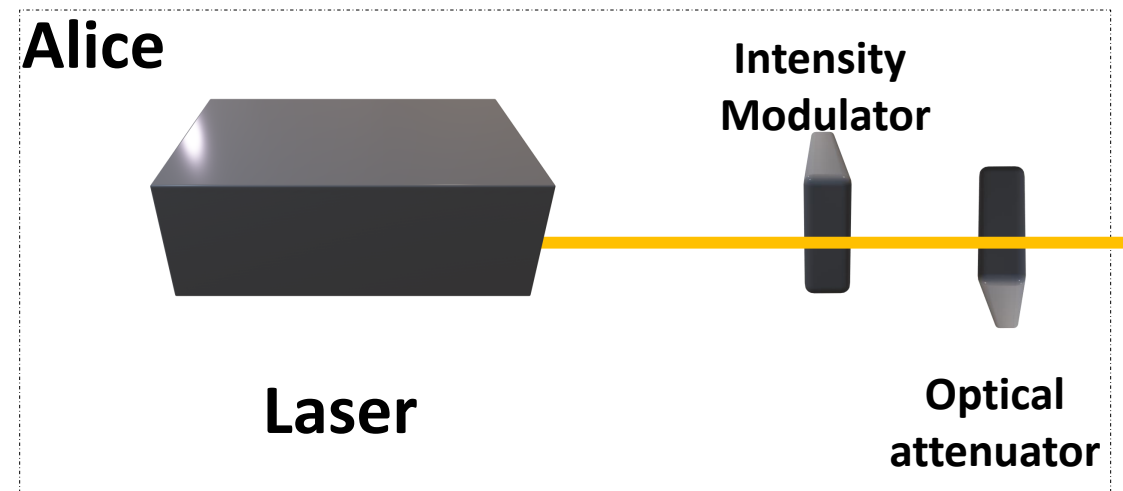
They use:

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



Time Bin QKD

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



Alice - COW protocol

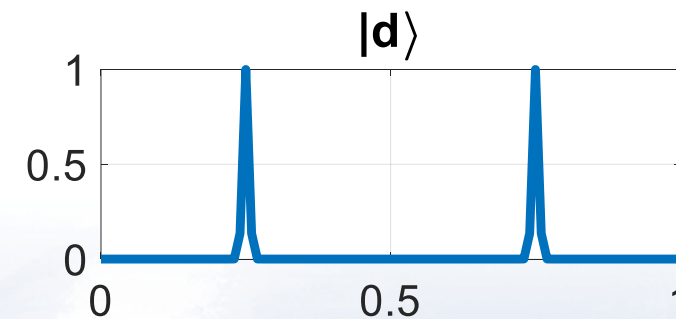
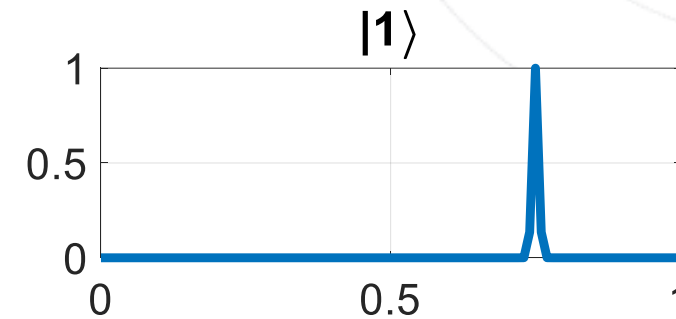
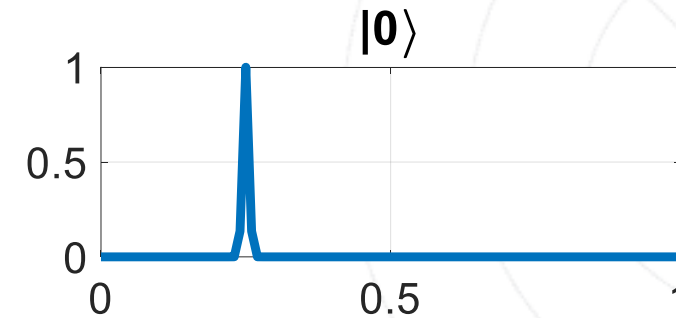
Step 1 Alice creates a random key using:

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

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

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

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

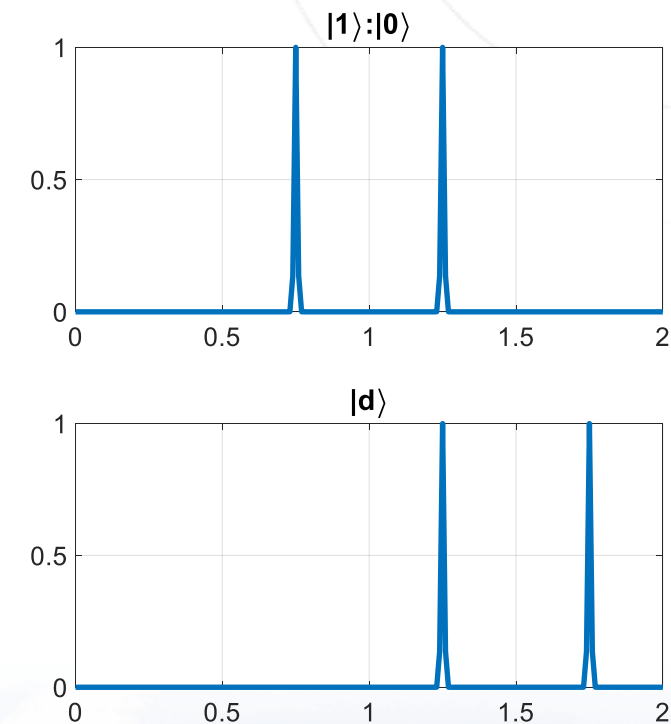
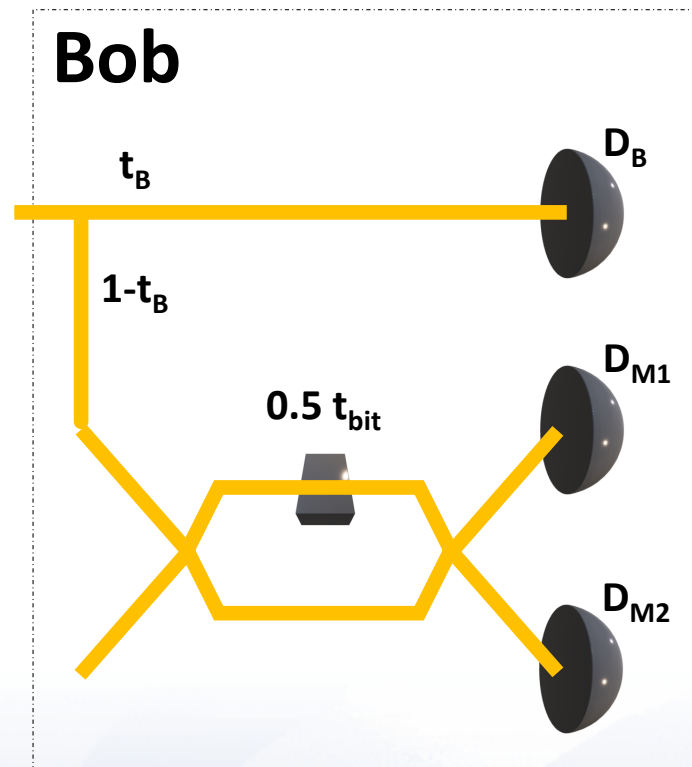


Bob - COW protocol

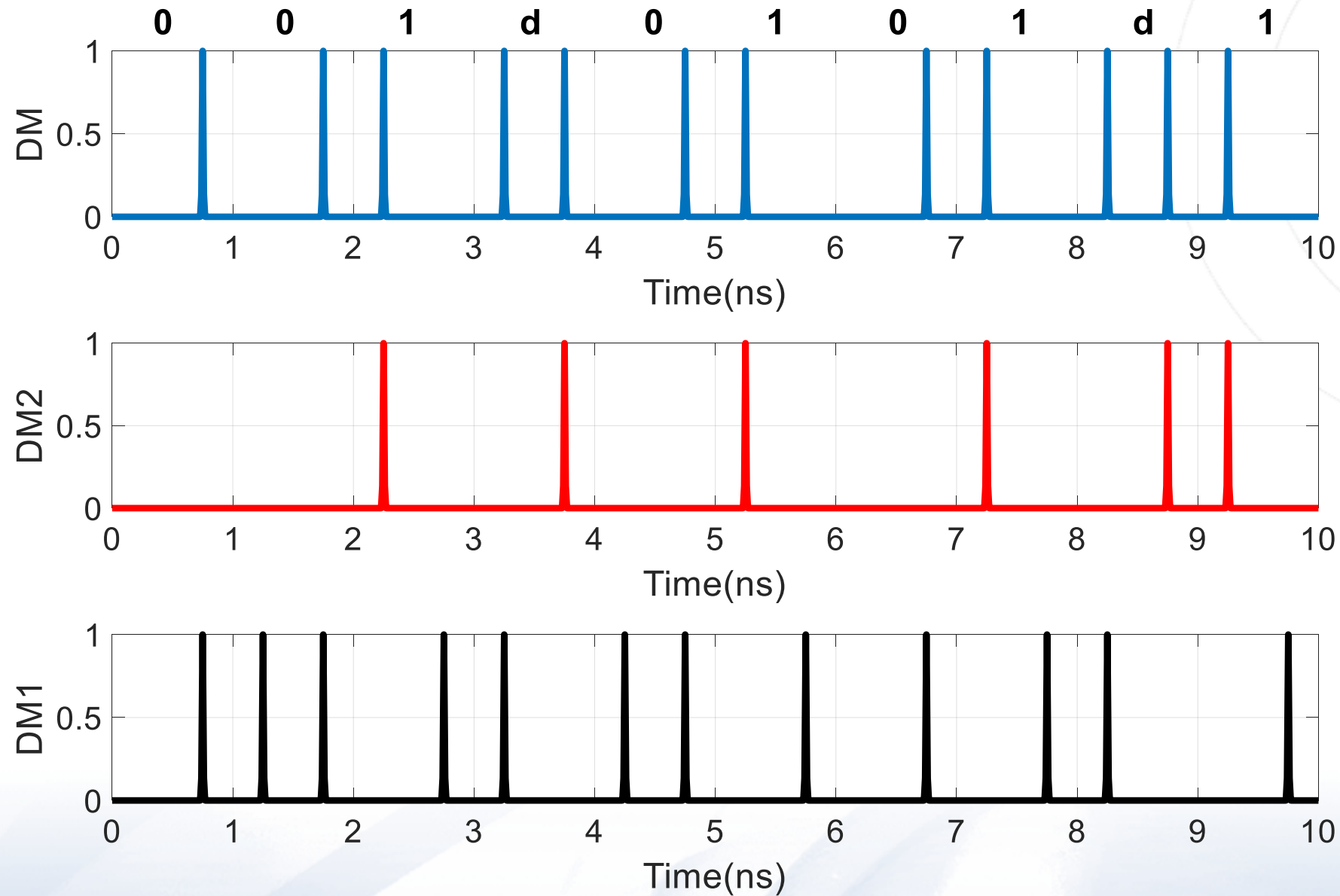
Step 2 A fraction t_B of the photons go into the photon counter D_B , where the bits are discriminated by the time of arrival.

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

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



Monitoring line - COW protocol



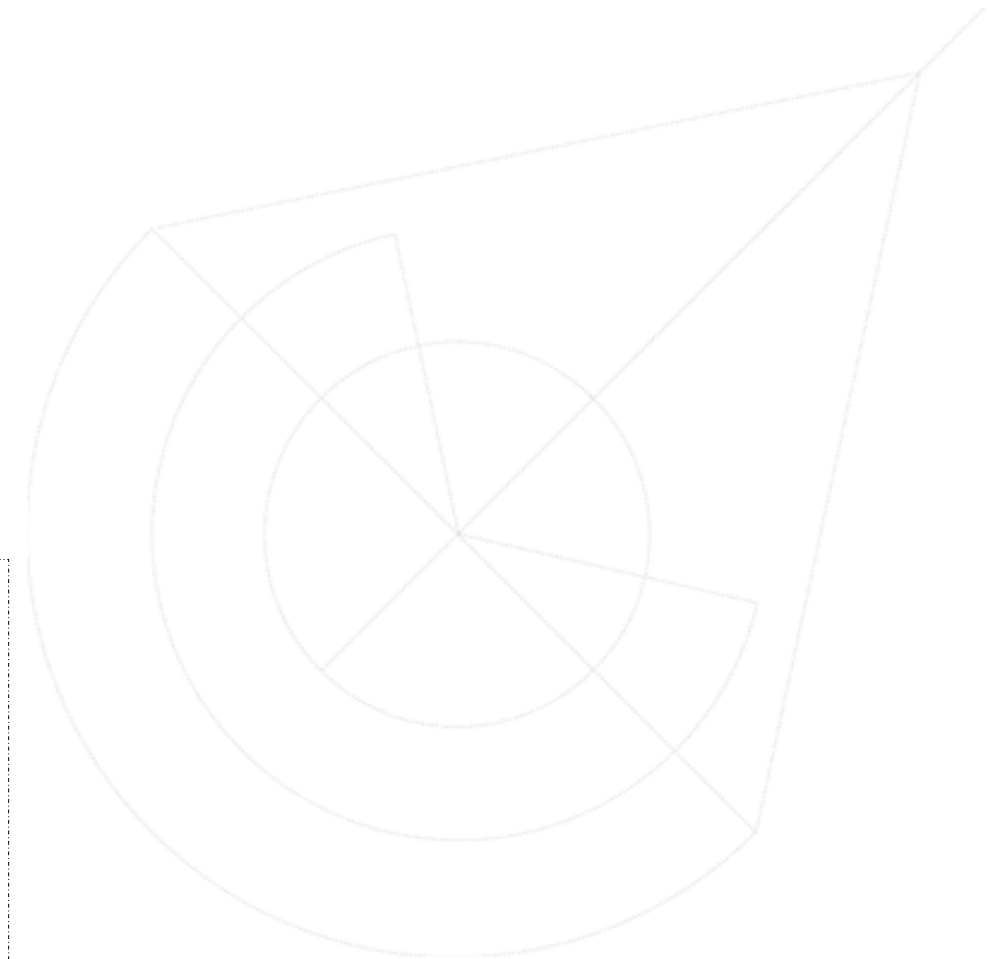
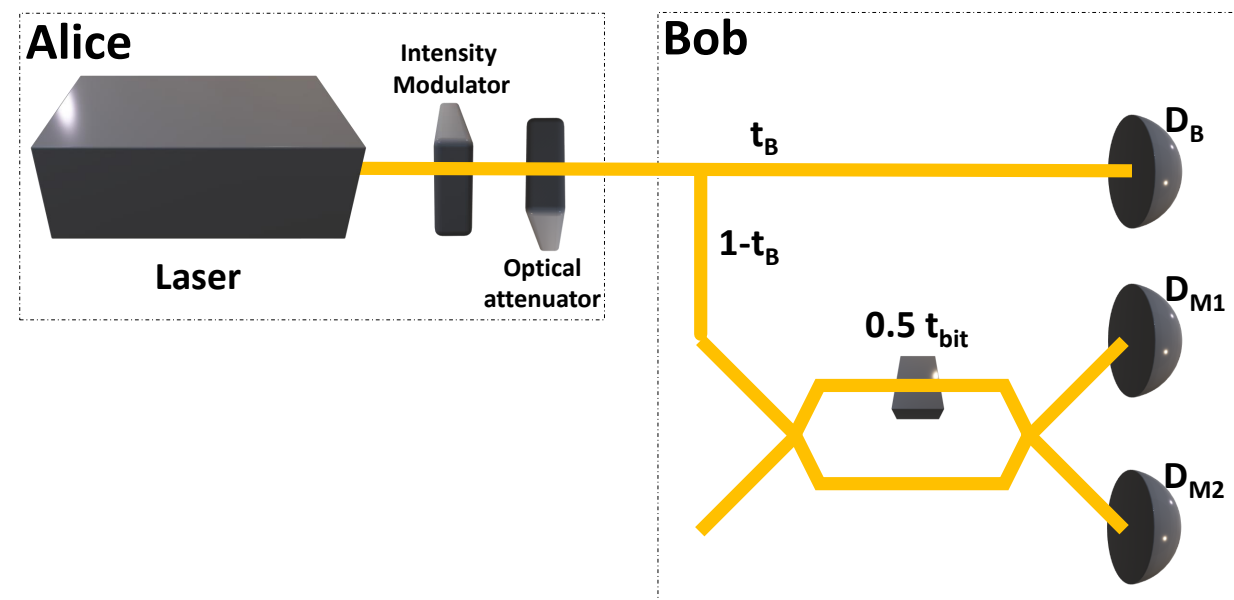
Testing Visibility and Errors - COW protocol

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 $|1\rangle : |0\rangle$.
(If someone created single photons and send it, this D_{M2} would click on wrong times or don't click at all.)

Step 5 Bob reveals the times that D_B fired, and they use those as key.

Step 6 They calculate QBER, check the number of the detections for every detector and if this two properties are within the expected they declared they run error correction and privacy amplification.

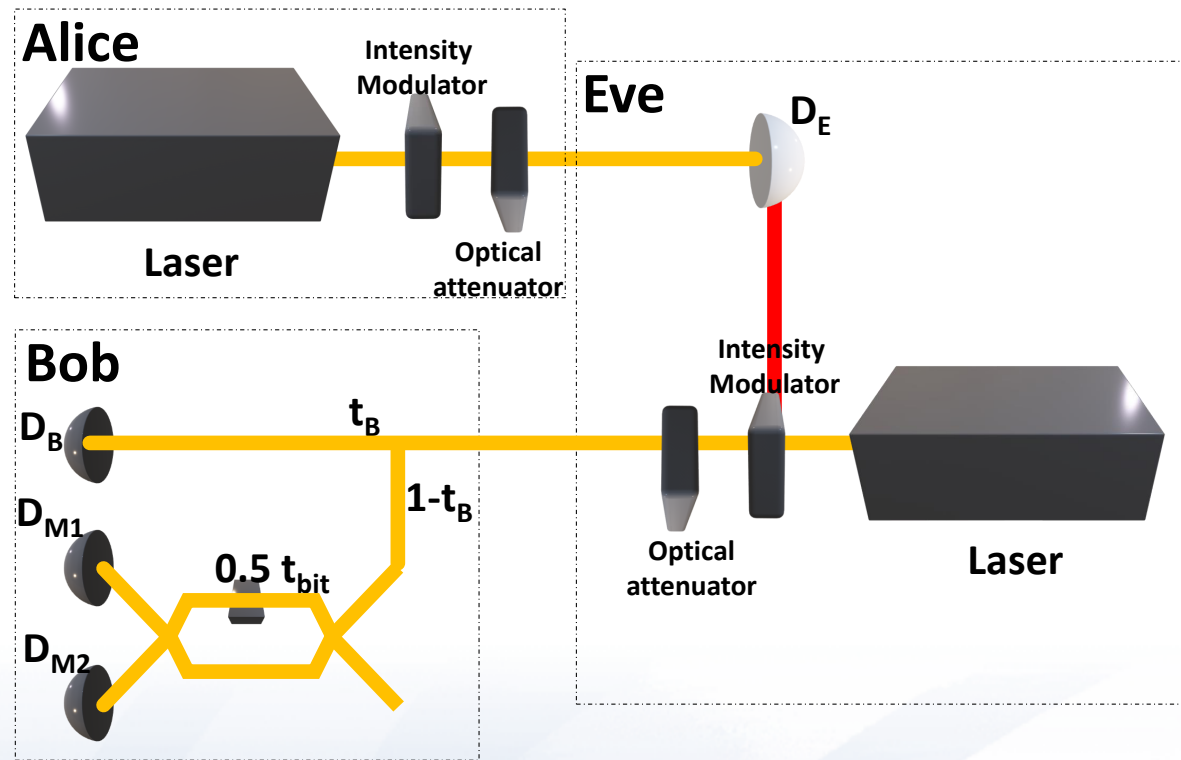


Security

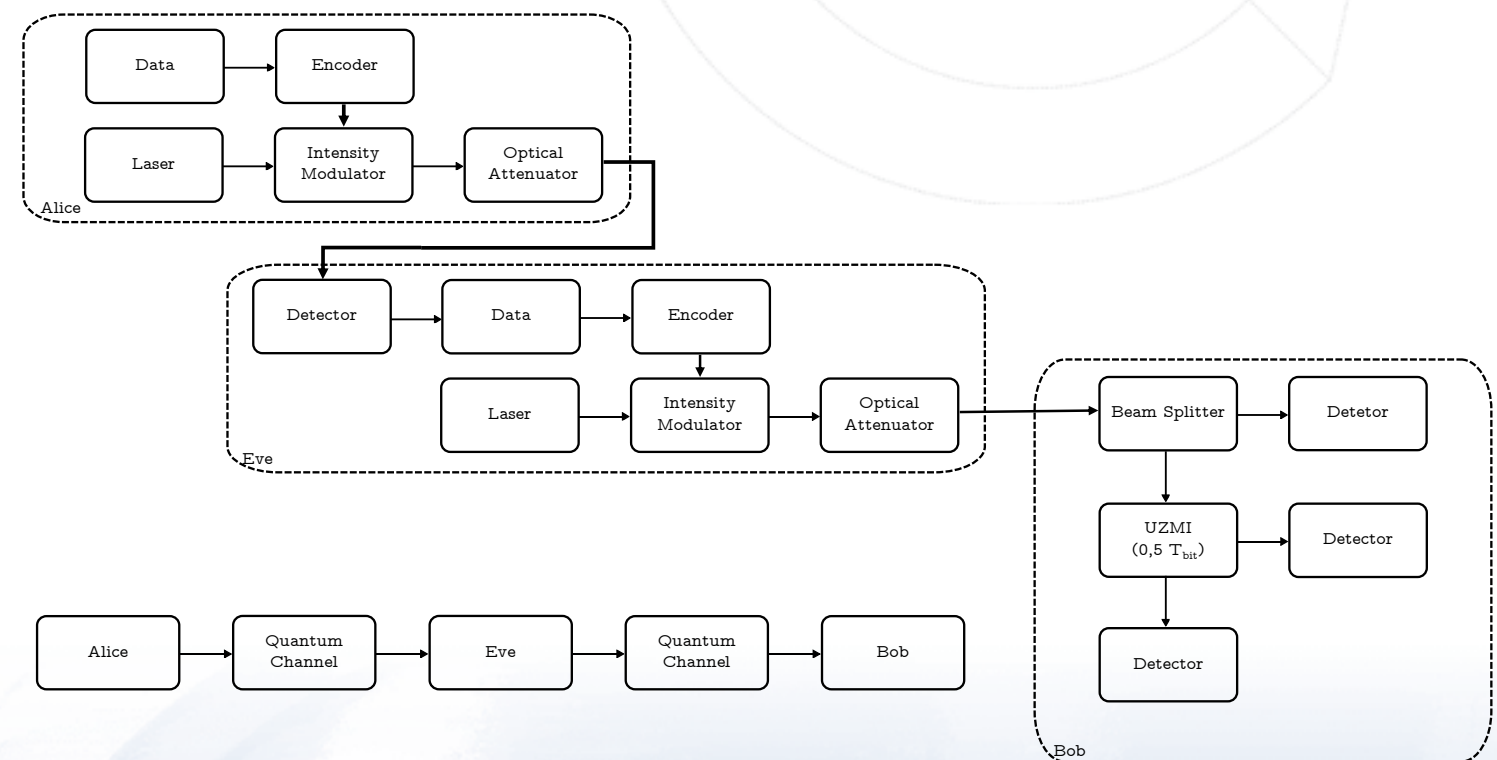
The two main security features of the model is the test of **coherence** and the **Length of the Key**.

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:



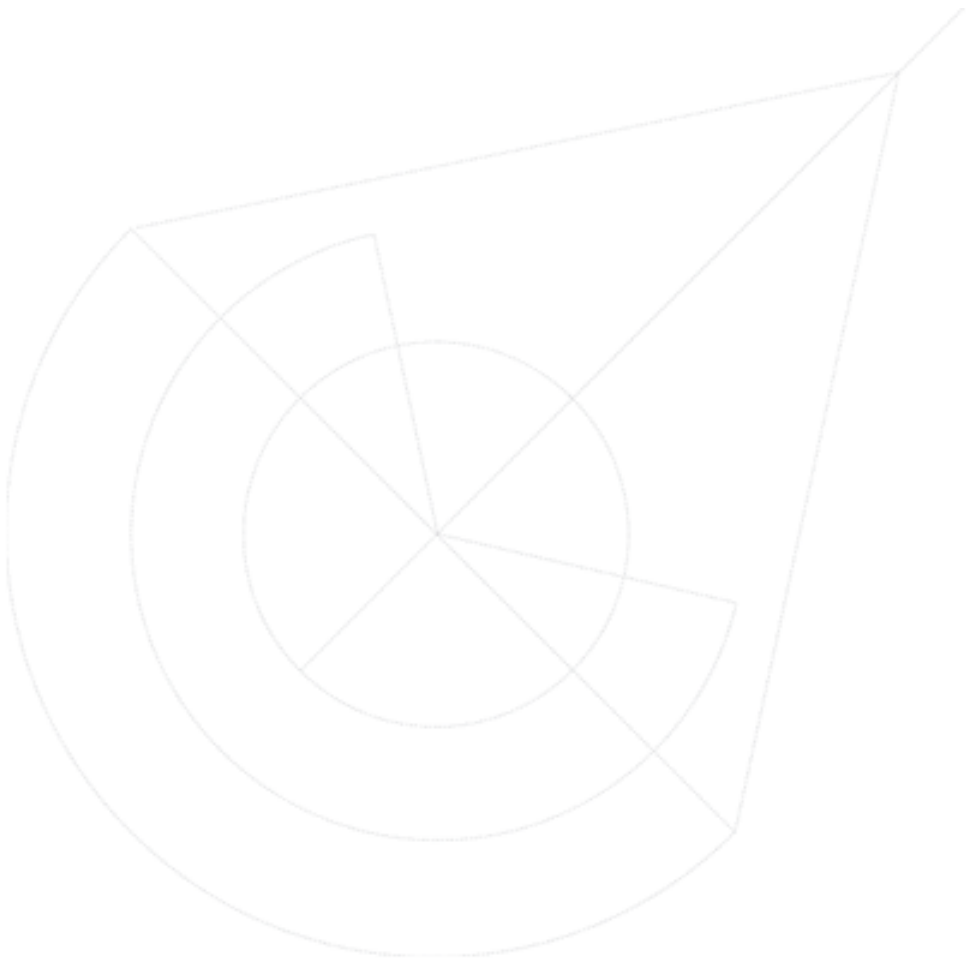
Using a bloc Diagram:



Simulation

For the Simulation, using a fiber without losses:

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 %



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

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.

IR - Eve Attenuation

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

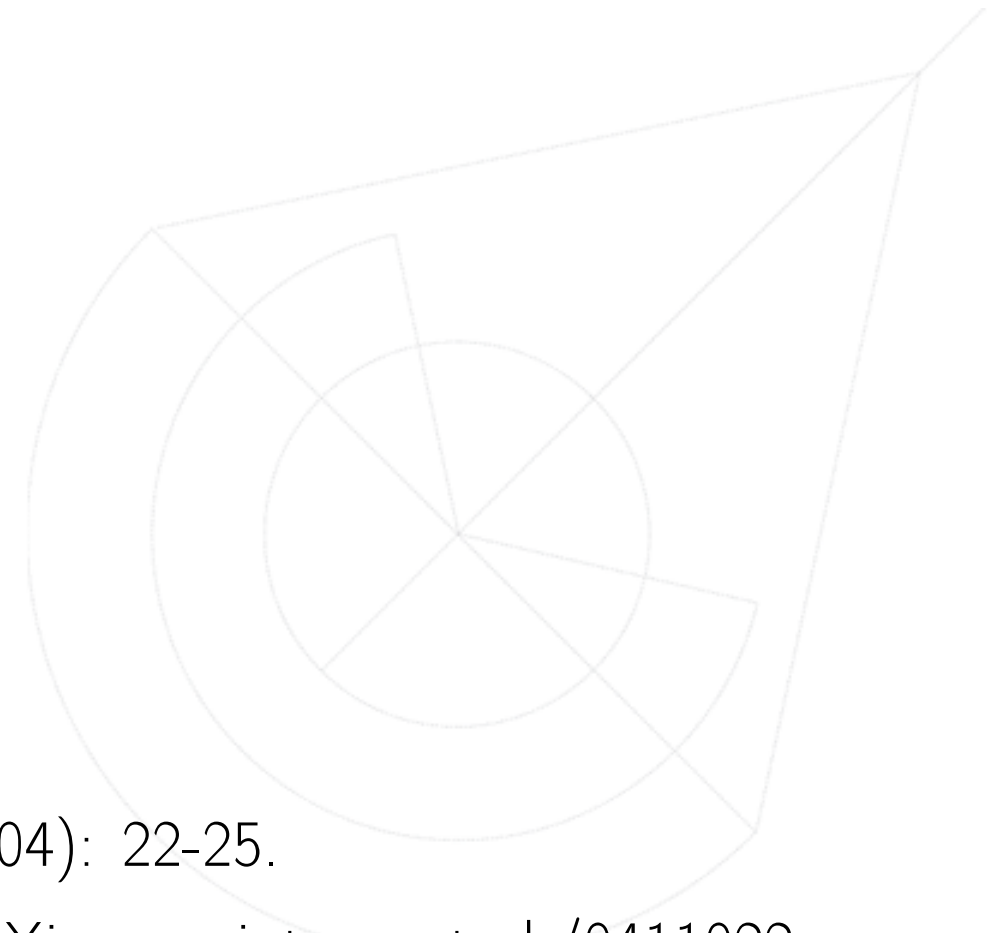
	Eve Attenuation = 1.101			Eve Attenuation = 2		
	Min	Averag.	Max	Min	Averag.	Max
QBER	0.00011775	0.00017323	0.00022875	6.21×10^{-5}	8.93×10^{-5}	0.00011472
$B_{M1} + B_{M2}$	99146	100632	101557	181047	182217	183986
Key Length	423756	424850	426440	739744	741841	743701

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.

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.