universidade de aveiro
theoria poiesis praxis

Coherent One Way (COW) QKD Protocol

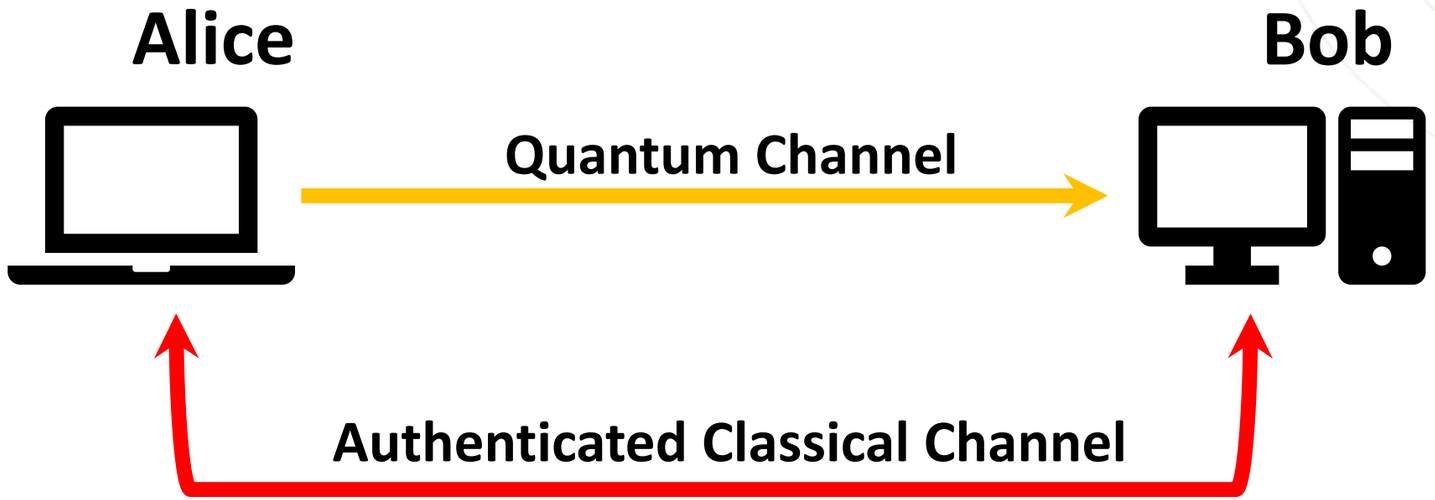
João António[1], Daniel Pereira[2,3], Armando N. Pinto[2,3]

Physics Department[1],
Department of Electronics, Telecommunications and Informatics[2],
University of Aveiro, Aveiro, Portugal
Instituto de Telecomunicações,[3], Aveiro, Portugal

instituto de telecomunicações

Quantum Key Distribution

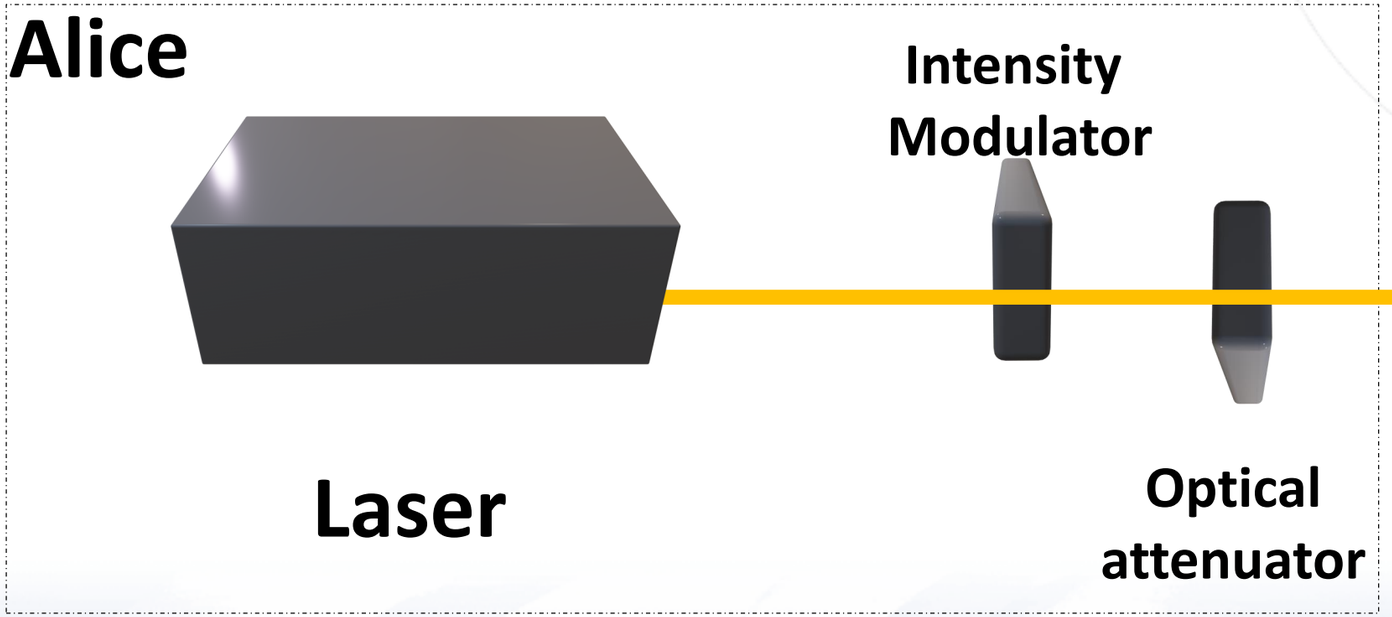
- Quantum Key Distribution (QKD) is a secure way of create and share a unique random key between two spatially distant parties;
- Discrete vs Continuous QKD;
- Codification on polarization or time bins.



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

Time Bin QKD

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



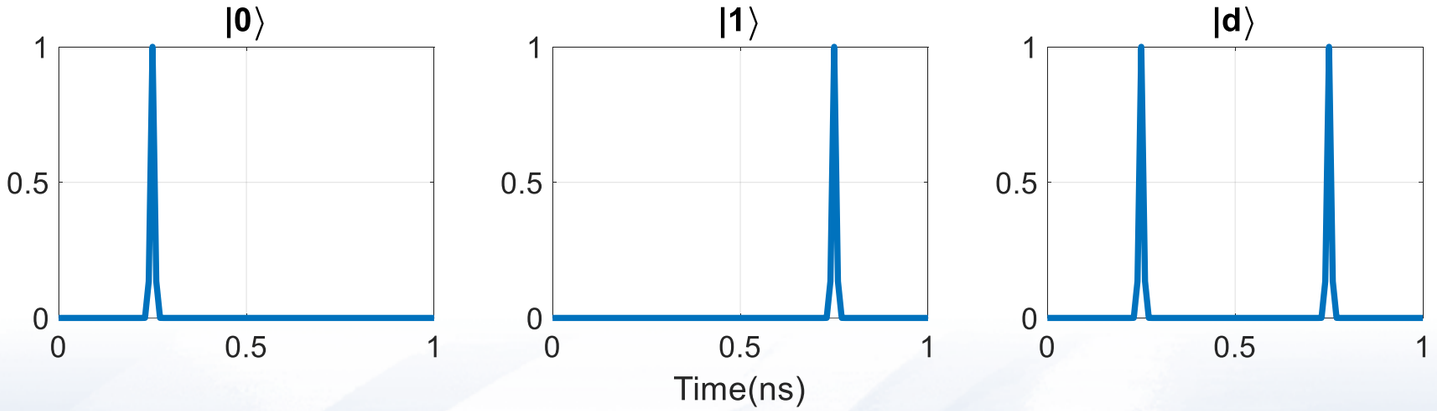
Gisin, Nicolas, et al. "Towards practical and fast quantum cryptography." arXiv preprint quant-ph/0411022 (2004)

Alice

Step 1 Alice creates a random key using:

$$|0\rangle = |\alpha\rangle|\emptyset\rangle = \quad Logical\ 0$$
$$|1\rangle = |\emptyset\rangle|\alpha\rangle = \quad Logical\ 1$$
$$|d\rangle = |\alpha\rangle|\alpha\rangle = DecoyState$$

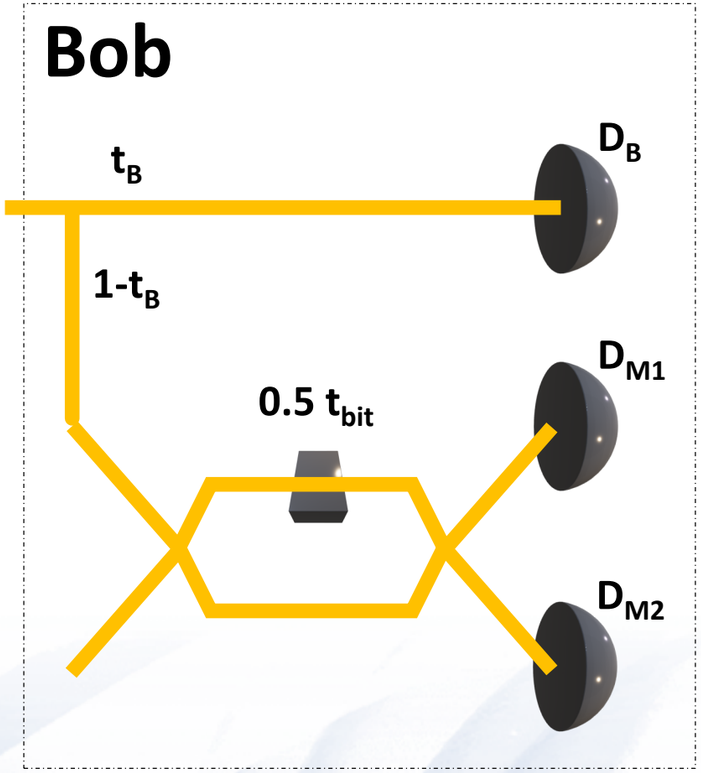
Where $|\emptyset\rangle$ is the vacuum state and $|\alpha\rangle$ is a coherent state of light. The average number of photons by impulse is modulated by a Poisson distribution with $\lambda = 0.1$.



Bob

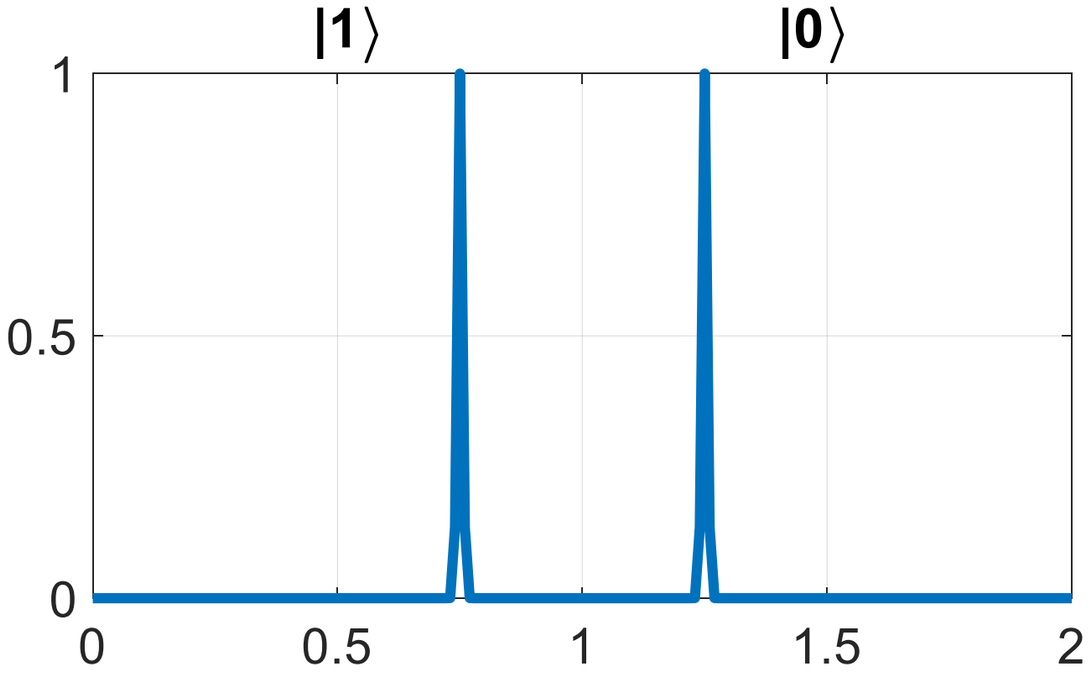
Step 2 A fraction t_B of the photons go into the photon counter D_B, where the bits are discriminated by the time of arrival and are used to create the key.

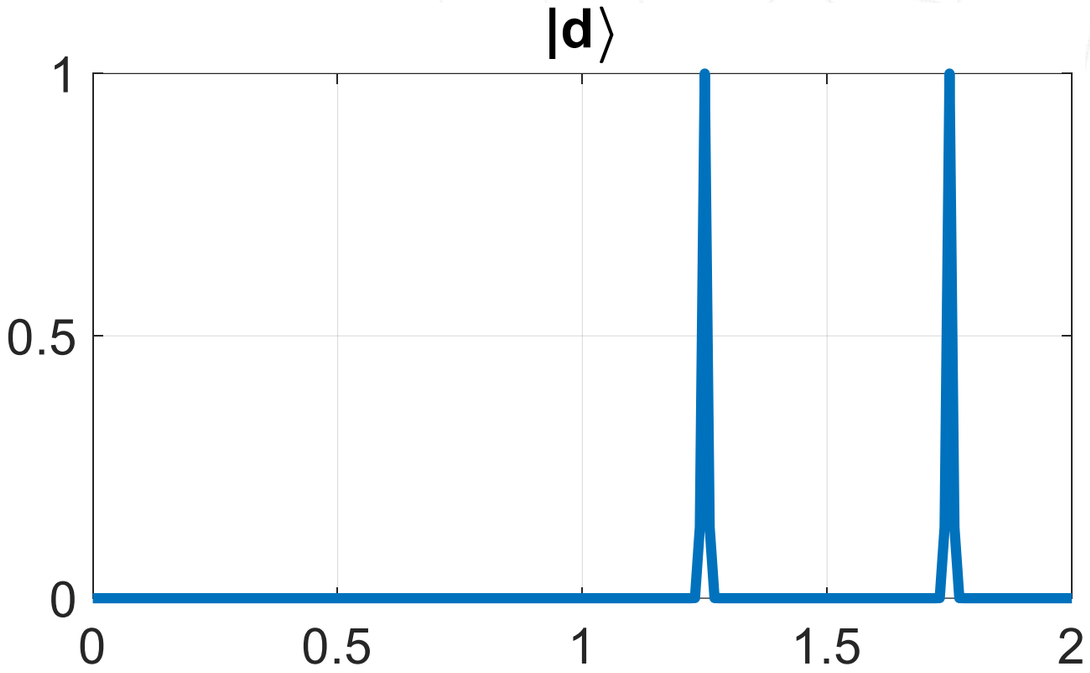
Half of the other photons are delayed by 0.5 t_{bit} interacting with the half of non-delayed bits.



Monitoring line clicks

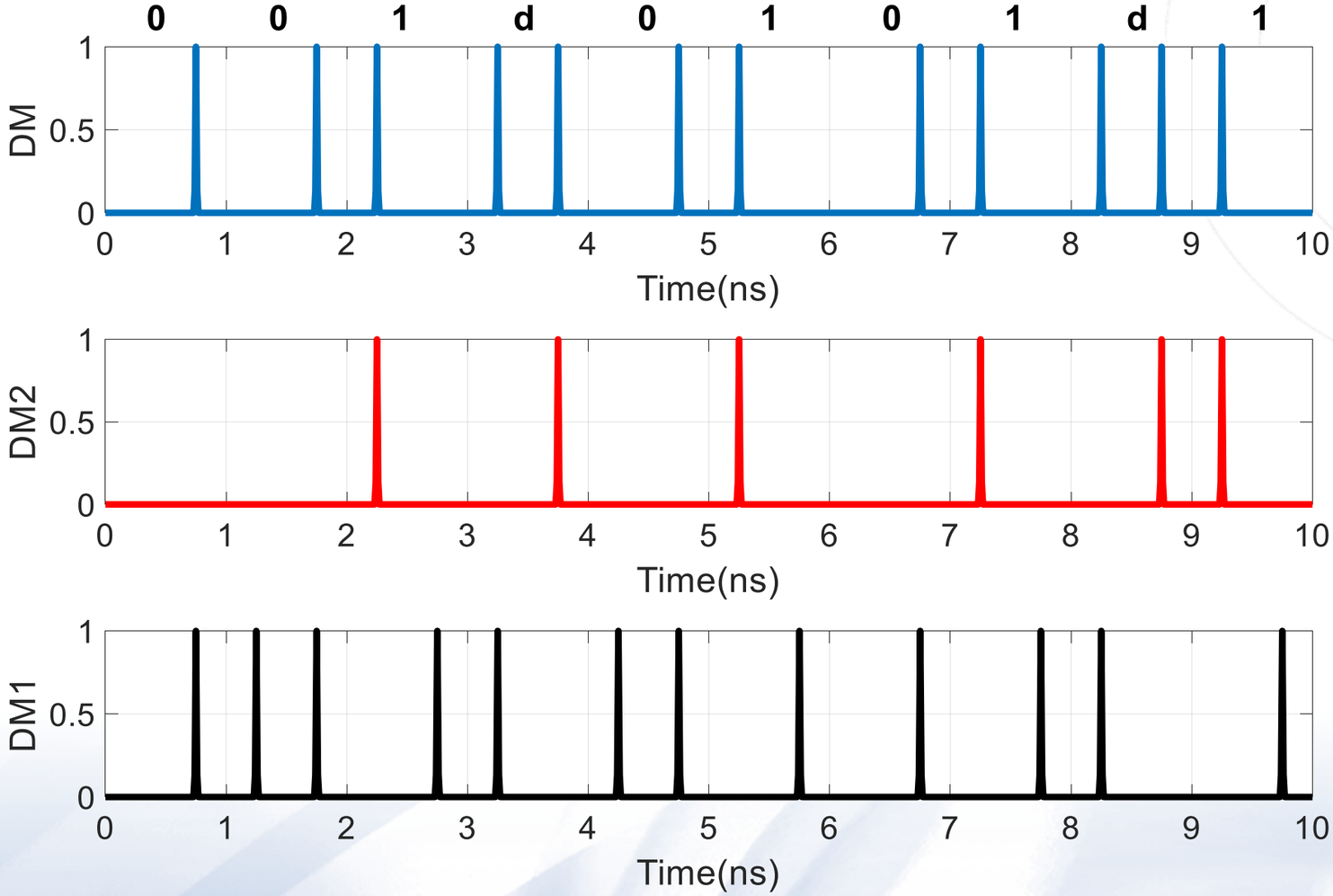
Therefore D_{M2} (constructive photon counter) should only click when, the two pulses go to the monitoring line and the first impulse is delayed:





Monitoring line example

Supposing that all impulses have multiple photons, and all go to the monitoring line.



Testing Visibility and Errors

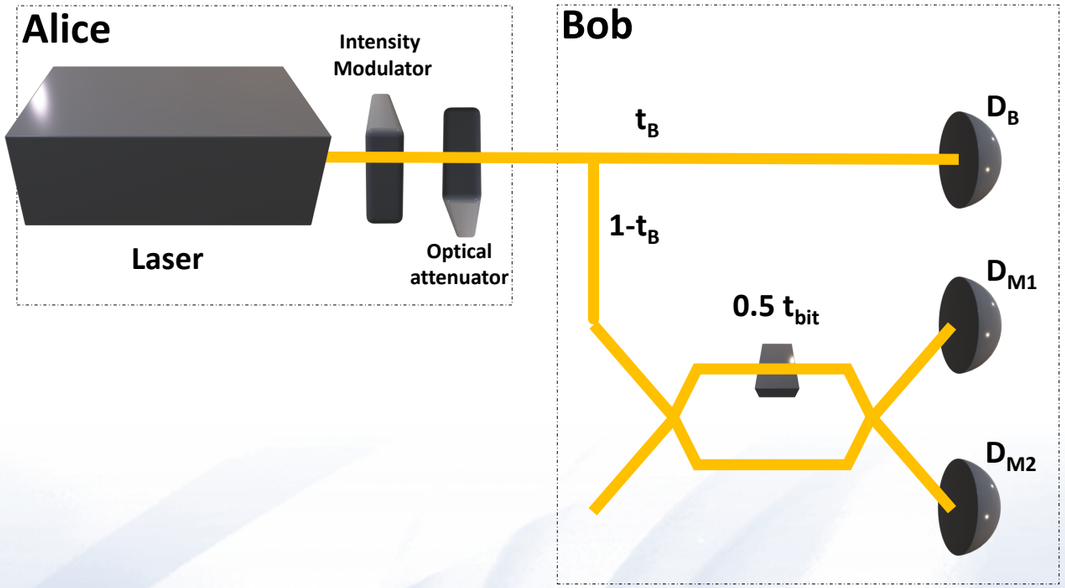
Step 3 Alice tell the decoy times. Bob checks if the D_{M2} has fired during those times.

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.

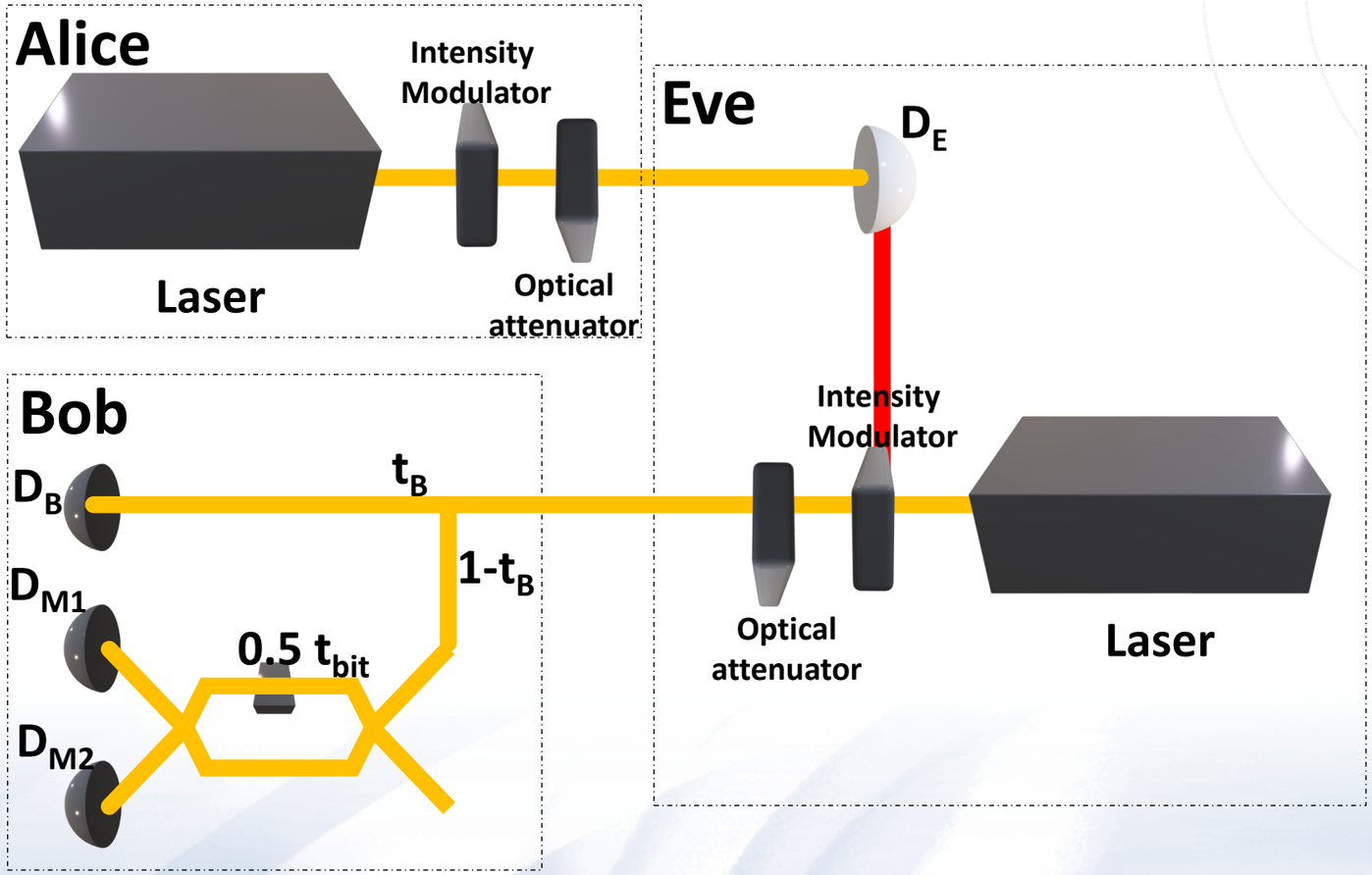
Step 6 QBER, check the number of the detections for every detector.

Step 7 Run error correction and privacy amplification.



Intercept-Resend Attack

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.



Simulation

For the Simulation, using a fiber without looses:

Logical Bits from Alice	$10^7(0.1s)$
Probability of Decoy	10 %
Alice- Nº of Photons per pulse	0.1
Bob Detectors Efficiency	10 %
Bob DarkCount Probability	10^{-5}
Run over	$200\times$
Percentage of the Key for QBER	50 %

The meaning of 0.1 seconds

10^7	$\times 0.1$	$\times 0.9$	$\times 0.9$	$\times 0.5$	$\times 0.5$	$= 40500$
0.1 seconds Alice raw characters	Average Nº of photons by impulse	Bits that go to the Data line	Logical bits that are not decoy states	Used to calculate QBER	Efficiency of Bob's Detectors	Final bits in in the end of Stage 6

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

IR - Eve Efficiency

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

Eve Efficiency	10 %		50 %		90 %		100 %	
	Mean	Std	Mean	Std	Mean	Std	Mean	Std
QBER	0.731298	0.417496	0.192879	0.345973	0.0049682	0.0103909	0.00232442	0.000224006
D_B	5191.22	13182.9	20815	19809.5	38151.9	9209.9	40459.6	122.252
D_{M1}	1153.02	2986.12	4722.48	4519.43	8661.34	2098.9	9169.48	81.2168
D_{M2}	0.04	0.197949	0.24	0.656521	0.36	0.525279	0.64	0.749422

Simulation without attack for comparison:

	Mean	Std
QBER	1.366e-04	0.185e-04
D_B	423899	432.52
D_{M1}	96288.8	329.216
D_{M2}	59.615	8.531

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 Avg. Num. photons/Imp	1.0001		1.1		1.2	
	Mean	Std	Mean	Std	Mean	Std
QBER	0.000171	0.000015	0.000162117	0.000020	0.000151815	0.000017
D_B	387664	665	424371	380.8	461107	569.7
D_B	91434	232.5	100067	183.6	109942	614.0
D_B	52	7.04	65.4	10.41	70.4	5.64

Simulation without attack again for comparison:

	Mean	Std
QBER	1.366e-04	0.185e-04
D_B	423899	432.52
D_{M1}	96288.8	329.216
D_{M2}	59.615	8.531

Conclusion

- It is a practical protocol, it’s already being used by ID Quantic.
- And it is robust to a basic Intercept-resend attack as we just showed.

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.