ScuDo

Scuola di Dottorato ~ Doctoral School

WHAT YOU ARE,TAKES YOU FAR

XXXIII Cycle

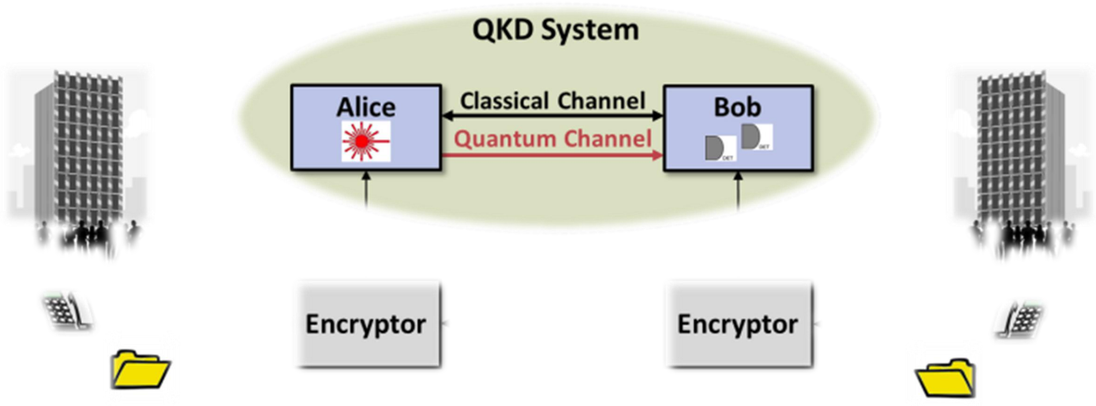
Iterative Information Reconciliation Scheme for Discrete Variable QKD

Francesco Di Stasio, s244644

Supervisor: Prof. Garello Roberto, Mondin Marina

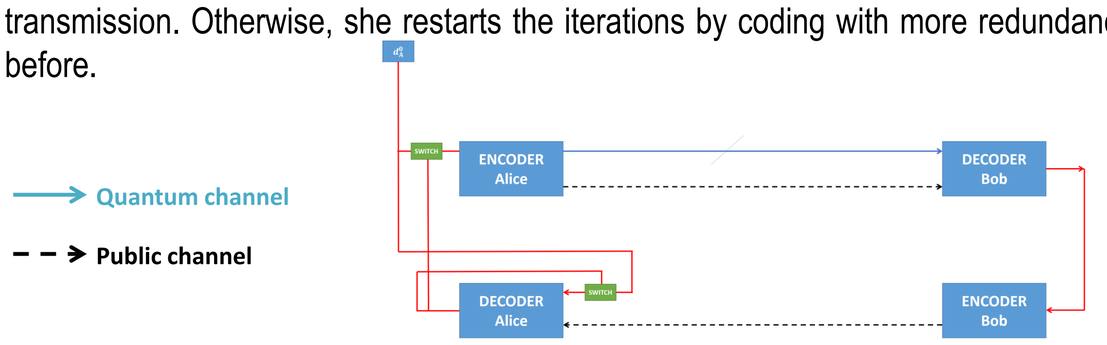
Quantum Key Distribution

- Quantum key distribution (QKD) is a **secure communication method** which implements a cryptographic protocol involving concepts of quantum mechanics.
- It enables two parties, commonly called Alice (transmitter) and Bob (receiver), to produce a secret key known only by them, which can then be used to encrypt and decrypt messages.
- Thanks to quantum mechanics laws, QKD has the ability to notice the presence of any third part (Eve) trying to intercept the key.
- The easiest way to implement a quantum transmission is through free space. Free Space Optics (FSO) employs light propagating through air, vacuum, outer space, or water, to share data.



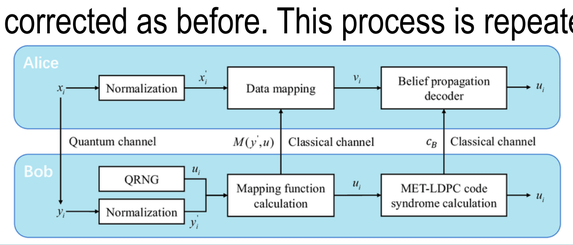
Iterative information reconciliation

- Our idea is to create an **iterative information reconciliation scheme** exploiting the public channel, sending incremental redundancy iteration per iteration. The goal is to minimize the total amount of redundancy (which can be easily intercepted by Eve).
- At the beginning, Alice encodes her message (using a coding scheme c_0), and sends it to Bob over the quantum channel and a minimal amount of redundancy on the public channel (Eve can easily intercepts data over public channels).
- The quantum channel presents some impairments (error rate around 10-13%), public channel is supposed to be perfect (100% success probability).
- Bob receives the informational bits and the redundancy ones, he tries to decode with all the redundancy he has. After that, Bob re-encode the message using a new coding scheme with more redundancy, then he sends back to Alice the redundancy bits using the public channel. Quantum channel is no more used after the first iteration.
- Alice receives and decodes using Bob's redundancy, now she compares the decoded message with the message that she sent at the previous iteration.
- If there are no imparities, she can assume that Bob decoded correctly, so she stops the transmission. Otherwise, she restarts the iterations by coding with more redundancy than before.



Information Reconciliation

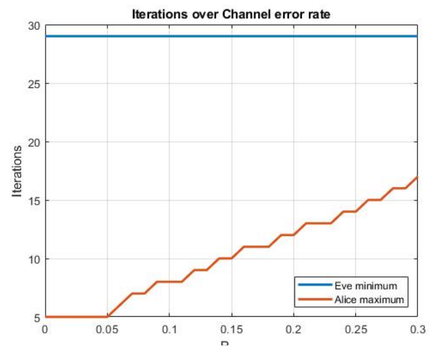
- The message received by Bob can contain differences respect to the sent one. These differences can be caused by eavesdropping, but also by imperfections in the transmission line and detectors.
- **Information reconciliation** is a fundamental step in quantum communications, it is a form of handshake/error correction protocol between Alice and Bob.
- It is conducted over the public channel and as such it is vital to minimize the information sent about each key, as this can be read by Eve.
- **Cascade protocol** operates in several steps, with both keys divided into blocks in each round and the parity of those blocks compared. If an error is found in a block from a previous round that had correct parity then another error must be contained in that block; this error is found and corrected as before. This process is repeated recursively.

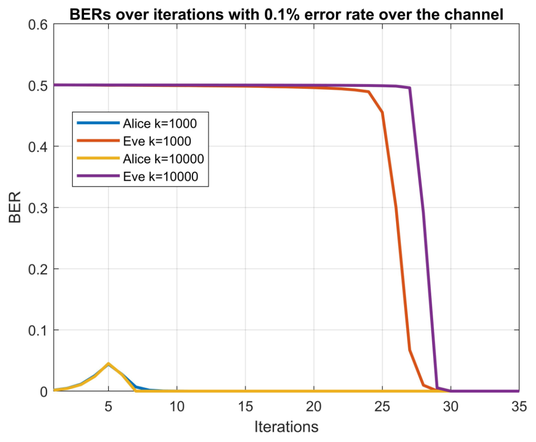


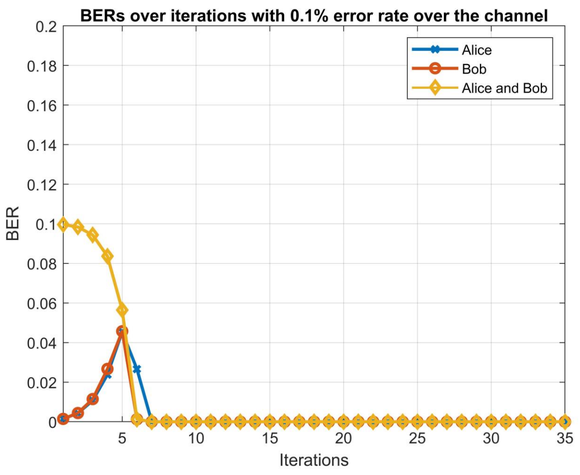
Numerical Results

Simulation environment:

- Coding scheme: **Turbo coding**
- **Puncturing technique** to provide incremental redundancy
- **k=1000/10000** (data length)
- Presence of **one eavesdropper**
- Error rate over quantum channel **[0-0,3%]**
- **Puncturing step 1/40**
- Simulation computed over **1000 codewords**.







Future work

- Simulate with a reslistic Free Space Optics quantum channel.
- Improve the built framework by introducing more efficient coding schemes.
- Reproduce the iterative scheme in the continuous variable domain (Reverse Reconciliation domain).

Submitted and published works

- Mondin, M., Daneshgaran, F., Di Stasio, F., "*Performance of IA-MMSE Iterative Structures for SFBC Decoding in MIMO Systems Using Realistic System Parameters*", 2018 International Symposium on Networks, Computers and Communications (ISNCC).
- Di Stasio, F., Mondin, M., Daneshgaran, F., "*Multirate 5G Downlink Performance Comparison for f-OFDM and w-OFDM Schemes with Different Numerologies*", 2018 International Symposium on Networks, Computers and Communications (ISNCC).
- Daneshgaran, F., Mondin, M., Di Stasio, F., et ali, "*Realistic QKD system hacking and security*", 2018 SPIE Optics + Photonics .
- Daneshgaran, F., Mondin, M., Di Stasio, F., et ali, "*Information reconciliation (IR) for continuous variable quantum key distribution (QKD) over free space optics (FSO) channel*", Free-Space Laser Communications XXXI 2019.
- Daneshgaran, F., Mondin, M., Di Stasio, F., et ali, "*System parameter optimization for minimization of sign error probability in free space optical CV-QKD*", 2019 SPIE Optics + Photonics .
- Daneshgaran, F., Mondin, M., Di Stasio, F., Zacheo, L. "*Use of Deep Learning for Automatic Detection of Cracks in Tunnels: Prototype-2 Developed in the 2017 2018 Time Period*", Journal paper, TRANSPORTATION RESEARCH RECORD.
- Riviello, D. G., Di Stasio, F., "*Analysis of circular and cylindrical array arrangements for mmWave 5G beamforming techniques*", 2019 IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks.
- Riviello, D. G., Di Stasio, F., "*5G beamforming implementation and trade-off investigation of cylindrical array arrangements*", Wireless Personal Multimedia Communications- 2019. Accepted.
- Riviello, D. G., Di Stasio, F., "*A simplified MU-MIMO clustering strategy based on NR Type-2 CSI codebook reports*", Wireless Personal Multimedia Communications- 2019. Accepted.
- Daneshgaran, F., Mondin, M., Di Stasio, F., "*Anatomy of the Mutual Information and Security Analysis of Continuous Variable (CV) Quantum Key Distribution (QKD)*", Journal paper, IEEE J-SAC SI-AQuantumC, Submitted

List of attended classes

Hard skills:

- 01LCPIU – Experimental modeling: costruzione di modelli da dati sperimentali (May 2018, 33 hrs)
- EE 4540 – Introduction of Machine Learning (Jul 2018, 30 hrs) *
- EE 5230 – Wireless Communications (Jul 2018, 30 hrs)*
- 01MMRRV - Tecniche numeriche avanzate per l'analisi ed il progetto di antenne (March 2019, 20 hrs)
- Mobile propagation for 5G and beyond (Doctorate school, June 2019, 30 hrs).

Soft skills:

- 02RISRV – Communication (June 2018, 5 hrs)
- 01RNBRV – Communication II (Sept 2019, 12 hrs)
- 01SWPRV - Time management (July 20019, 2 hrs)
- Decision Making and Policy Design (ASP school, July 2019, 15 hrs)

- * Attended in California State University in Los Angeles

POLITECNICO DI TORINO

PhD program in

Electrical, Electronics and Communications Engineering