POLITECNICO
DI TORINO

SOFT PROCESSING TECHNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Marina Mondin

January 27°, 2012

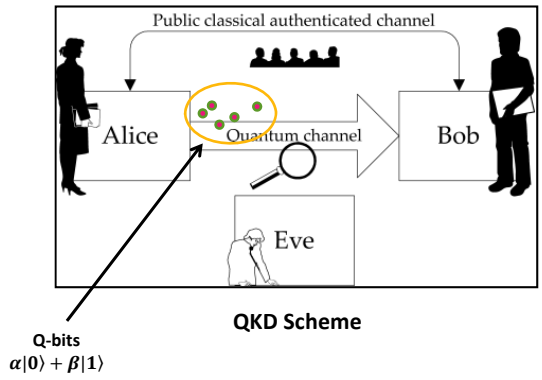
Quantum Communications

- In the past decades, the key to improving computer performance has been the **reduction of size in the components** used in modern processors
- If the components become much smaller, **the effects of quantum mechanics** will begin to affect their performance. It would therefore seem that these effects present a fundamental limit to our computer technology.

Quantum Key Distribution (QKD)

- In the last decades QKD it has emerged as one of the **most important practical applications of quantum mechanics**
- While the security of traditional cryptographic techniques relies on assumptions about the complexity of mathematical algorithms, **the security of quantum cryptography is firmly based on the laws of quantums physics**
- The security of Quantum Key Distribution (QKD) comes from the fact that **measuring the state of a quantum system cannot be made without perturbing it**

Introduction to QKD



QKD Scheme

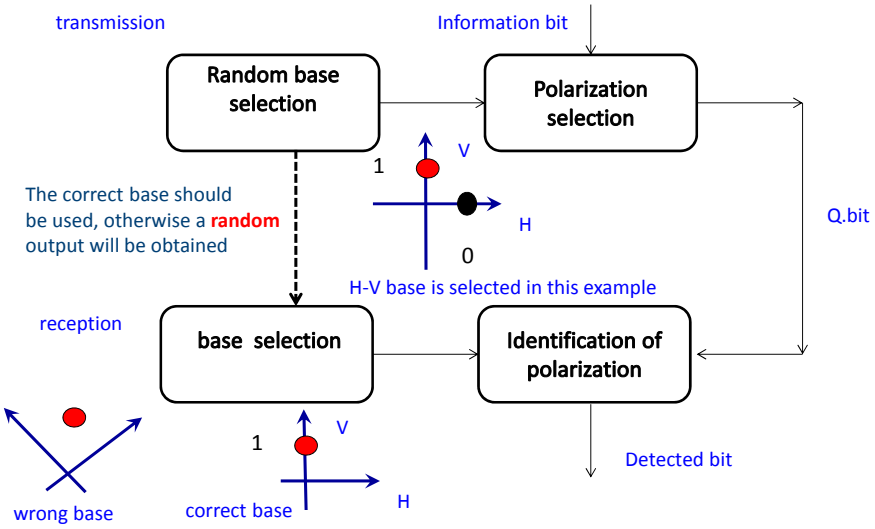
SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Introduction to QKD

- Bits are associated ideally to a single **PHOTON** (therefore called Q-bit)
- Photons can be “encoded” using different bases ((H-V), diagonal, circular)
- Each «base» is composed of two orthogonal polarizations
- The transmission of each photon is composed of
  - Selection of a random base (out of two possible options)
  - Selection of the desired polarization within the considered base
- We consider a valid **KEY** any set of random bits known by bot Alice and Bob (and not Eve)
- The received secure key will be used for (one time pad) public-key encription

SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Introduction to QKD



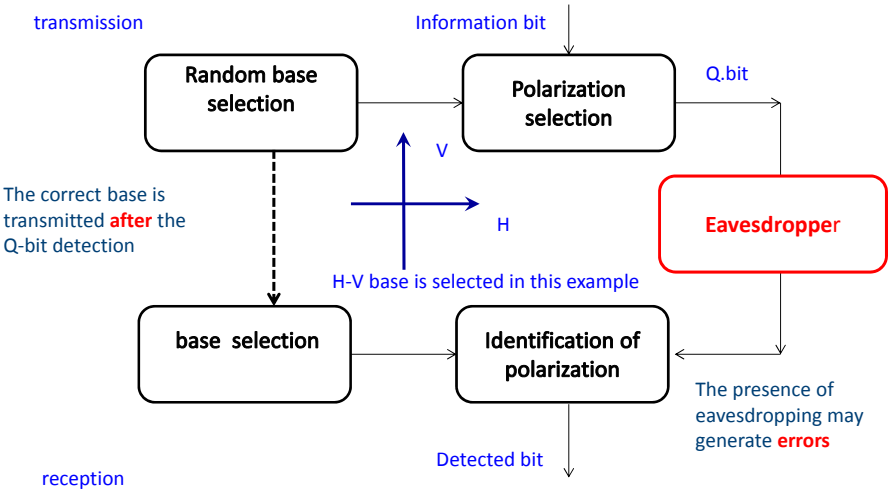
Quantum Superposition Principle

When making a **measurement** the system is forced to make a random selection among the possible states and choose one. After the measurement, the system is in the state that will always give that answer; the possibility of other answer is gone

No-cloning theorem

The no-cloning theorem **forbids the creation of identical copies** of an arbitrary unknown quantum state.

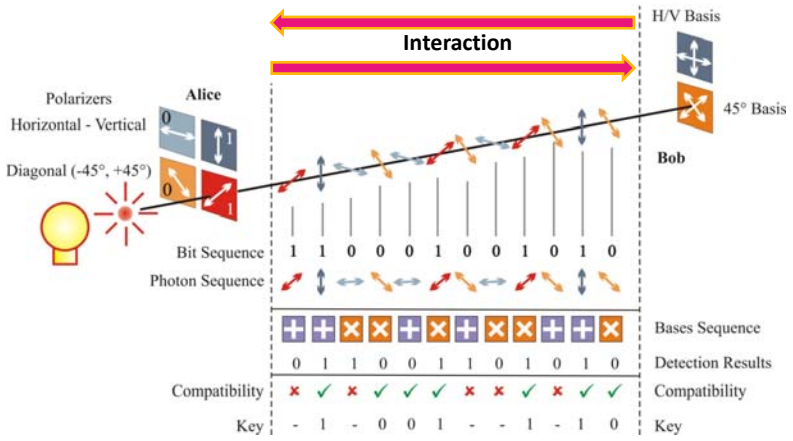
Introduction to QKD



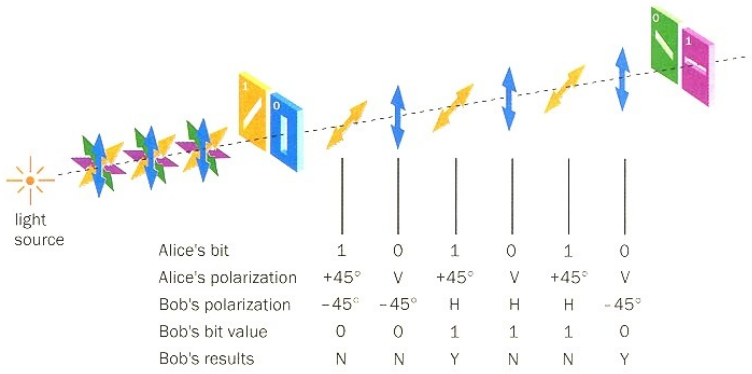
Introduction to QKD

- Up to now, the most famous protocol suggested for QKD is the BB84 protocol
- The BB84 protocol consists of four stages:
  - ✓ Transmission of the randomly encoded single photon stream
  - ✓ Sifting of the previously exchange key
  - ✓ Reconciliation to correct errors
  - ✓ Privacy amplification in order to distill a final secure key
- BB84 uses the cascade reconciliation protocol, which operates in a number of rounds, and requires **interaction** between the two parties

BB84 Protocol



B92 Protocol



Soft-QKD Protocols

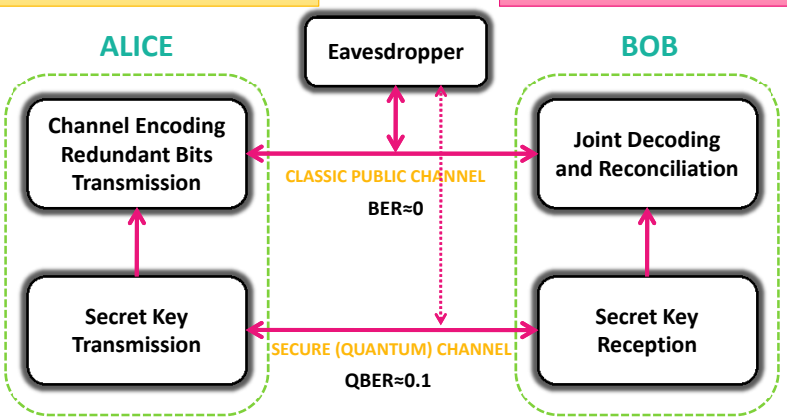
- Even in absence of eavesdopping, errors may occur, and error correction (information reconciliation) may be needed
- We have been focusing on pragmatic information reconciliation schemes applied to QKD schemes using **soft information** processing techniques
- They can be applied to QKD schemes based both on **Single Photons** or **WLP (weak laser pulse)** sources with or without the use of decoy states
- The proposed information reconciliation protocols will use typically **feed-forward techniques**, minimizing the interaction between transmitter and receiver

SOFT METRIC BASED QKD PROTOCOL

The considered QKD Scheme

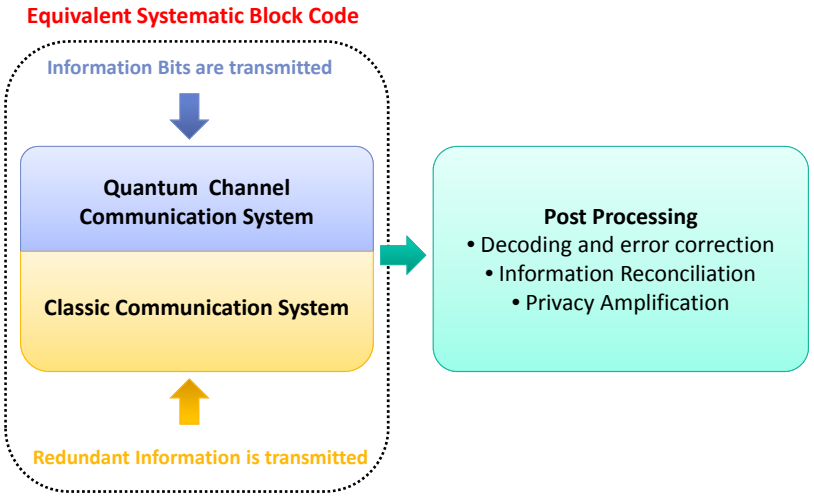
Transmission rate on QKD secret channel is generally low compared to the rate on the public channel

Many attack strategies can be used by Eve, but they will alter the independent nature of the quantum channel



The BER on the public channel is low, while the QBER on the secure channel is high. Channel coding is required to make the secure channel more reliable

Soft-Metric Based QKD Protocol

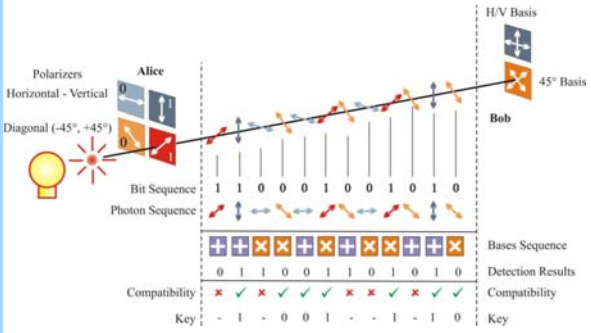


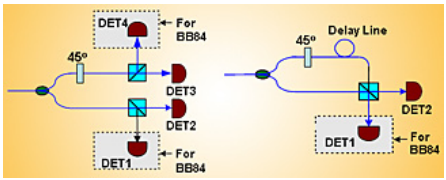
LDPC for Information Reconciliation

- **Low Density Parity Check codes (LDPC)** are suggested, with the use of long information blocks. LDPC codes are **forward error correcting (FEC)** codes that have performance close to Shannon's channel capacity
- In spite of the large block length (which guarantees high coding rate), the use of **iterative decoding allows for acceptable decoding complexity**
- To minimize the quantity of information derived by Eve from the public channel **the code rate must be maximized**

SYSTEM CHARACTERIZATION: QUANTUM CHANNEL MODELS

Quantum Channel

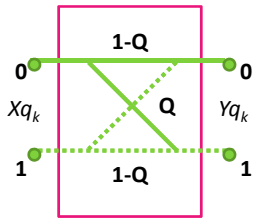




Some schemes for BB84 Protocol

BSC Quantum Channel

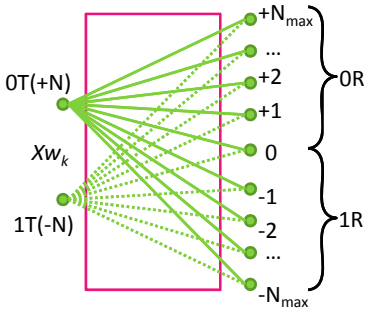
- Quantum channel can be modeled as a simply binary channel with error probability equal to the quantum bit error rate Q, when a **single photon** is transmitted



Single Photon Quantum Channel

Multiple Output Quantum Channel

- When using **WLP** and **decoy states**, where N_{max} photons are transmitted for every information bit, the quantum channel can be modeled as a multiple output discrete channel



Quantum Channel using WLP

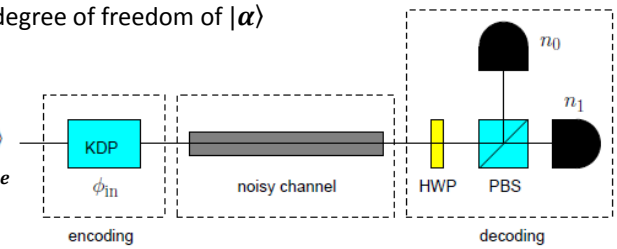
SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Bayesian Inference Quantum Channel

The information is encoded in **qubits** representing the polarization degree of freedom of $|\alpha\rangle$

$|\alpha\rangle$: ***coherent state***

$|+\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}$



x_{in}	$\rightarrow$	φ_{in}
0	$\rightarrow$	$\pi/4$
1	$\rightarrow$	$3\pi/4$

Bayesian estimation is used to obtain the stimated phase received at the detection stage

SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

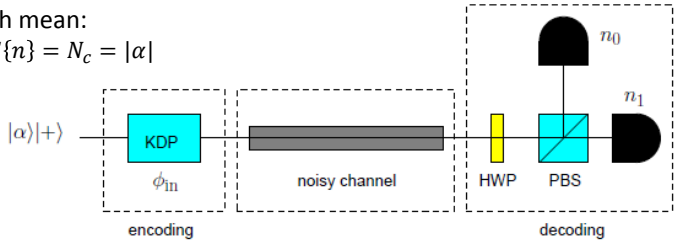
Bayesian Inference Quantum Channel

The number of transmitted photons (n) is a Poisson distributed random variable with mean:

$$E\{n\} = N_c = |\alpha|$$

Total numer of detected photons:

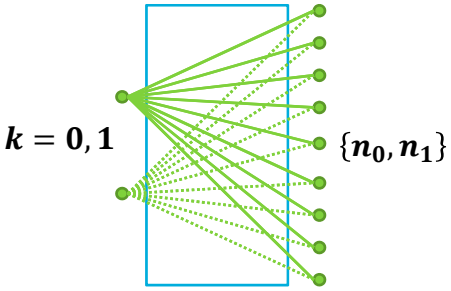
$$n = n_0 + n_1$$



x_{in}	$\rightarrow$	φ_{in}
0	$\rightarrow$	$\pi/4$
1	$\rightarrow$	$3\pi/4$

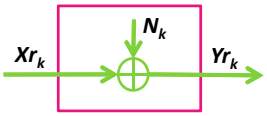
BIMO Quantum Channel

The system described up to this point can be modeled as a Discrete Memoryless Channel (DMC) and more precisely as a **Binary Input Multiple Output** (BIMO) channel



Classic Communication System

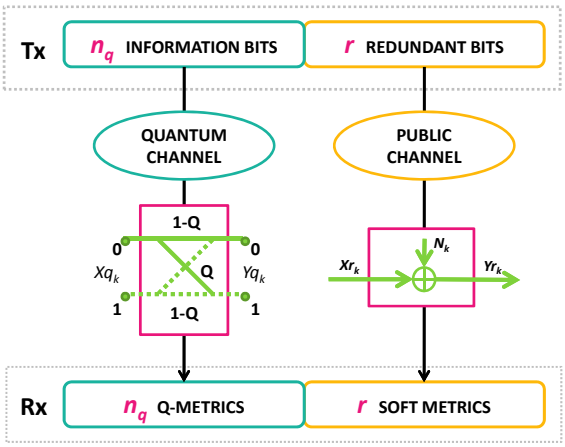
- The public channel uses **classic communication schemes**, typically a radiofrequency link
- Since **deep coding is allowed** the BER is extremelly small
- It is modelled using an aditive white Gaussian noise channel **(AWGN)**



Public Channel

AVAILABLE BITS AND METRICS

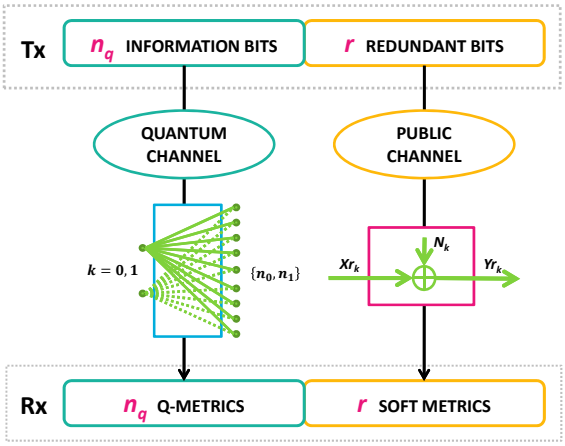
BSC Quantum Channel



Code Rate

$R_c = n_q/(n_q+r)$

BIMO Quantum Channel



Code Rate

$R_c = n_q/(n_q+r)$

Log Likelihood Ratios

$$LLR(y_{r_k}) = log\left[\frac{p(x_{r_k}=1|y_{r_k})}{p(x_{r_k}=0|y_{r_k})}\right] = log\left[\frac{p(y_{r_k}|x_{r_k}=1)}{p(y_{r_k}|x_{r_k}=0)}\right]$$

Evaluation Of Soft Metrics: Classical Channel

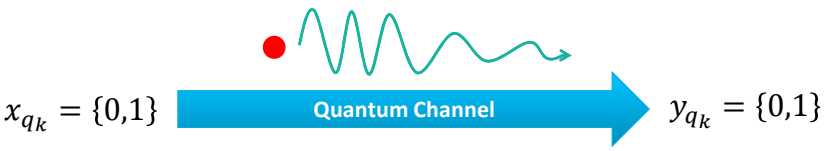
- As far as the **redundant bits** are concerned, we are dealing with the real received signal samples, whose conditional probability density function is

$$f_Y(Yr_k \mid b_k) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{\left(Yr_k - \sqrt{E_b}(2b_k - 1)\right)^2}{2\sigma^2} \right)$$

- Hence, the corresponding log-likelihood metrics are

$$LLR(Yr_k) = \frac{2Yr_k\sqrt{E_b}}{\sigma^2}.$$

Log Likelihood Ratios



$$LLR(y_{q_k}) = log\left[\frac{p(x_{q_k}=1|y_{q_k})}{p(x_{q_k}=0|y_{q_k})}\right] = log\left[\frac{p(y_{q_k}|x_{q_k}=1)}{p(y_{q_k}|x_{q_k}=0)}\right]$$

Evaluation of Soft Metrics: Quantum Channel (case 1)

- As far as the **information bits** are concerned, when single photon transmission is used, a BSC channel model as shown previously must be considered, with transmitted bits and received bits, whose soft metrics are

$$LLR(Yq_k) = \begin{cases} \log[(1-Q)/Q] \text{ if } Yq_k = 1 \\ \log[Q/(1-Q)] \text{ if } Yq_k = 0 \end{cases}.$$

Evaluation of Soft Metrics: Quantum Channel (case 2)

- An alternative metric has also been considering supposing that the equivalent BSC model used in the private channel is obtained transmitting with a **2 PAM scheme** so that:

$$Yp_k = \sqrt{Ep_b}(2b_k - 1) + Np_k \qquad P(b_k \text{in error}) = \frac{1}{2} erfc\left(\frac{\sqrt{Ep_b}}{\sqrt{2}\sigma_p}\right) = Q$$

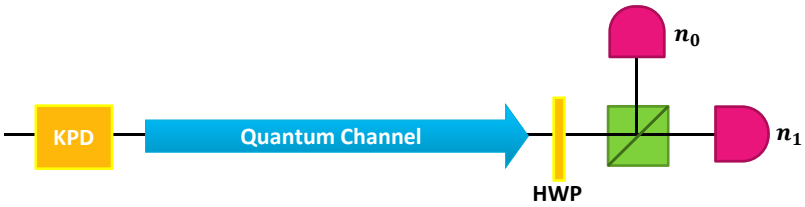
$$Yp_k \cong \sqrt{Ep_b}(2b_k - 1) \cong \sqrt{Ep_b}(2\hat{b}_k - 1))$$

$$LLR(Yp_k) = \frac{4Yp_k\sqrt{Ep_b}}{2\sigma_p^2} = \frac{4Ep_b(2\hat{b}_k - 1)}{2\sigma_p^2} =$$

$$= 4erfc^{-1}(2Q)(2\hat{b}_k - 1) = \begin{cases} +4erfc^{-1}(2Q) \text{ if } \hat{b}_k = 1 \\ -4erfc^{-1}(2Q) \text{ if } \hat{b}_k = 0 \end{cases}$$

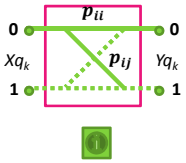
SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Evaluation of Soft Metrics: Bayesian Inference Quantum Channel



$$LLR(n_0, n_1) = (\boldsymbol{n_1} - \boldsymbol{n_0})\, log\left(\frac{p_{ii}}{p_{ij}}\right)$$

$$LLR(n_0, n_1) = (\boldsymbol{n_1} - \boldsymbol{n_0})\, log\left(\frac{1-p_{ij}}{p_{ij}}\right)$$



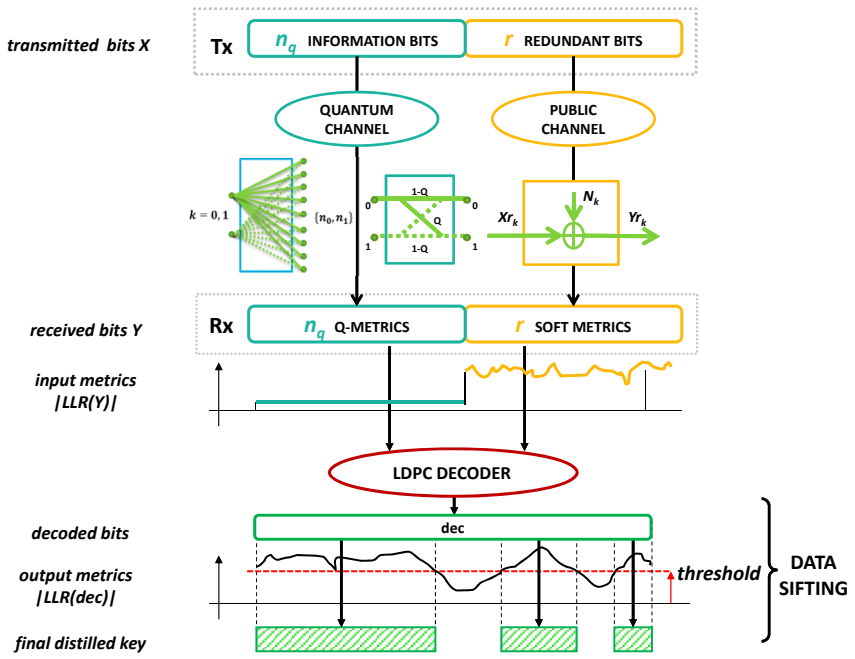
SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Evaluation of the Log-Likelihood Ratios

From the work of *Teklu and Olivares*, where it is assumed that during propagation, the qubit goes under a phase diffusion process whose amplitude is characterized by the parameter Δ, the following expression can be derived:

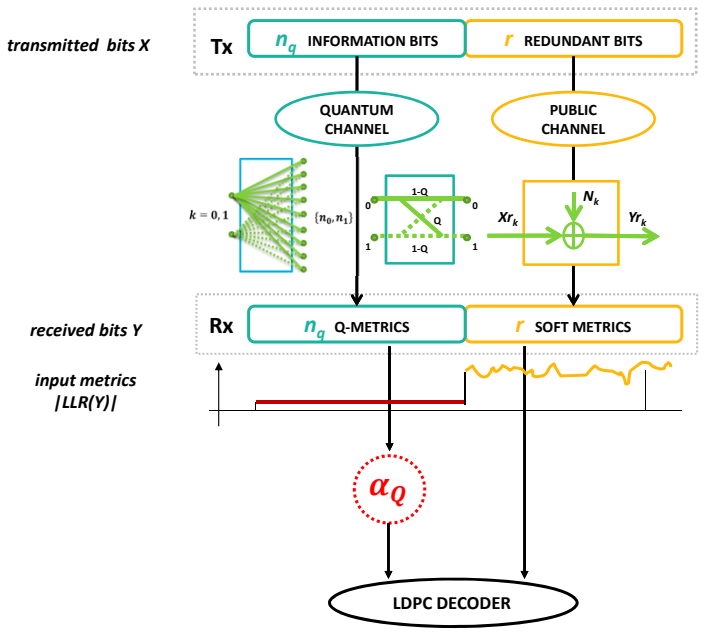
$$p_{ii} = p(0|\varphi_0) = p(1|\varphi_1) \qquad p_{ij} = p(0|\phi_1) = p(1|\phi_0)$$

$$p(0|\phi_k) = \tfrac{1}{2}\left(1 + e^{-\Delta^2}\cos(\phi_k)\right), \qquad p(1|\phi_k) = 1 - p(0|\phi_k)$$



DATA SIFTING

- The availability of **soft output information**, where the decoded bits are paired with the associated reliability, offers an instrument for performing **efficient and selective information reconciliation**
- Deleting from the decoded sequence (i.e., form the quantum key), the bits with low reliability, maintaining the most trusted information, allows for a **variable rate security key generation protocol**

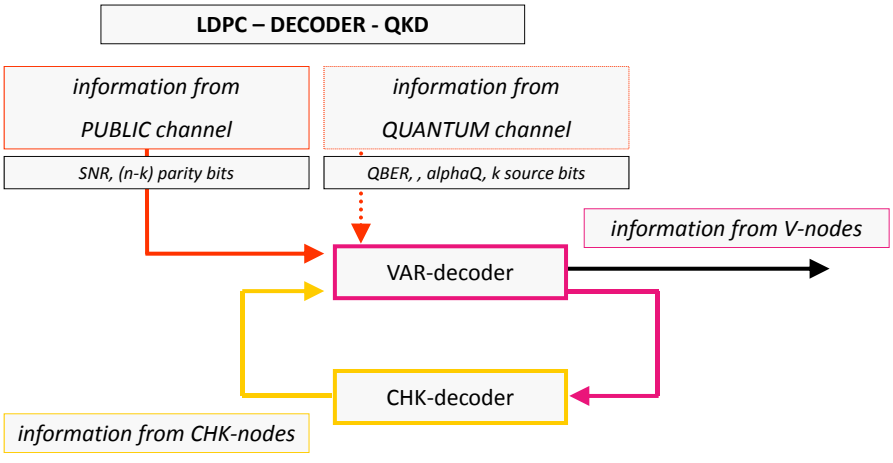


CONVERGENCE ANALYSIS

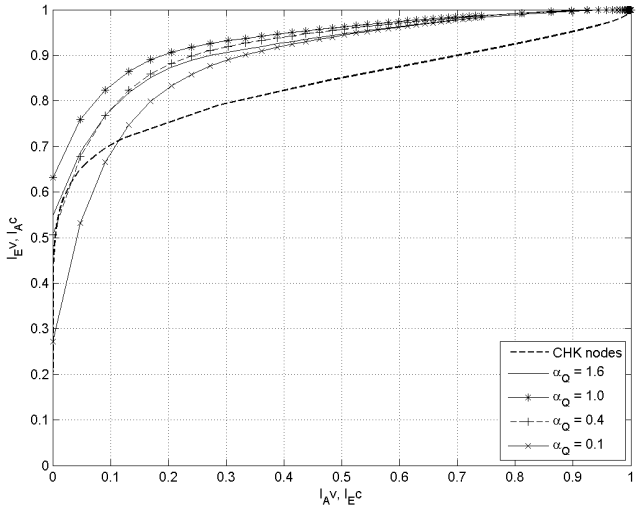
EXIT CHARTS

- An **Extrinsic information transfer chart**, commonly called **EXIT chart**, is a technique to aid the construction of good iteratively-decoded error-correcting codes (in particular LDPC and Turbo codes)
- An EXIT chart includes the response of the elements of decoder. The response can either be seen as extrinsic information or a representation of the messages in belief propagation

EXIT CHARTS



EXIT CHARTS



EXIT chart of the LDPC decoder considered for Rc=0.61 as a function of α_Q and for Q = 0.08

EXIT CHARTS

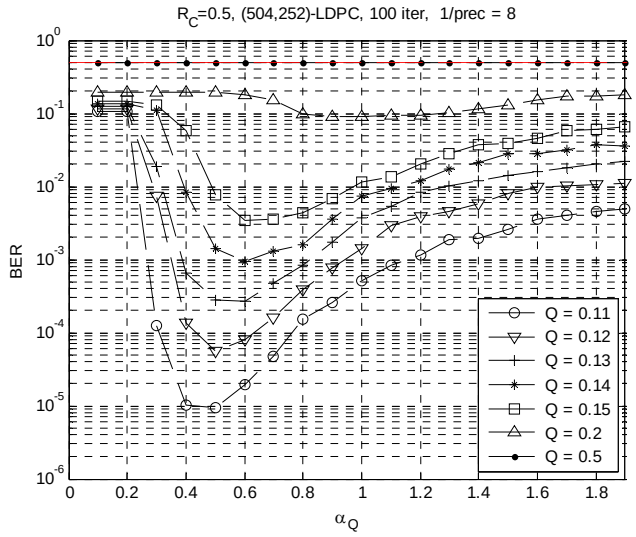
- The EXIT chart evaluated for the Rc = 0.61 LDPC decoder is depicted for Q = 0.08 and various values of α_Q
- The maximum opening of the decoding tunnel between the variable and check nodes decoding curves is achieved for $\alpha_Q = 1$. When the value of α_Q is too small (for instance 0.1) or too large (for instance 1.6) variable nodes curve intersects the check nodes curve and, consequently, the belief propagation decoder cannot converge to any codeword in the space of possible solutions

SIMULATIONS RESULTS

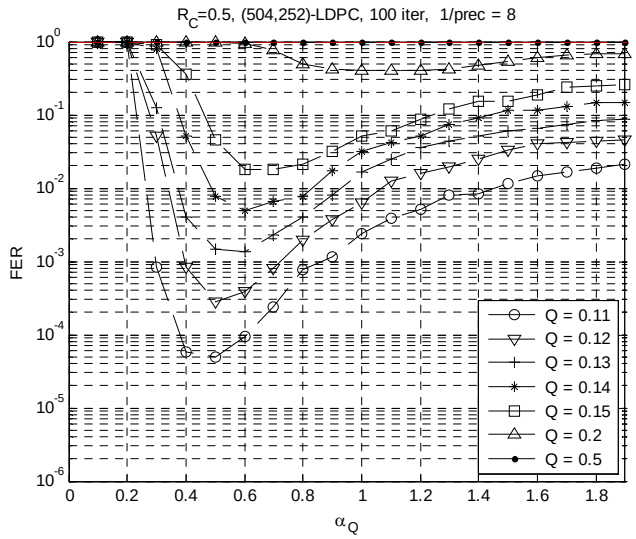
Considerations

- LDPC codes with various rates (0.5 and 0.61) and various block lengths have been simulated
- α_Q has been inserted in order to properly weigh the information derived from the q-bits, which is typically less reliable than the information derived from the public channel.
- Weighed q-metric values $\alpha_Q \cdot LLR(Y_{qk})$ have been considered as well as various values of the QBER parameter Q
- Public channel has been considered almost noiseless (η_S=20dB), and perfect estimate of the QBER value has been assumed (Q_{est}=Q)

Performance Evaluation: BER

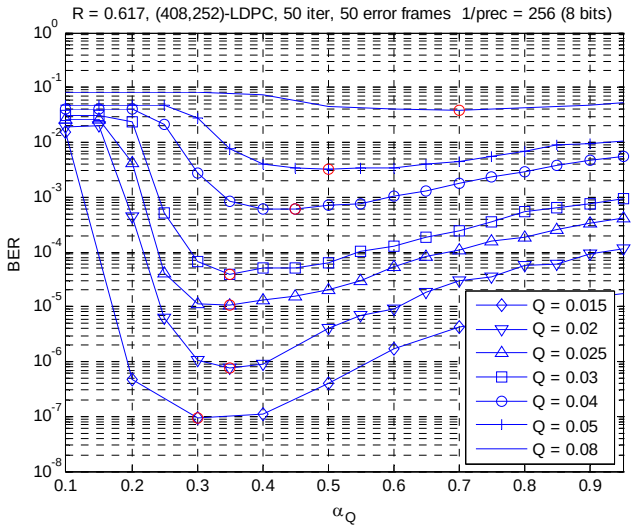


Performance Evaluation: FER



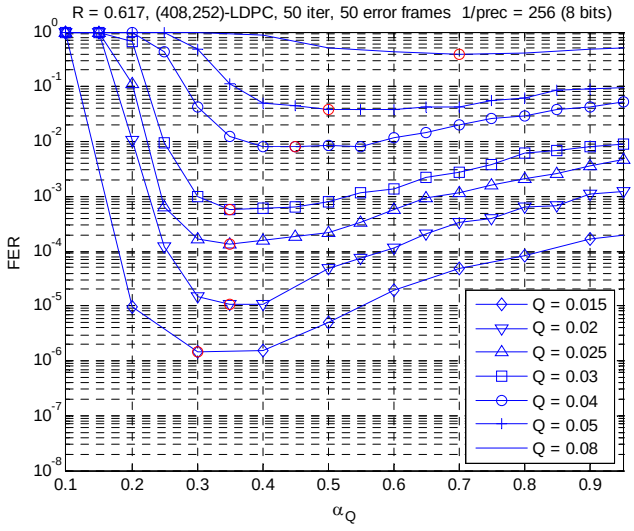
SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Performance Evaluation: BER



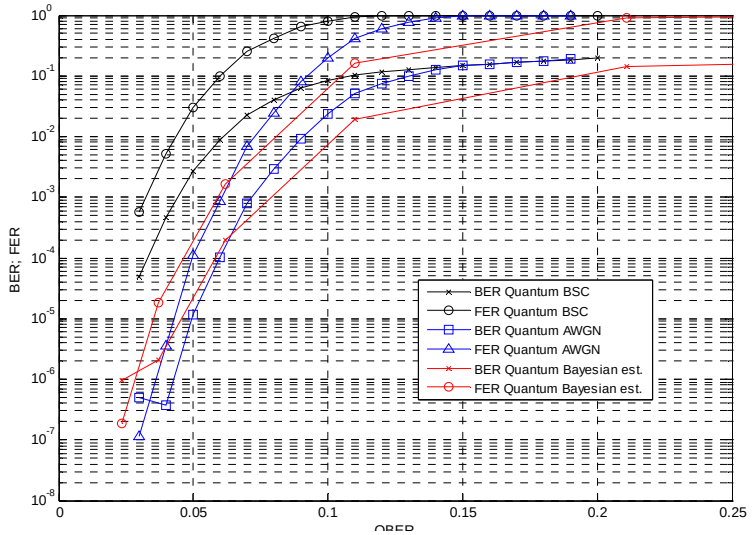
SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Performance Evaluation: FER



SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

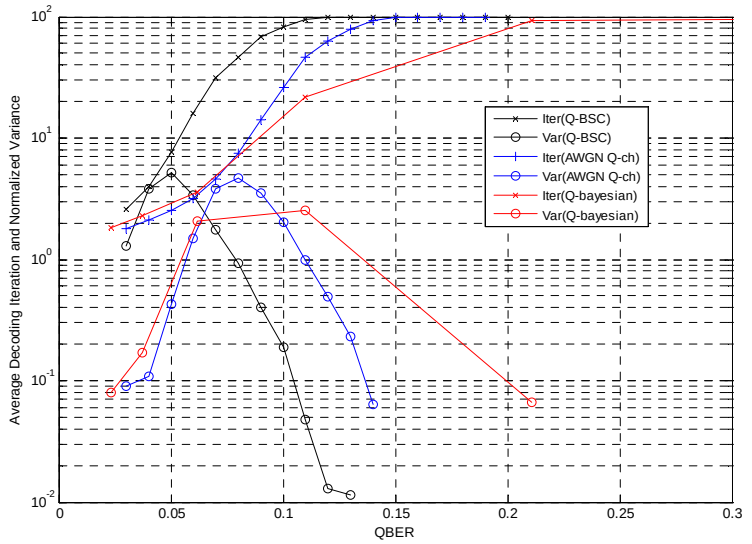
Performance Comparison: Q-Channel Models



BER and FER simulations Results for a LDPC code with rate $R_c = 0.61$

SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

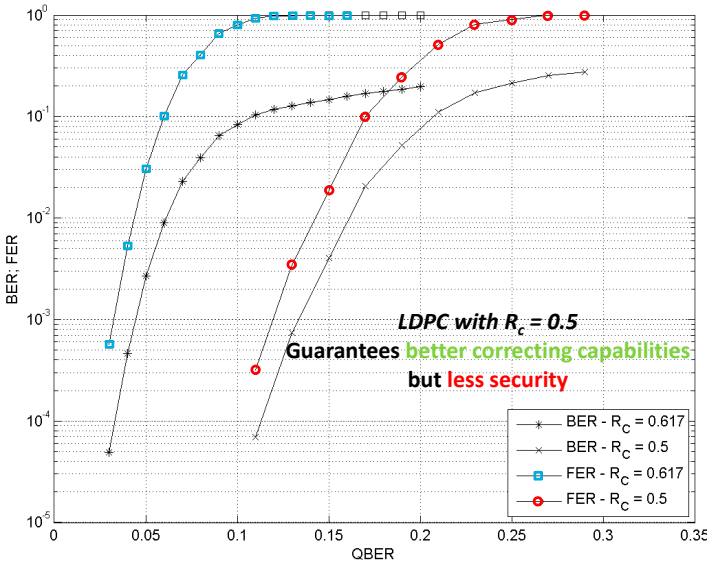
Performance Comparison: Q-Channel Models



Average decoding Iteration and Normalized Variance of the LDPC Decoder (Rc=0.61)

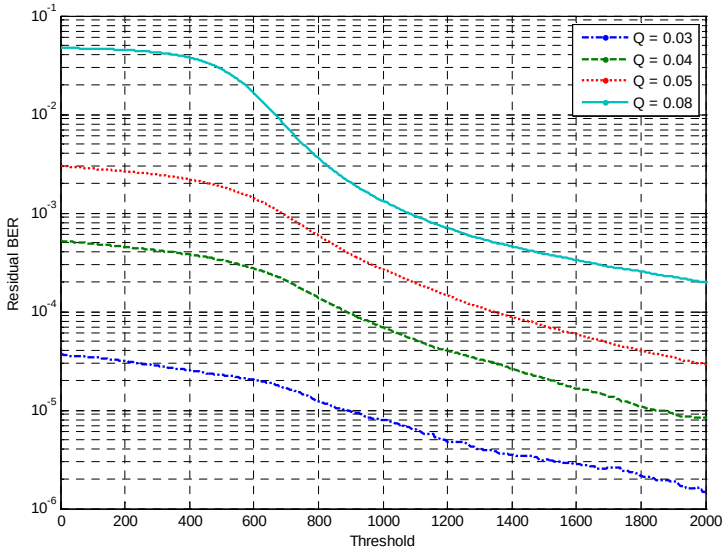
SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Overall Performance of the LDPC Decoders



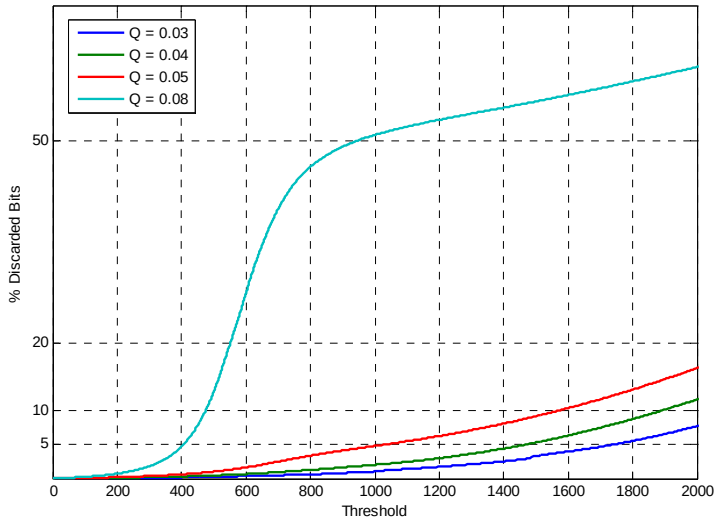
SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Overall Performance after Data Sifting



Residual BER after data sifting for different values of Q for the LDPC code with n = 408, r = 252 and Rc = 0.61, as a function of the considered sifting threshold

Overall Performance after Data Sifting



%Discarded Bits after data sifting for different values of Q for the LDPC code with n = 408, r = 252 and Rc = 0.61, as a function of the considered sifting threshold

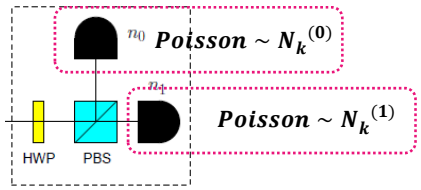
CAPACITY EVALUATION BIMO QUANTUM-DMC

SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Capacity Evaluation

$$C_{Shan}(\Psi) = \sup_{\varepsilon, \mathcal{M}} I(X,Y) \qquad I(X,Y) = H(X) - H(X|Y)$$

$(n_1 - n_0)$ Skellam Distribution



$$N_k^{(0)} + N_k^{(1)} = N_c$$

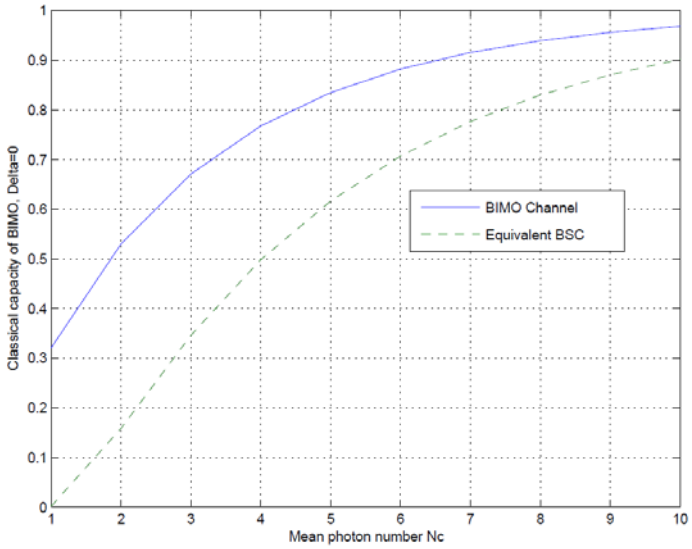
$$\frac{N_k^{(1)}}{N_k^{(0)}} = \frac{p(1|\varphi_k)}{p(0|\varphi_k)}$$

$$N_k^{(0)} N_k^{(1)} = N_c^2 p(0|\varphi_k) p(1|\varphi_k)$$

$$I(X,Y) = \sum_i p(\varphi_i) log \frac{1}{p(\varphi_i)} - \left\{ \begin{array}{c} \sum_m p(\varphi_0) p(m|\varphi_0) \frac{1}{log(p(m|\varphi_0)} + \\ \sum_m p(\varphi_1) p(m|\varphi_1) \frac{1}{log(p(m|\varphi_1)} \end{array} \right\}$$

SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Classical Capacity of BIMO Quantum-DMC



Classical Capacity of BIMO Quantum-DMC and equivalent BSC as a function of the mean photon count Nc

SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Some Considerations

- A **«composite channel»** has been identified. The model consists of a quantum channel and a classic channel in parallel, through which a secret key is securely exchanged between two parties
- The use of **mixed metrics** is suggested. These metrics are derived from the composite channel and combined in the LDPC decoder to perform a more efficient reconciliation of the exchange key, using "belief propagation" techniques
- The design and implementation of an algorithm for the stages of **information reconciliation and error correction** in QKD schemes, using channel coding along with "soft-processing" techniques and iterative decoding has been proposed
- An analysis on the convergence of the LDPC decoders as a function of the channel parameters, has been performed with the intention of suggesting a technique to detect the presence of a possible eavesdropper interfering the communication

SOFT PROCESSING TECNIQUES FOR QUANTUM KEY DISTRIBUTION APPLICATIONS

Some Considerations

- A multi-level quantum channel **« BIMO Quantum-DMC»** has been identified and the evaluation of its theoretical capacity bound has been calculated
- **BIMO Quantum-DMC** offers a **capacity improvement** over the equivalent BSC quantum channel (leading to a BER improvement when comparing the two channel in presence of an error correction code).
  From the results obtained via simulation it is evident that there is a **significant reduction** in the values of the **B**
  ER and FER for several QBER values; meaning that a significant larger portion of the data after the stages of sifting and reconciliation can be kept
- The proposed protocol, having a **negligible cost**, can reduce the residual FER in QKD systems, largely **reducing the interaction** required between the two parties involved, **increasing the key rate** and protecting the secrecy of the information exchanged