Universidade de Aveiro
2017-2018

CV-QKD System

Daniel Pereira
(danielfpereira@ua.pt)

Department of Electronics, Telecommunications and Informatics,
University of Aveiro, Aveiro, Portugal
Instituto de Telecomunicações, Aveiro, Portugal

INSTITUIÇÕES ASSOCIADAS:

instituto de telecomunicações

creating and sharing knowledge for telecommunications

Introduction - Objectives

- Study pilot-aided, locally generated Local Oscillator Continuous Variables Quantum Key Distribution (CV-QKD) with 4 state discrete modulation.
- Both simulation and experimental results where obtained.
- Results where linked to theoretical expected values, not each other (missing detector information to compare simulation to experimental values).

Theoretical notes - Security of CV-QKD

In CV-QKD, the key for a One Time Pad (OTP) protocol is shared through a quantum channel. The security of this key is evaluated in terms of secret key generation rate (bits/symbol):

$$K = \beta I(A:B) - S(B:E). \tag{1}$$

The rate is positive if Alice and Bob manage to share more information, $I(A:B)$, than the information obtained by Eve on Bob's results, $S(B:E)$. β represents the efficiency of the employed error correction.

Theoretical notes - Estimating information rates

The quantum information Eve possesses, $S(B:E)$, is upper bounded by the quantum information between Alice and Bob, $S(B:A)$, which can be estimated by knowledge of the covariance matrices.

$$\gamma_{AB} = \begin{bmatrix} (1+2\langle n\rangle)\mathbb{I}_2 & \sqrt{\frac{T}{2}}Z\sigma_Z \\ \sqrt{\frac{T}{2}}Z\sigma_Z & \left(T\langle n\rangle + 1 + \frac{T}{2}\varepsilon\right)\mathbb{I}_2 \end{bmatrix} \tag{2}$$

$$\gamma_{AB|B} = \left((1+2\langle n\rangle) - \frac{\frac{T}{2}Z^2}{T\langle n\rangle + 2 + \frac{T}{2}\varepsilon}\right)\mathbb{I}_2 \tag{3}$$

The quantum information can then be calculated from the symplectic eigenvalues of the two previous covariance matrices.

Theoretical notes - Security of practical CV-QKD

Taking into account the need to estimate the channel parameters, the covariance matrices are altered to:

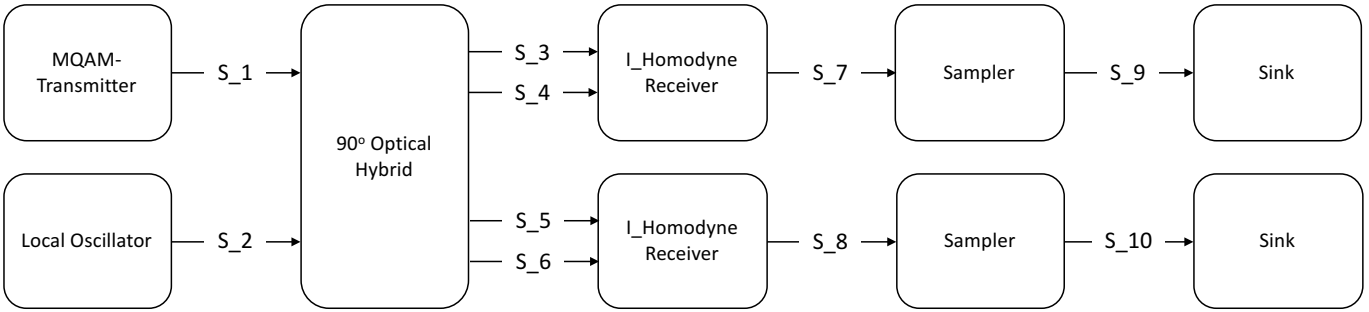
$$\gamma_{\varepsilon} = \begin{bmatrix} (1+2\langle n \rangle)\mathbb{I}_2 & t_{\min} Z \sigma_z \\ t_{\min} Z \sigma_z & \left(2t_{\min}^2 \langle n \rangle + \sigma_{\max}^2\right)\mathbb{I}_2 \end{bmatrix}, \tag{4}$$

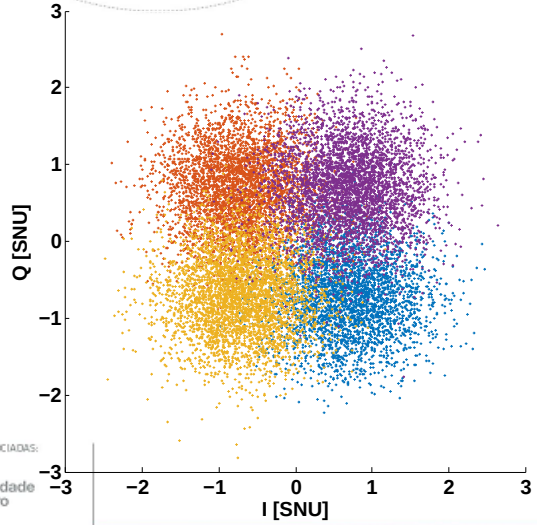
$$\gamma_{AB|B_{\varepsilon}} = \left(1 + 2\langle n \rangle - \frac{t_{\min}^2 Z^2}{2t_{\min}^2 \langle n \rangle + 1 + \sigma_{\max}^2}\right)\mathbb{I}_2. \tag{5}$$

$t_{\min}$ is the minimum value of $t = \sqrt{\frac{T}{2}}$ except with a probability of $\Delta/2$.
$\sigma_{\max}^2$ is the maximum value of $\sigma^2 = 1 + \frac{T}{2}\varepsilon$ except with a probability of $\Delta/2$.

This is dubbed the **finite size analysis**.

Simulation - Block diagram



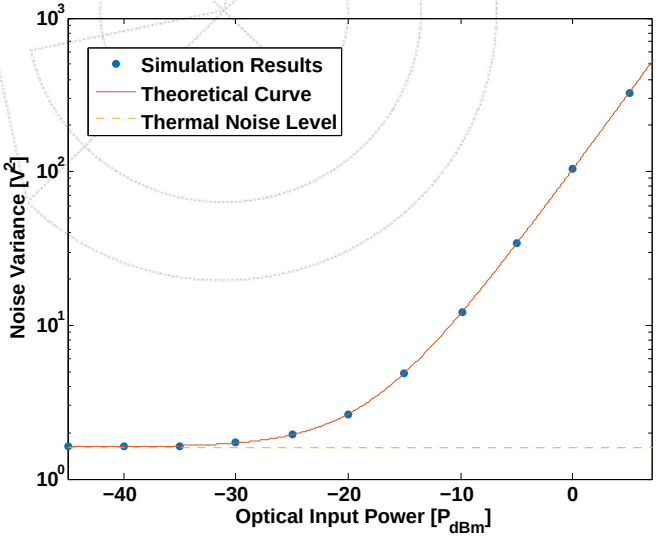


Two independent noise sources are considered:

- Thermal noise.
- Shot noise.

Simulation - Detector noise characterization

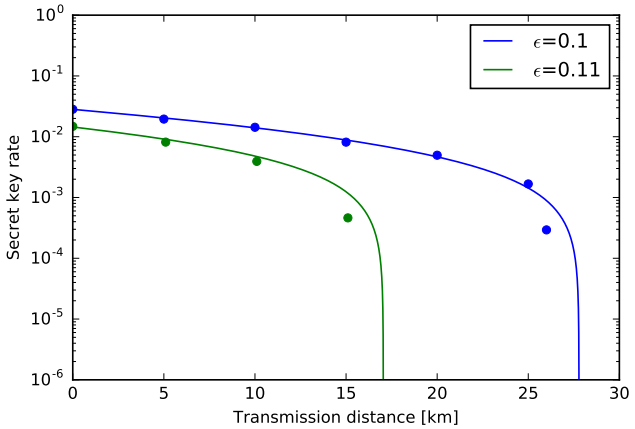
The first results presented here pertain to a noise variance characterization of the simulated homodyne receiver:



The simulation results closely follow the theoretical expectation values for all the studied power levels. The linear dominated stage of the detector is seen to start at a Local Oscillator optical input power of -15 dBm.

Simulation - Secret key generation rate

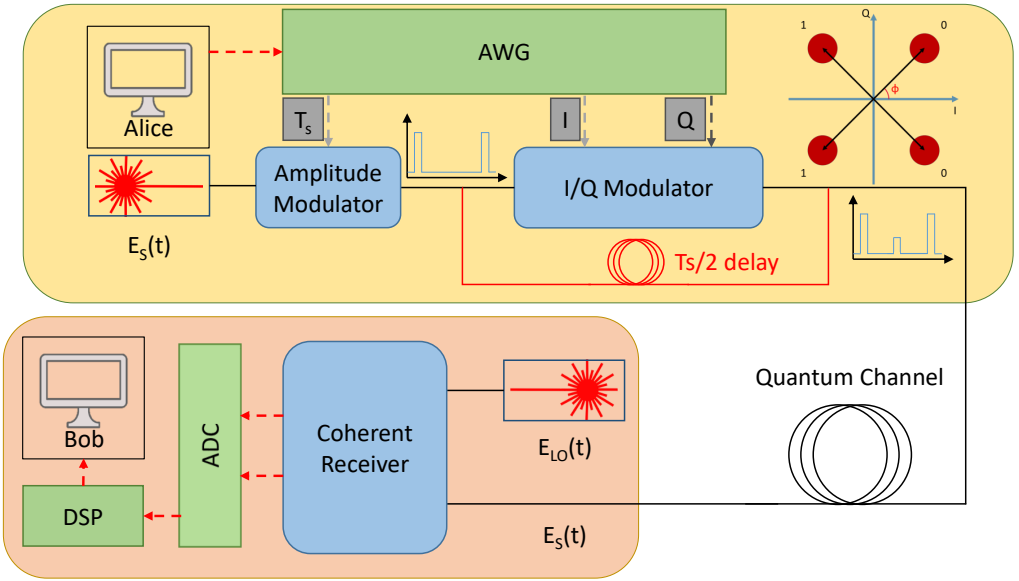
Following the noise characterization, the secret key generation rate of the simulation was evaluated and compared to the theoretical expectation values:



The simulation results closely follow the theoretical curve just until when the curve starts to quickly tend to 0, at which point they diverge.

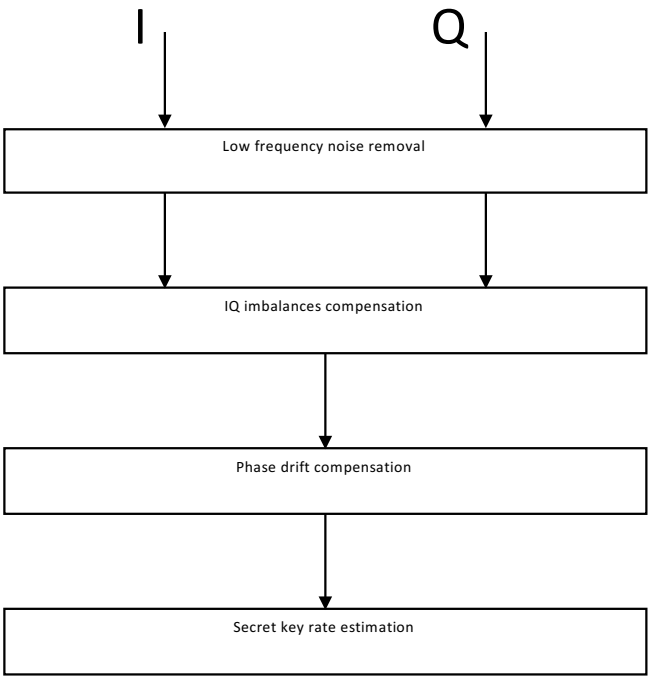
Theoretical (full line) and simulation (dots) results for secret key generation, reconciliation efficiency set at β=80% and transmission given by $T = 10^{-0.02d}$ (d is the transmission distance in kilometres).

Experimental results - Experimental system



Experimental results - Output data processing

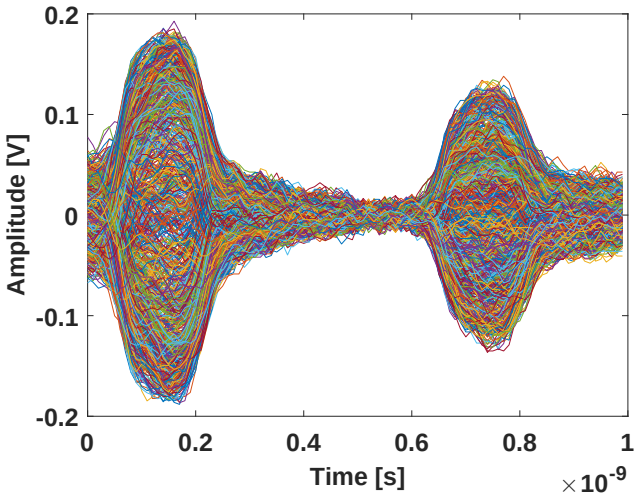
The following digital signal processing was employed:

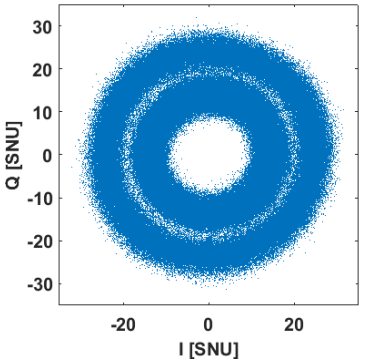


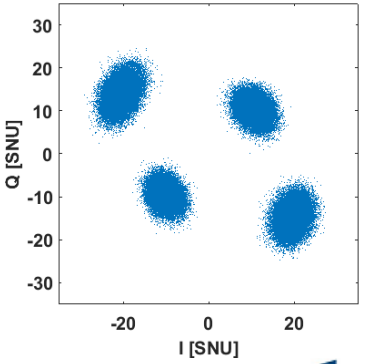
- The IQ imbalances are removed by applying a Gram-Schmidt orthogonalization process.
- The phase drift is compensated by measuring the relative phase between the two lasers and removing that value from the decoded results.
- The secret key rate is estimated through the finite size analysis method presented above.

Experimental results - Phase drift compensation

The phase drift compensation scheme was tested.

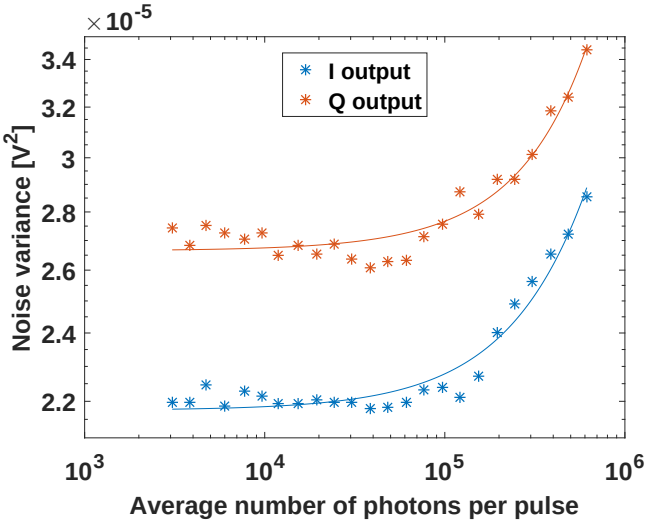






Experimental results - Detector noise characterization

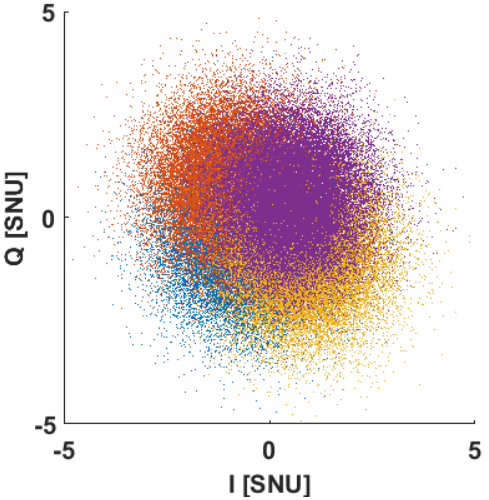
A shot noise characterization of the detector was performed



- The linear was stage was found to be below $\langle n \rangle \sim 4 \times 10^6$.
- Our detector has a very short linear stage, not ideal for this application.
- Shot Noise Units (SNU) conversion factor was obtained.

Experimental results - System performance

The system's performance was evaluated for 4 different setups, utilizing a single/double laser setup coupled with either a direct connection or a 10 km transmission channel. The secret key rate was estimated through the finite size analysis presented before.

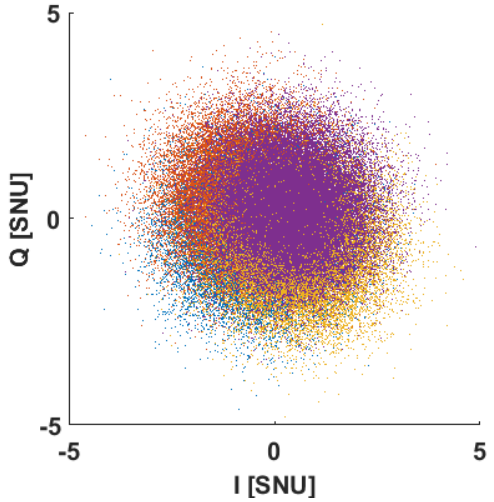


Single laser, BTB recovered constellation

ε[SNU]	0.074	
	Theo	**Exp**
T	Efficiency	0.9519
$K\left[\frac{\text{bits}}{\text{symb}}\right]$	0.0288	0.0213

Experimental results - System performance

The system's performance was evaluated for 4 different setups, utilizing a single/double laser setup coupled with either a direct connection or a 10 km transmission channel. The secret key rate was estimated through the finite size analysis presented before.

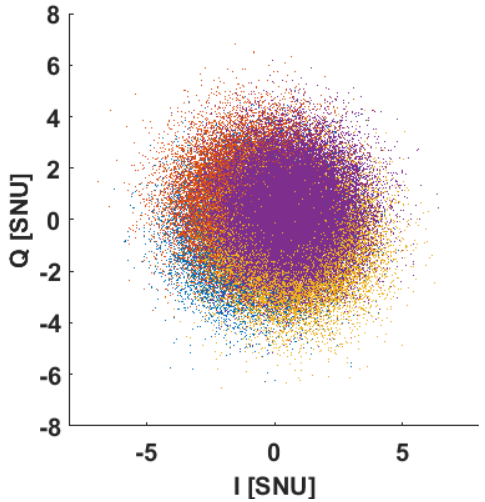


Single laser, 10 km recovered constellation

ε[SNU]	0.0156	
	Theo	**Exp**
T	0.4547	0.4317
$K\left[\frac{\text{bits}}{\text{symb}}\right]$	0.0132	0.0094

Experimental results - System performance

The system's performance was evaluated for 4 different setups, utilizing a single/double laser setup coupled with either a direct connection or a 10 km transmission channel. The secret key rate was estimated through the finite size analysis presented before.

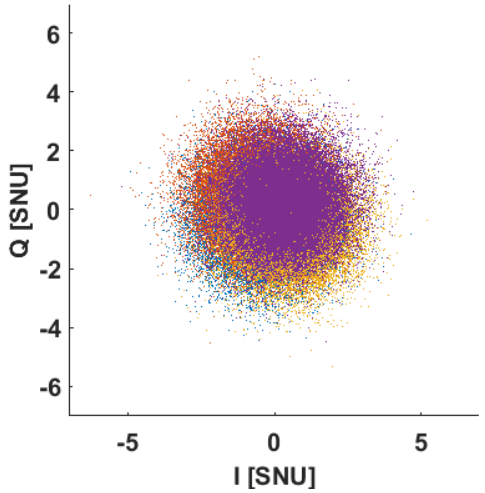


Double laser, BTB recovered constellation

ε[SNU]	2.9915	
	Theo	**Exp**
T	$\sim$0.95	0.9557
$K\left[\frac{\text{bits}}{\text{symb}}\right]$	Negative	-0.8011

Experimental results - System performance

The system's performance was evaluated for 4 different setups, utilizing a single/double laser setup coupled with either a direct connection or a 10 km transmission channel. The secret key rate was estimated through the finite size analysis presented before.



double laser, 10 km recovered constellation

ε[SNU]	2.8196	
	Theo	**Exp**
T	0.4547	0.4282
$K\left[\frac{\text{bits}}{\text{symb}}\right]$	Negative	-0.4769