Universidade de Aveiro
2017-2018

Continuous Variables 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 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).

Introduction - Content in this presentation

- Simulation results:
  - Noise characterization.
  - Secret key generation rate in function of transmission for two levels of excess noise.
- Experimental results:
  - Phase drift compensation.
  - Noise characterization experiment.
  - Key distribution experiment with secret key generation rate estimation.

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 mutual classical information is estimated as:

$$I(A:B) = \log_2\left(1 + \frac{T\langle n\rangle}{1+\frac{T}{2}\varepsilon}\right). \tag{2}$$

This definition of $I(A:B)$ assumes a Gaussian modulated signal, while we use discrete modulation. The effect of this inaccuracy on the mutual information is included in the error correction efficiency β.

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.

$$\gamma_{\mathrm{AB}} = \begin{bmatrix} (1+2\langle n\rangle)\mathbb{I}_2 & \sqrt{\frac{T}{2}}Z\boldsymbol{\sigma}_Z \\ \sqrt{\frac{T}{2}}Z\boldsymbol{\sigma}_Z & \left(T\langle n\rangle+1+\frac{T}{2}\varepsilon\right)\mathbb{I}_2 \end{bmatrix} \tag{3}$$

The effect of the measurement on Alice's mode for the case of double-homodyne detection can be expressed as follows.

$$\gamma_{AB|B} = \left[(1+2\langle n\rangle) - \frac{\frac{T}{2}Z^2}{T\langle n\rangle+2+\frac{T}{2}\varepsilon}\right]\mathbb{I}_2 \tag{4}$$

Theoretical notes - Estimating information rates

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

$$
\begin{aligned}
S(B:E) = \sum_{k=1}^{2} \left[(\bar{n}_k^{AB}+1)\log_2(\bar{n}_k^{AB}+1) - \bar{n}_k^{AB}\log_2 \bar{n}_k^{AB} \right] \\
- (\bar{n}^{AB|B}+1)\log_2(\bar{n}^{AB|B}+1) - \bar{n}^{AB|B}\log_2 \bar{n}^{AB|B},
\end{aligned} \tag{5}
$$

where $\bar{n} = (\mu - 1)/2$, with μ representing the symplectic eigenvalues.

Theoretical notes - Security of practical CV-QKD

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

$$\gamma_\varepsilon = \begin{bmatrix} (1+2\langle n\rangle)\mathbb{I}_2 & t_{\mathrm{min}} Z \sigma_z \\ t_{\mathrm{min}} Z \sigma_z & \left(2t_{\mathrm{min}}^2 \langle n\rangle + \sigma_{\mathrm{max}}^2\right)\mathbb{I}_2 \end{bmatrix}, \tag{6}$$

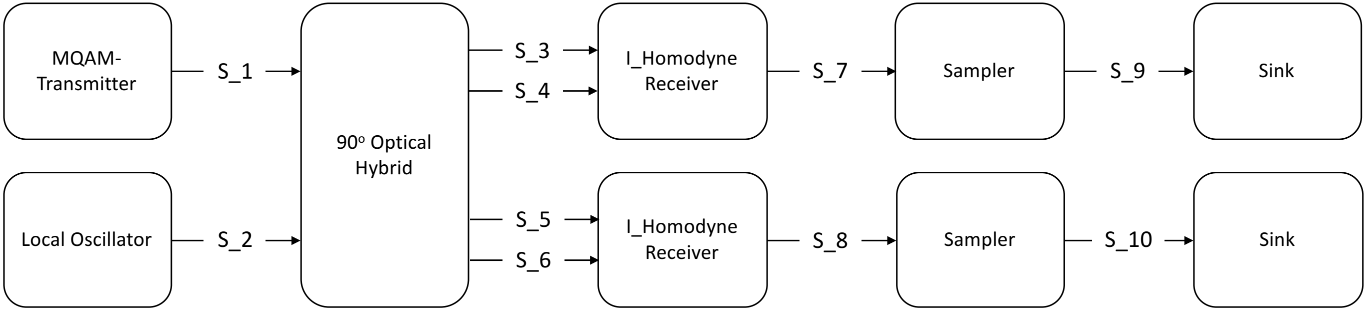
and:

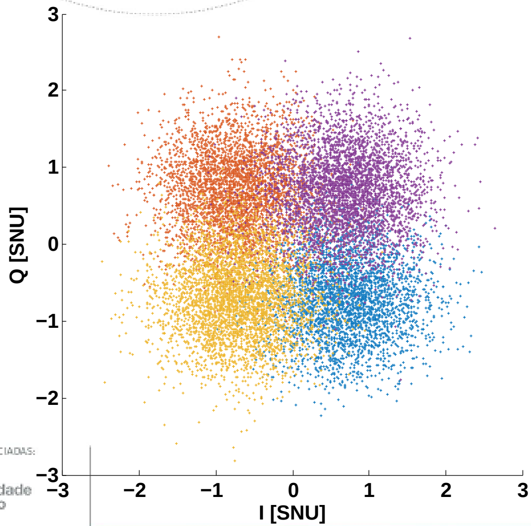
$$\gamma_{AB|B_\varepsilon} = \left(1+2\langle n\rangle - \frac{t_{\mathrm{min}}^2 Z^2}{2t_{\mathrm{min}}^2 \langle n\rangle + 1 + \sigma_{\mathrm{max}}^2}\right)\mathbb{I}_2. \tag{7}$$

t_{min} is the minimum value of $t = \sqrt{\frac{T}{2}}$ except with a probability of $\Delta/2$.

σ_{max}^2 is the maximum value of $\sigma^2 = 1 + \frac{T}{2}\varepsilon$ except with a probability of $\Delta/2$.

Simulation - Block diagram



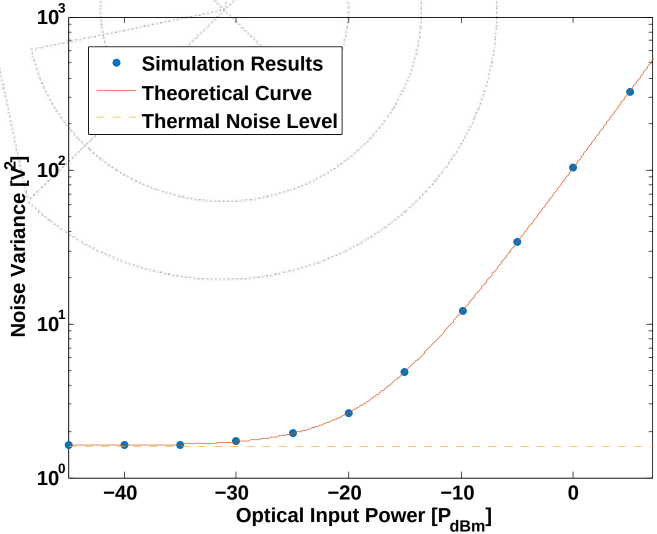


Two independent noise sources are considered:

- Thermal noise.
- Shot noise.

Simulation - Detector noise characterization

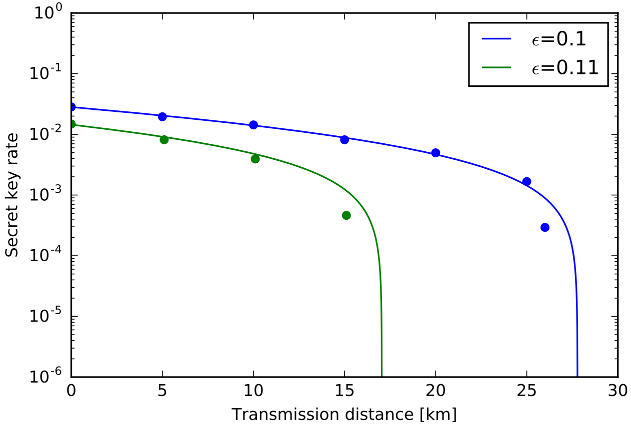
The first results presented here pertain to a noise variance characterization of the simulated homodyne receiver:



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

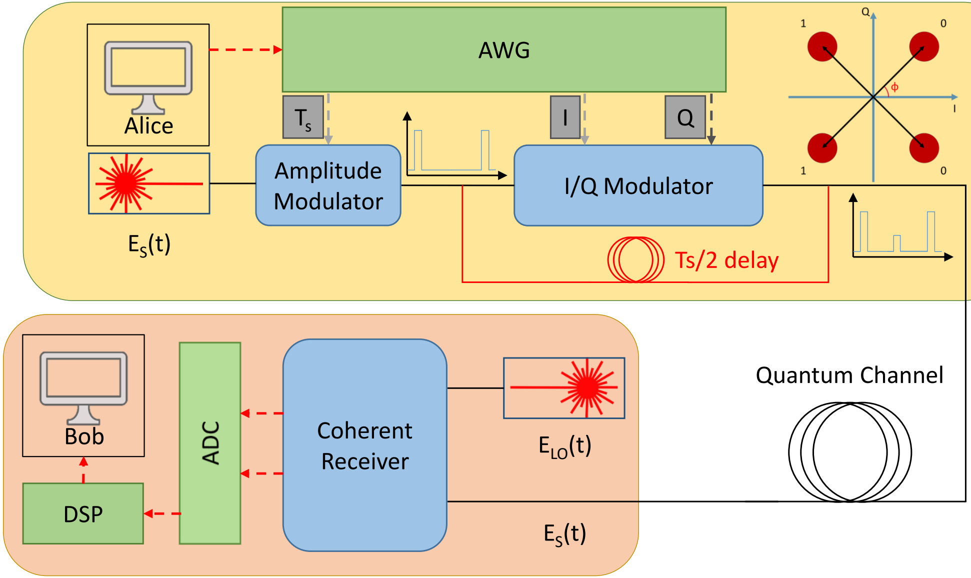
Simulation - Secret key generation rate

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



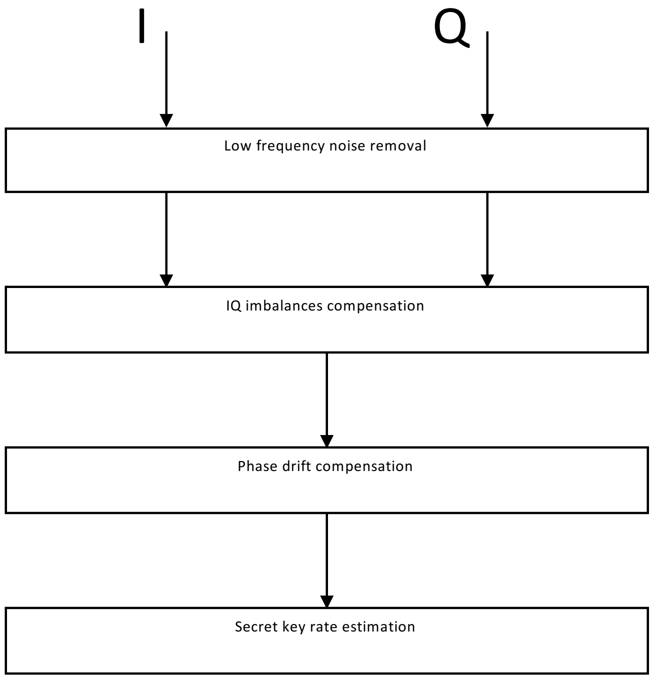
The simulation results closely follow the theoretical curve just until when the curve starts to quickly tend to 0, at which point they diverge.

Experimental results - Experimental system



Experimental results - Output data processing

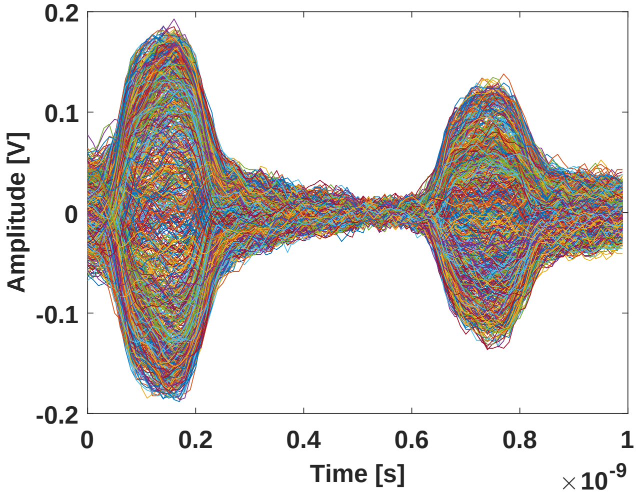
The following digital signal processing was employed:

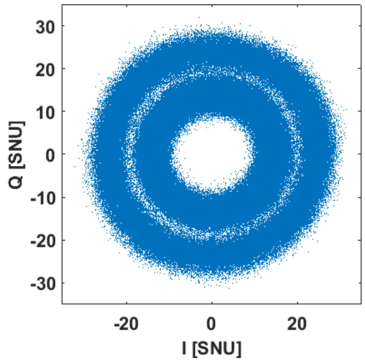


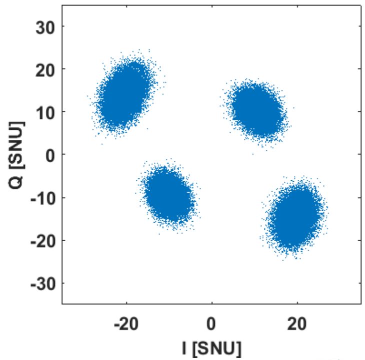
- The IQ imbalances are removed by applying a Gram-Schmidt orthogonalization process.
- The phase drift is compensated by measuring the relative phase between the two lasers and removing that value from the decoded results.
- The secret key rate is estimated through the finite size analysis method presented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

Experimental results - Phase drift compensation

The phase drift compensation scheme was tested.

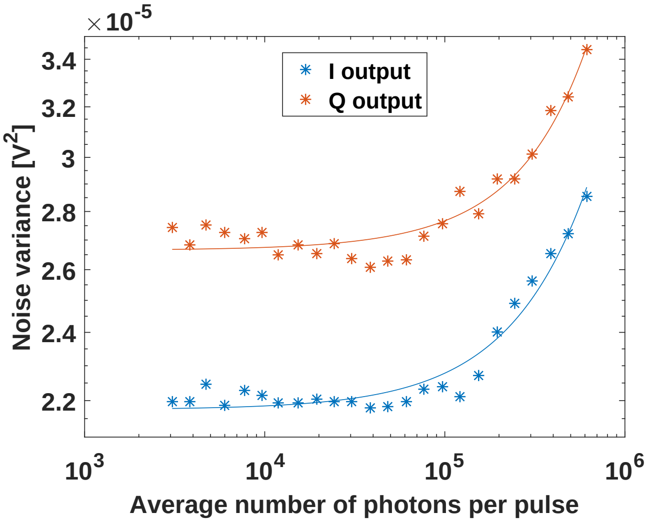






Experimental results - Detector noise characterization

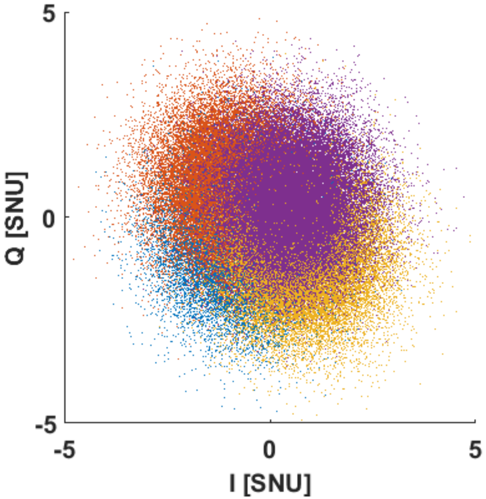
A shot noise characterization of the detector was performed



- 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.

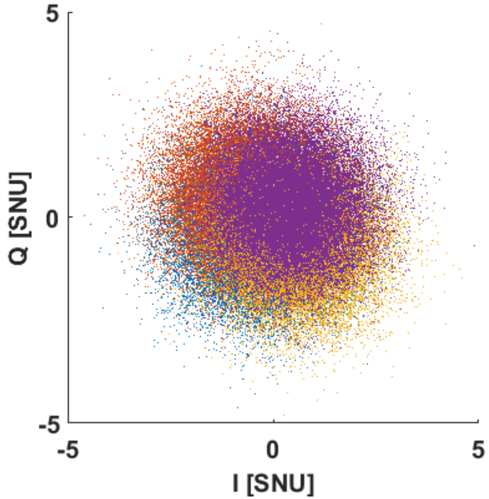


Single laser, BTB recovered constellation

ε	0.074	
	Theoretical	**Experimental**
T	Efficiency	0.9519
K	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.

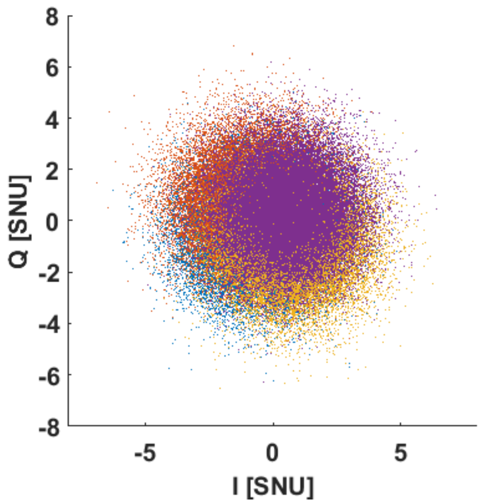


Single laser, 10 km recovered constellation

ε	0.0156	
	Theoretical	**Experimental**
T	0.4547	0.4317
K	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.

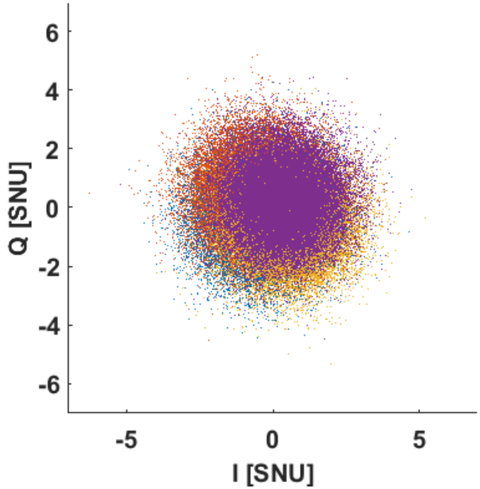


Double laser, BTB recovered constellation

ε	2.9915	
	Theoretical	**Experimental**
T	$\sim$0.95	0.9557
K	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	2.8196	
	Theoretical	**Experimental**
T	0.4547	0.4282
K	Negative	-0.4769