Safety study

1 Introduction

This document describes a model to simulate the results presented in [1]. In this article, the security of Continuous Variable Quantum Key Distribution (CV-QKD) is studied theoretically, stemming from the effects of an eavesdropper on the detected BER. Both direct and adapted to double homodyne detection results are presented.

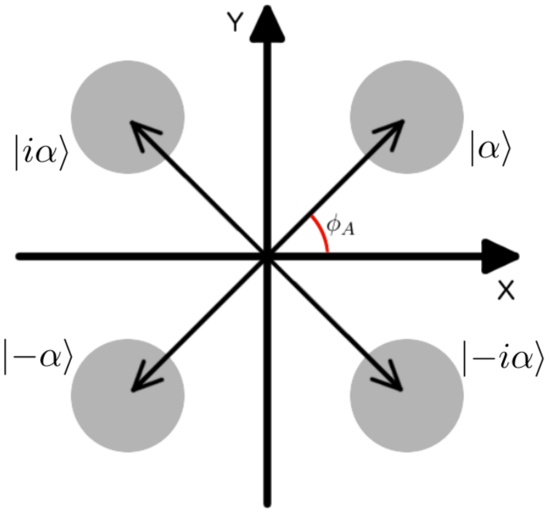


Figure 1: State constellation for CV-QKD

The state constellation used in the CV-QKD protocol is presented in Figure 1. The emitter (usually named Alice) is going to send one of the four states $|\alpha\rangle$, $|-\alpha\rangle$, $|-i\alpha\rangle$, and $|i\alpha\rangle$, with equal probability. Alice is going to use two basis, the 45 base and the -45 base. In the 45 base, she can send one of two values, 1 and -1, which correspond to the states $|\alpha\rangle$ and $|-\alpha\rangle$. In the -45 base, she can send also one of two values, 1 and -1, which correspond to the states $|-i\alpha\rangle$ and $|i\alpha\rangle$.

Because we don't know *à* prior which state is going be transmitted, neither which basis is going to be used, and to incorporate our "ignorance" in the system description, we can work with the density operator. The density operator is a proper tool to describe "statistical mixtures". A "statistical mixtures" is one state, from a possible set, but we don't know which state it is. There is no coherence superposition, in which a state is a superposition of two states and it is both states at the same time.

Since all states have the same probability of occurring, the state density operator is given by:

$$\hat{\rho} = \frac{1}{4}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha| + |i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|\right). \tag{1}$$

Note that the density operator is equivalent to the wave function in terms of the system description.

From the receiver perspective, i.e. from the Bob perspective, and after knowing the base used by Alice. The density operator can be reduce to, where 1 corresponds to the 45 base and -1 corresponds to -45.

$$\hat{\rho}_1 = \frac{1}{2}\left(\left|\alpha\right\rangle\left\langle\alpha\right| + \left|-\alpha\right\rangle\left\langle-\alpha\right|\right), \tag{2}$$

$$\hat{\rho}_2 = \frac{1}{2}\left(\left|i\alpha\right\rangle\left\langle i\alpha\right| + \left|-i\alpha\right\rangle\left\langle-i\alpha\right|\right). \tag{3}$$

1.1 Single Homodyne setup

The probability of obtaining a quadrature $\hat{X}_\phi = \hat{X}_1\cos\phi + \hat{X}_2\sin\phi$ when measuring the coherent state $|\alpha\rangle$ is given by the following gaussian distribution:

$$|\langle X_\phi|\alpha\rangle|^2 = \sqrt{\frac{2}{\pi}}e^{-2(X_\phi - \alpha\cos\phi)^2}, \tag{4}$$

We can define the "correct" and "wrong" basis measurement probability density, respectively, as:

$$\left\langle X_i\right|\hat{\rho}_j\left|X_i\right\rangle = \begin{cases} \frac{1}{\sqrt{2\pi}}\left(e^{-2(X_i-\alpha)^2} + e^{-2(X_i+\alpha)}\right), & i = j \\ \sqrt{\frac{2}{\pi}}e^{-2X_i^2}, & i \neq j \end{cases}. \tag{5}$$

The post selection efficiency (PSE) can be defined as the probability of a measurement in the correct basis yields a result that satisfies the limit value X_0:

$$\begin{aligned} P(X_0,\alpha) &= \int_{-\infty}^{-X_0}\left\langle X_1\right|\hat{\rho}_1\left|X_1\right\rangle dX_1 + \int_{X_0}^{\infty}\left\langle X_1\right|\hat{\rho}_1\left|X_1\right\rangle dX_1 \\ &= \frac{1}{2}\left[\mathrm{erfc}(\sqrt{2}(X_0+\alpha)) + \mathrm{erfc}(\sqrt{2}(X_0-\alpha))\right]. \end{aligned} \tag{6}$$

The bit error rate (BER) is the normalized probability of, after choosing the correct basis, obtaining the wrong bit value:

$$Q(X_0,\alpha) = \frac{1}{P(X_0,\alpha)}\int_{-\infty}^{-X_0}|\langle X_i|\alpha\rangle|\,dX_i = \frac{\mathrm{erfc}\left(\sqrt{2}(X_0+\alpha)\right)}{2P(X_0,n)} \tag{7}$$

1.2 Double Homodyne setup

In our proposed double homodyne protocol both quadratures are measured simultaneously, as such the concept of correct and wrong basis measurements has no value. Our protocol also makes use of a locally generated Local Oscillator (LO), obtained from a different laser than the one used to generate the signal, thus we have to take into account the phase drift between both lasers. High intensity reference pulses are sent periodically to allow for an estimation of the phase drift. The double homodyne setup requires the signal to be divided into the two utilized detectors, so each measurement is made on a coherent state with half the amplitude of the incoming signal $\alpha \rightarrow \frac{\alpha}{\sqrt{2}}$

For each incoming pulse we measure quadratures X_ϕ and Y_ϕ. ϕ has contributions from both the encoded angle, θ, and the phase difference between lasers, ϵ, we assume $\phi = \theta + \epsilon$. On the reference pulses no phase is encoded, that is $\theta = 0$, thus ϵ can be estimated. Assuming ϵ doesn't change between a reference pulse and the following signal pulse, the measured quadratures can be cast into the originally sent quadratures X_θ and Y_θ via:

$$\begin{aligned} X_\theta &= X_\phi\cos\epsilon - Y_\phi\sin\epsilon \\ Y_\theta &= X_\phi\sin\epsilon + Y_\phi\sin\epsilon \end{aligned} \tag{8}$$

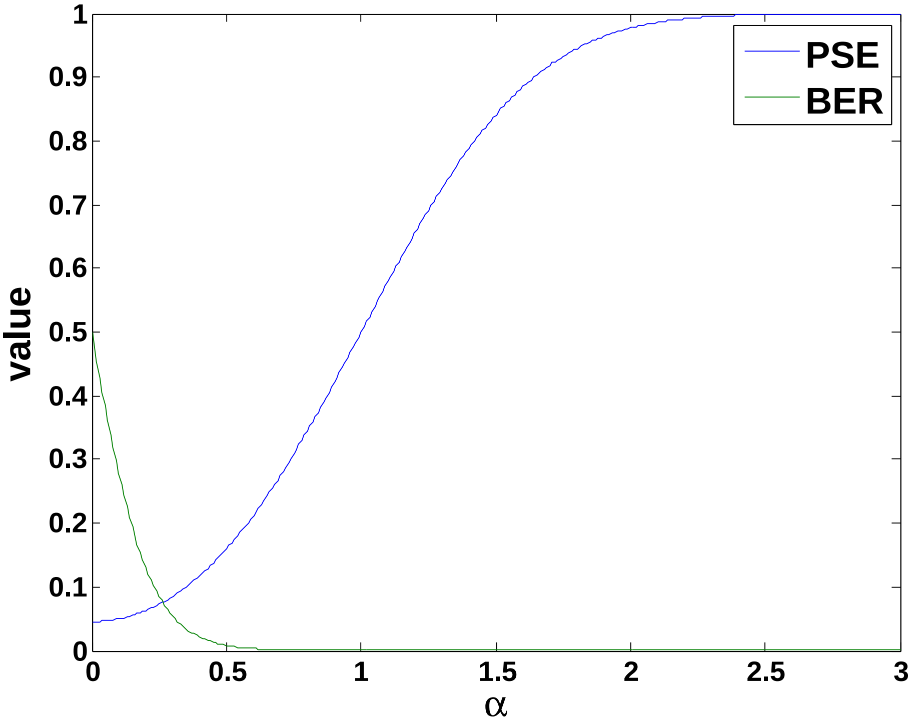


Figure 2: BER and PSE in function of α for the single homodyne setup. $X_0 = 1$ was used

Assuming an announcement of the coding basis, the density operators (2) and (3) still apply. We can now define the probability density of obtaining results X_θ and Y_θ, assuming a state in the X_1 base was sent, as:

$$\langle X_\theta|\hat{\rho}_1|X_\theta\rangle = \frac{\sqrt{\frac{2}{\pi}}}{4}\left(e^{-2\left(x_\theta - \frac{\alpha}{\sqrt{2}}\cos\theta\right)^2} + e^{-2\left(x_\theta + \frac{\alpha}{\sqrt{2}}\cos\theta\right)^2}\right), \tag{9}$$

$$\langle Y_\theta|\hat{\rho}_1|Y_\theta\rangle = \frac{\sqrt{\frac{2}{\pi}}}{4}\left(e^{-2\left(y_\theta - \frac{\alpha}{\sqrt{2}}\sin\theta\right)^2} + e^{-2\left(y_\theta + \frac{\alpha}{\sqrt{2}}\sin\theta\right)^2}\right). \tag{10}$$

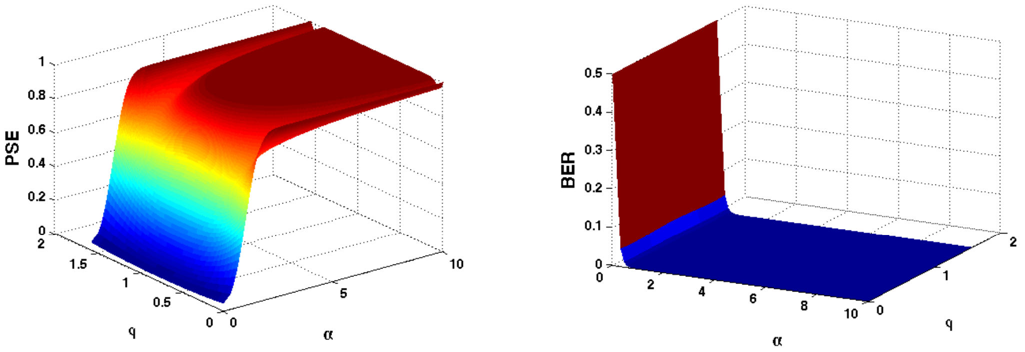
Now each state needs to satisfy two limit values, X_0 and Y_0, to be accepted. Thus, the PSE is now defined as:

$$\begin{aligned} P_{DH}(X_0, Y_0, \alpha) = &\int_{-\infty}^{-X_0} \langle X_\theta|\hat{\rho}_1|X_\theta\rangle\, dx_\theta \int_{-\infty}^{-Y_0} \langle Y_\theta|\hat{\rho}_1|Y_\theta\rangle\, dy_\theta + \\ &\int_{X_0}^{\infty} \langle X_\theta|\hat{\rho}_1|X_\theta\rangle\, dx_\theta \int_{Y_0}^{\infty} \langle Y_\theta|\hat{\rho}_1|Y_\theta\rangle\, dy_\theta \\ &= \frac{1}{4}\left\{\operatorname{erfc}\left[\sqrt{2}\left(X_0 - \frac{\alpha}{\sqrt{2}}\cos\theta\right)\right] + \operatorname{erfc}\left[\sqrt{2}\left(X_0 + \frac{\alpha}{\sqrt{2}}\cos\theta\right)\right]\right\} \\ &\left\{\operatorname{erfc}\left[\sqrt{2}\left(Y_0 - \frac{\alpha}{\sqrt{2}}\sin\theta\right)\right] + \operatorname{erfc}\left[\sqrt{2}\left(Y_0 + \frac{\alpha}{\sqrt{2}}\sin\theta\right)\right]\right\}, \end{aligned} \tag{11}$$

The DH subscript denotes Double Homodyne. In a somewhat similar manner, the BER is now defined as:

$$\begin{aligned} Q_{DH}(X_0, Y_0, \alpha) = \frac{1}{P_{DH}} \Bigg(\int_{-\infty}^{-X_0} \left| \langle X_\theta | \frac{\alpha}{\sqrt{2}} \rangle \right|^2 dx_\theta \int_{-\infty}^{-Y_0} \left| \langle Y_\theta | \frac{\alpha}{\sqrt{2}} \rangle \right|^2 dy_\theta + \\ \int_{X_0}^{\infty} \left| \langle X_\theta | -\frac{\alpha}{\sqrt{2}} \rangle \right|^2 dx_\theta \int_{Y_0}^{\infty} \left| \langle Y_\theta | -\frac{\alpha}{\sqrt{2}} \rangle \right|^2 dy_\theta \Bigg) \\ = \frac{1}{2P_{DH}} \mathrm{erfc} \left[\sqrt{2} \left(X_0 + \frac{\alpha}{\sqrt{2}} \cos\theta \right) \right] \mathrm{erfc} \left[\sqrt{2} \left(Y_0 + \frac{\alpha}{\sqrt{2}} sin\theta \right) \right], \end{aligned} \tag{12}$$

note that, in this definition for BER, only values $\theta \in \left[0, \frac{\pi}{2}\right]$ make sense (the sent state was α).



(a) PSE in function of α and θ for the double homodyne setup. $X_0 = 1$ was used

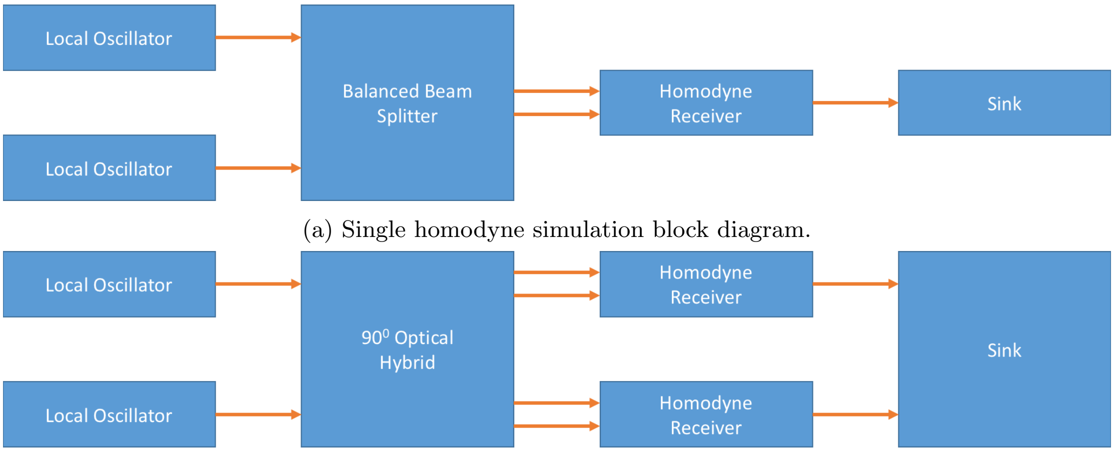
(b) BER in function of α and θ for the double homodyne setup. $X_0 = 1$ was used

Figure 3: Theoretical results for double homodyne setup.

2 Functional Description

Simplified diagrams of the systems being simulated are presented in Figures 4a. and 4b. Two optical signals are generated, one with a constant power level of 10 dBm and the other with power in multiples of the power corresponding to a single photon per sampling time (6.4078e$\times 10^{-13}$ W for a sampling time of 200 ns). The two signals are mixed, with a Balanced Beam Splitter in the single homodyne case and with a 90° Optical Hybrid in the double homodyne one, and are subsequently evaluated with recourse to Homodyne Receivers.

System Blocks	netxpto Blocks
Local Oscillator	LocalOscillator
Homodyne Receiver	I_HomodyneReceiver
Balanced Beam Splitter	BalancedBeamSplitter
90° Optical Hybrid	OpticalHybrid



(a) Single homodyne simulation block diagram.

(b) Double homodyne simulation block diagram.

Figure 4: Block diagrams of both simulation results presented in this report.

3 Required files

Header Files

File	**Description**
netxpto.h	Generic purpose simulator definitions.
local_oscillator.h	Generates continuous coherent signal.
balanced_beam_splitter.h	Mixes the two input signals into two outputs.
optical_hybrid.h	Mixes the two input signals into four outputs.
homodyne_reciever.h	Performs coherent detection on the input signal.
sink.h	Closes any unused signals.

Source Files

File	**Description**
netxpto.cpp	Generic purpose simulator definitions.
local_oscillator.cpp	Generates continuous coherent signal.
balanced_beam_splitter.cpp	Mixes the two input signals into two outputs.
optical_hybrid.cpp	Mixes the two input signals into four outputs.
homodyne_reciever.cpp	Performs coherent detection on the input signal.
sink.cpp	Closes any unused signals.

4 System Input Parameters

This system takes into account the following input parameters:

System Parameters	Description
numberOfBitsGenerated	Gives the number of bits to be simulated
bitPeriod	Sets the time between adjacent bits
samplesPerSymbol	Establishes the number of samples each bit in the string is given
localOscillatorPower_dBm1	Sets the optical power, in units of dBm, at the reference output
localOscillatorPower2	Sets the optical power, in units of W, of the signal
localOscillatorPhase1	Sets the initial phase of the local oscillator used for reference
localOscillatorPhase2	Sets the initial phase of the local oscillator used for signal
transferMatrix	Sets the transfer matrix of the beam splitter used in the homodyne detector
responsivity	Sets the responsivity of the photodiodes used in the homodyne detector
amplification	Sets the amplification of the trans-impedance amplifier used in the homodyne detector
electricalNoiseAmplitude	Sets the amplitude of the gaussian thermal noise added in the homodyne detector
shotNoise	Chooses if quantum shot noise is used in the simulation

5 Inputs

This system takes no inputs.

6 Outputs

The single homodyne system outputs the following objects:

- Signals:
  - Local Oscillator Optical Reference; (S_1)
  - Local Oscillator Optical Signal; (S_2)
  - Beam Splitter Outputs; (S_3, S_4)
  - Homodyne Detector Electrical Output; (S_5)

The double homodyne system outputs the following objects:

- Signals:
  - Local Oscillator Optical Reference; (S_1)
  - Local Oscillator Optical Signal; (S_2)
  - 90° Optical Hybrid Outputs; (S_3, S_4, S_5, S_6)
  - Homodyne Detector Electrical Output; (S_7)

7 Simulation Results

7.1 Single homodyne results

The numerical results presented in Figure 5 were obtained with the simulation described by the block diagram in Figure 4a. Theoretical results are a direct trace of (7). One can see that the numerical results adhere quite well to the expected curve.

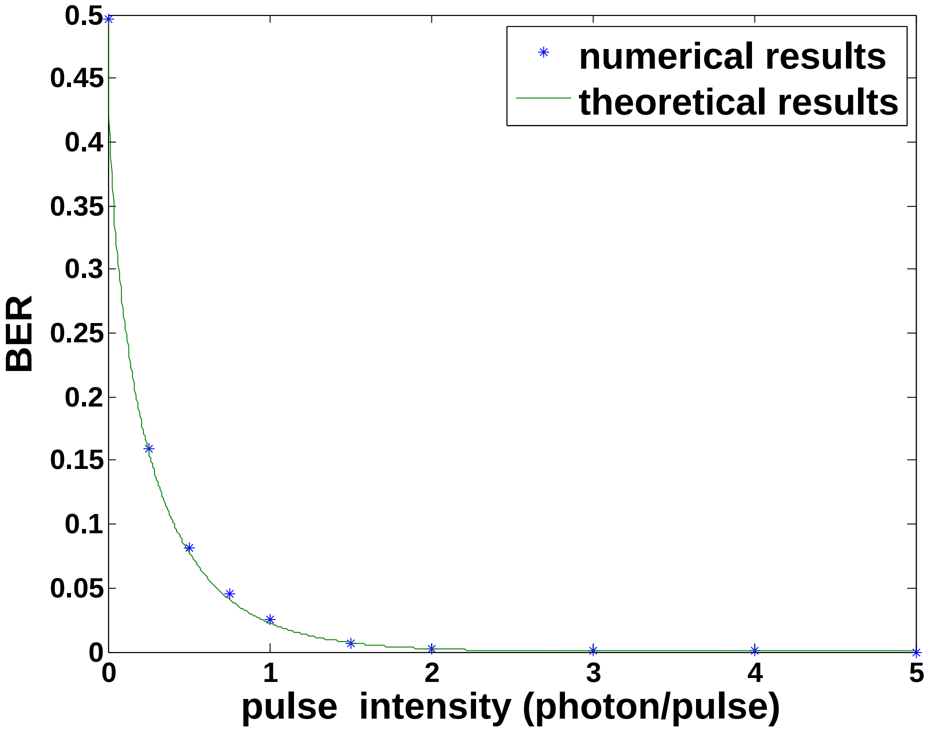


Figure 5: BER in function of α for the single homodyne setup. $X_0 = 0$ was used

7.2 Double homodyne results

The numerical results presented in Figure 6 were obtained with the simulation described by the block diagram in Figure 4b. Theoretical results are a direct trace of (12) with $\theta = \frac{\pi}{4}$. One can see that the numerical results adhere quite well to the expected curve.

8 Block Description

8.1 Homodyne Receiver

Homodyne Receiver

Introduction

This super-block compresses the function of the following blocks:

- Photodiode;
- Trans-Impedance Amplifier;

This compression allows for a cleaner code.

Input Parameters

- Responsivity
- Gain

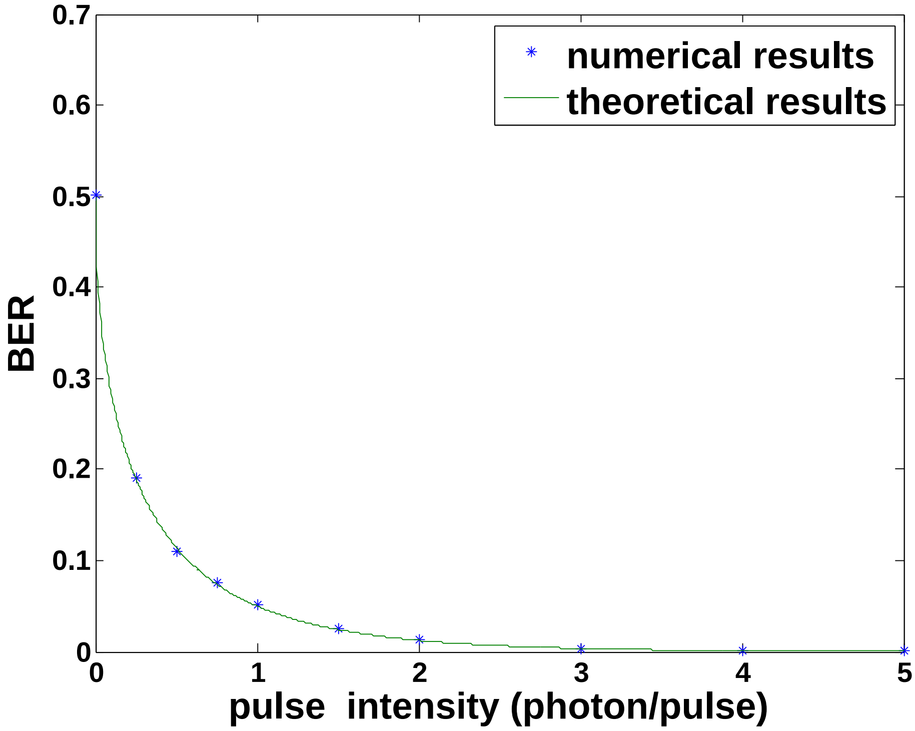


Figure 6: BER in function of α for the double homodyne setup. $X_0 = 0$ was used

- ElectricalNoiseSpectralDensity
- RollOffFactor
- ImpulseResponseTimeLength
- ImpulseResponseLength
- PassiveFilterMode

Functional Description

The input signals are evaluated by coherent detection and an electrical signal is generated from this evaluation. A diagram of the blocks that constitute this super-block, with the corresponding relations is presented in Figure 7.

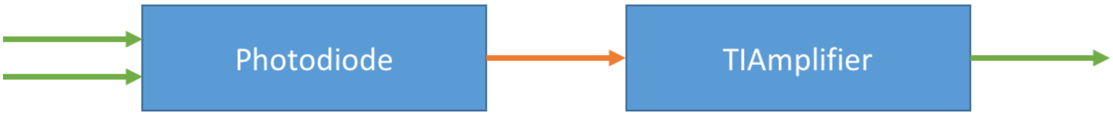


Figure 7: Homodyne Receiver Block Diagram.

Inputs

Number: 2
Type: Complex or Complex_XY (OpticalSignal)

Outputs

Number: 1
Type: Real Signal (ContinuousTimeContinuousAmplitude)

8.2 Local Oscillator

Local Oscillator

Input Parameters

- LocalOscillatorPhase
- LocalOscillatorOpticalPower
- LocalOscillatorOpticalPower_dBm

Functional Description

This blocks outputs a complex signal with a user defined length, phase and power. The phase and optical power are defined by the values of *LocalOscillatorPhase* and *LocalOscillatorOpticalPower* respectively.

Input Signals

Number: 0

Output Signals

Number: 1
Type: Complex or Complex_XY optical signal (ContinuousTimeContinuousAmplitude)

8.3 Beam Splitter

Beam Splitter

Input Parameters

- setTransferMatrix

For simplicity, the input of the transfer Matrix is in the form of a 4x1 array, with the following relation between the array, A, and matrix, M, elements:

$$A = \{ \ \{ \ \alpha, \ \beta, \ \gamma, \ \delta \ \} \ \} \Rightarrow M = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \tag{13}$$

Functional Description

This block accepts two complex signals and outputs two complex signals built from a mixture of the two inputs according to a pre-determined and user defined transfer matrix.

Input Signals

Number: 2
Type: Complex signal (ContinuousTimeContinuousAmplitude)

Output Signals

Number: 2
Type: Complex signal (ContinuousTimeContinuousAmplitude)

8.4 90^o Optical Hybrid

8.5 Photodiode

Photodiode

Input Parameters

- setResponsivity
- useNoise

Functional Description

This block accepts two complex signals and outputs one real signal built from an evaluation of the power of the input signals and their subsequent subtraction. The responsivity is defined by the value of *Responsivity.* This block also adds random gaussian distributed shot noise with an amplitude defined by the power of the inputs. The shot noise is activated by the boolean variable set by the *useNoise* parameter.

Input Signals

Number: 2
Type: Complex signal (ContinuousTimeContinuousAmplitude)

Output Signals

Number: 1
Type: Real signal (ContinuousTimeContinuousAmplitude)

8.6 Amplifier

Ideal Amplifier

Input Parameters

- setGain

Functional Description

This block accepts one time continuous signal and outputs one time continuous signal of the same type built from multiplying the input signals by a predetermined value. The multiplying factor is defined by the values of *Gain.* The input and output signals must be of the same type.

Input Signals

Number: 1
Type: Real, Complex or Complex_XY signal (ContinuousTimeContinuousAmplitude)

Output Signals

Number: 1
Type: Real, Complex or Complex_XY signal (ContinuousTimeContinuousAmplitude)

8.7 Electrical Filter

Pulse Shaper

This blocks applies a time domain, finite impulse response filter to the signal. The filter's transfer function is defined by the vector *impulseResponse.* It allows for passive filter mode operation via a boolean check.

Input Parameters

- filterType
- impulseResponseTimeLength
- rollOfFactor
- usePassiveFilterMode

Functional Description

Input Signals

Number: 1
Type: Sequence of Dirac Delta functions (ContinuousTimeDiscreteAmplitude)

Output Signals

Number: 1
Type: Sequence of impulses modulated by the filter (ContinuousTimeContiousAmplitude)

Suggestions for future improvement

Introduce other types of filters.

9 Known Problems

1. Homodyne Super-Block not functioning
2. 90° Optical Hybrid PDF needs to be written

References

[1] Ryo Namiki and Takuya Hirano. Security of quantum cryptography using balanced homodyne detection. *Physical Review A*, 67(2):022308, 2003.