6.2.2 Simulation Analysis

Students Name	:	Mariana Ramos (7/11/2017 - 9/4/2018)
Goal	:	Perform a simulation of BB84 communication protocol.

In this sub section the simulation setup implementation will be described in order to implement the BB84 protocol. In figure 6.11 a top level diagram is presented. Then it will be presented the block diagram of the transmitter block (Alice) in figure 6.12 and the receiver block (Bob) in figure 6.13. In a first approach, we do not consider the existence of eavesdropper.

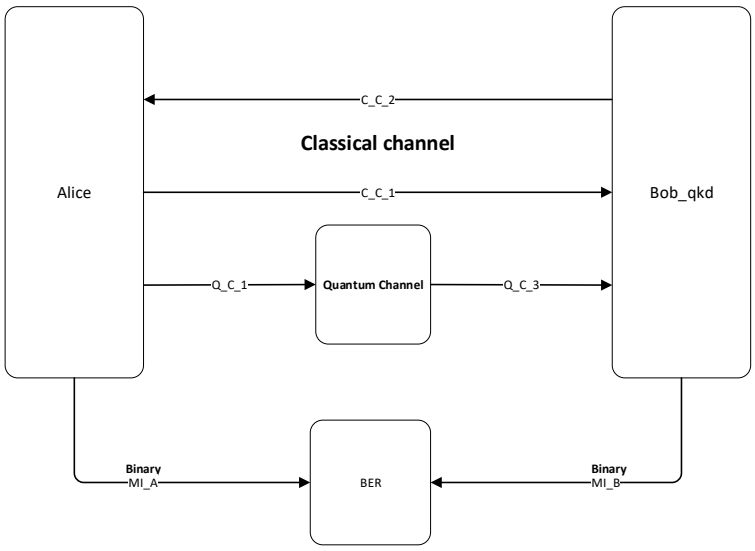

Figure 6.11: Simulation diagram at Alice's side

Figure 6.11 presents the top level diagram of our simulation. The setup contains two parties Alice and Bob, where the communication between them is done throughout two authenticated classical channels and one public quantum channel. In a first approach we will perform the simulation without eavesdropper presence. Furthermore, for bit error rate calculation between Alice and Bob.

In figure 6.12 one can observe a block diagram of the simulation at Alice's side. As it is shown in the figure, Alice must have one block for random number generation which is responsible for basis generation to polarize the photons, and for key random generation in order to have a random state to encode each photon. Furthermore, she has a Processor block for all logical operations: array analysis, random number generation requests, and others. This block also receives the information from Bob after it has passed through a fork's block. In addition, it is responsible for set the initial length l of the first array of photons which will send to Bob. This block also must be responsible for send classical information

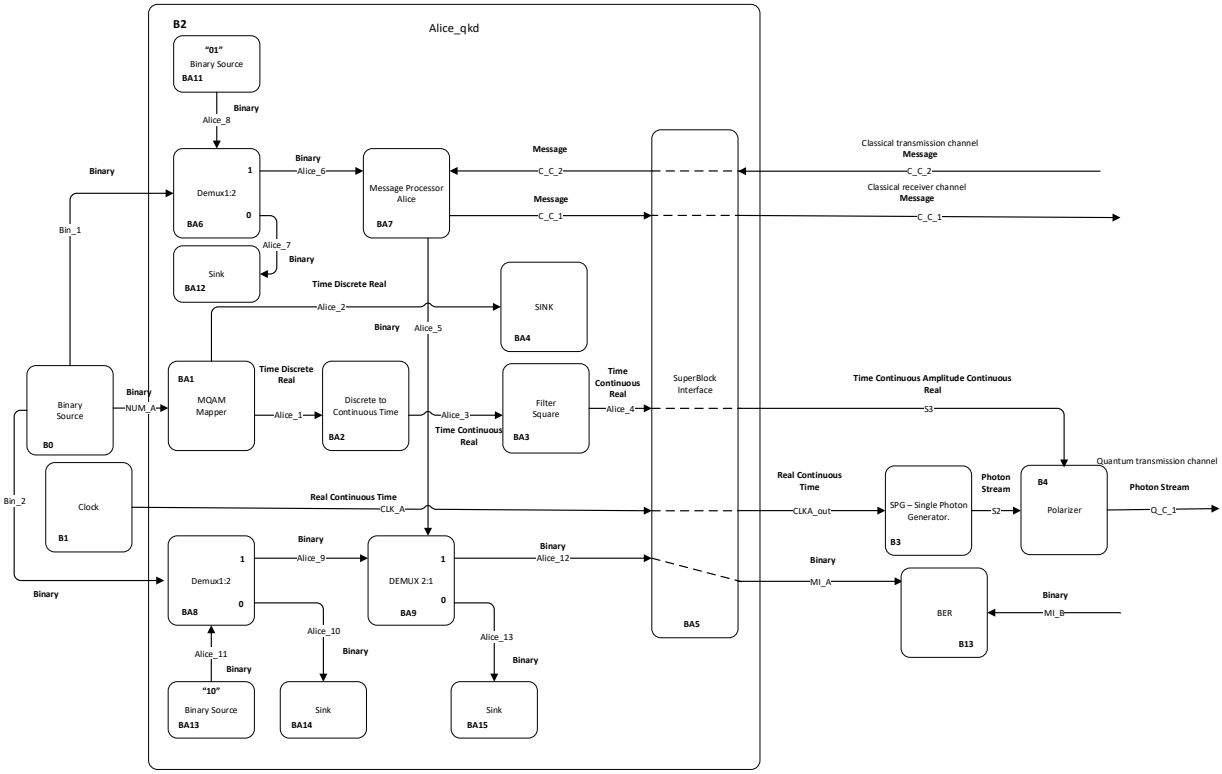

Figure 6.12: Simulation diagram at Alice's side

to Bob. Finally, Processor block will also send a real continuous time signal to single photon generator, in order to generate photons according to this signal, and finally this block also sends to the polarizer a real discrete signal in order to inform the polarizer which basis it should use. Therefore, she has two more blocks for quantum tasks: the single photon generator and the polarizer block which is responsible to encode the photons generated from the previous block and send them throughout a quantum channel from Alice to Bob.

Finally, Alice's processor has an output to Mutual Information top level block, Ms_A.

In figure 6.12 one can observe a block diagram of the transmitter. As it is shown in the figure, the transmitter must have one block for random number generation (binary source) which is responsible for basis generation to polarize the photons, and for key random generation in order to have a random state to encode each photon. This block has three outputs which will be inputs for the super block Alice. Furthermore, Alice block is responsible for all logical operations: random single photons state values generation, receive and send messages to the receiver Bob by using the classical channels, binary output for mutual information calculations. Each block of the super block is described in Library chapter. Finally, Alice block will also send a real continuous time signal to single photon generator (clock sets the rate oh photons generation), in order to generate photons polarized in the horizontal axis by default. Therefore, the transmitter has one more block, the polarizer

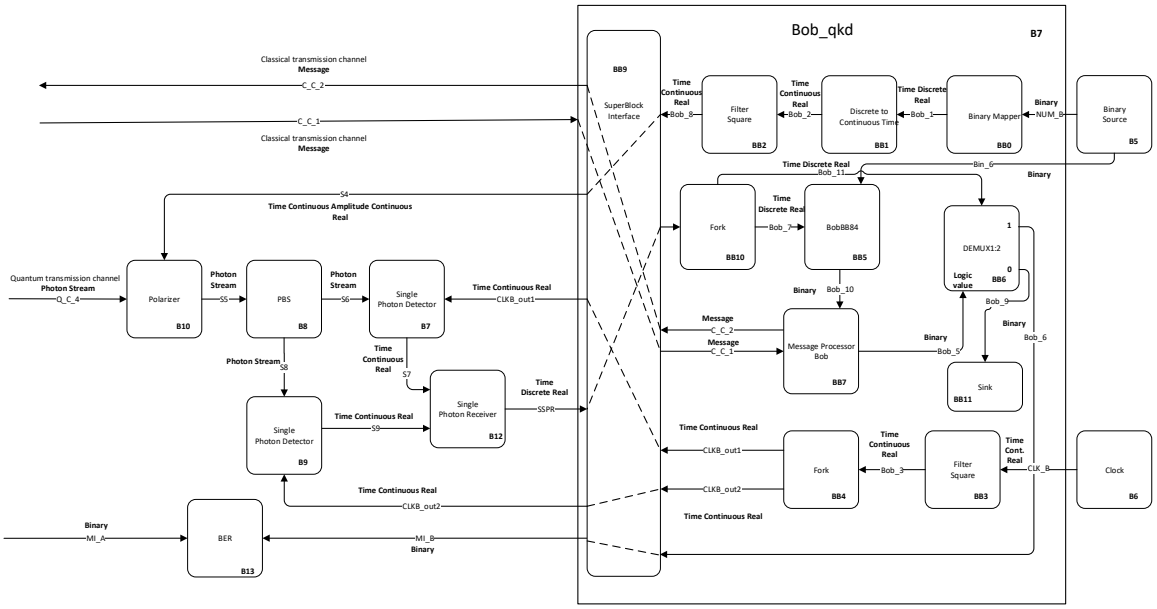

Figure 6.13: Simulation diagram at Bob's side

block, which is responsible to encode the photons generated from the previous block and send them throughout a quantum channel from Alice to Bob.

In figure 6.13 one can see a block diagram of the simulation for receiver (Bob). The receiver has one block for Random Number Generation which is responsible for randomly generate basis values which Bob will use to measure the photons sent by Alice throughout the quantum channel. Like transmitter, the receiver has the Bob block responsible for receive and send messages through the classical channel, receive single photons values detection from the single photon detectors, provides a clock signal to the detectors and send binary values for mutual information calculation. Furthermore, the receiver has two blocks for single photon detection (one for horizontal detection and other for vertical detection) which receives from Bob block a real continuous time signal which will set the detection window for the detector and outputs for Bob block the result value for detection. In addition, there is a polarizer which receives from Bob block a time continuous real signal which provides information about the rotation angle. If the basis chosen by Bob is the diagonal basis he sends "$45°$", otherwise sends "$0°$". The polarization beam splitter divides the input photon stream in horizontal component and vertical component.

Table 6.7: System Signals

Signal name	Signal type
NUM_A, NUM_B, Bin_1, Bin_2, Bin_6	Binary
MI_A, MI_B	Binary
CLK_A, CLK_B	TimeContinuousAmplitudeContinuous
CLK_A_out, CLKB_out1, CLKB_out2	TimeContinuousAmplitudeContinuous
S2, S5, S6, S8	PhotonStreamXY
S3, S7, S9	TimeContinuousAmplitudeDiscreteReal
S4	TimeContinuousAmplitudeContinuousReal
C_C_1, C_C_3	Messages
C_C_6, C_C_4	Messages
Q_C_1, Q_C_4	PhotonStreamXY

Table 6.14 presents the system signals as well as them type.

Table 6.8: System Input Parameters

Parameter	Default Value	Description
rateOfPhotons	1000 photons/s	Number of photon per sample.
iqAmplitudeValues	{-45,0},{0,0},{45,0},{90,0}	Possible photon states.
numberOfSamplesPerSymbol	16	Number of samples per symbol.
detectorWindowTimeOpen	0.2 ms	smaller than 1 ms
detectorPulseDelay	0.7 ms	in units of ms
detectorProbabilityDarkCount	0.0	Probability of dark counts in single-photon detector.
rotationAngle	0.0	Polarization angle in XY axis to introduce in Deterministic SOP changes.
elevationAngle	0.0	Polarization angle in Poincare sphere to introduce in Deterministic SOP changes.
fiberLength	10 km	Length of the optical fibre in km.
fiberAttenuation	0.2 dB/km	Attenuation of the optical fibre in dB/km.

Table 6.9: Header Files

File name	Description	Status
netxpto_20180118.h		✓
alice_qkd_20180409.h		✓
binary_source_20180118.h		✓
bob_qkd_20180409.h		✓
clock_20171219.h		✓
discrete_to_continuous_time_20180118.h		✓
m_qam_mapper_20180118.h		✓
polarization_beam_splitter_20180109.h		✓
polarization_rotator_20180113.h		✓
pulse_shaper_20180111.h		✓
single_photon_detector_20180206.h		✓
single_photon_receiver_20180303.h		✓
SOP_modulator_20180319.h		✓
coincidence_detector_20180206.h		✓
single_photon_source_20171218.h		✓
sink_20180118.h		✓
super_block_interface_20180118.h		✓
message_processor_alice_20180205.h		✓
demux_1_2_20180205.h		✓
binary_mapper_20180205.h		✓
bobBB84_20180221.h		✓
message_processor_bob_20180221.h		✓
sampler_20171119.h		✓
optical_attenuator_20180304.h		✓
fork_20180112.h		✓

Table 6.10: Source Files

File name	Description	Status
netxpto_20180118.cpp		✓
bb84_with_discrete_variables_sdf.cpp		✓
alice_qkd_20180409.cpp		✓
binary_source_20180118.cpp		✓
bob_qkd_20180409.cpp		✓
clock_20171219.cpp		✓
discrete_to_continuous_time_20180118.cpp		✓
m_qam_mapper_20180118.cpp		✓
polarization_beam_splitter_20180109.cpp		✓
polarization_rotator_20180113.cpp		✓
pulse_shaper_20180111.cpp		✓
single_photon_detector_20180206.cpp		✓
single_photon_receiver_20180303.cpp		✓
SOP_modulator_20180319.cpp		✓
coincidence_detector_20180206.cpp		✓
single_photon_source_20171218.cpp		✓
sink_20180118.cpp		✓
super_block_interface_20180118.cpp		✓
message_processor_alice_20180205.cpp		✓
demux_1_2_20180205.cpp		✓
binary_mapper_20180205.cpp		✓
bobBB84_20180221.cpp		✓
message_processor_bob_20180221.cpp		✓
sampler_20171119.cpp		✓
optical_attenuator_20180304.cpp		✓
fork_20180112.cpp		✓

Simulation Results

Figure 6.14 represents the block diagram of the first simulation performed between Alice and Bob. This simulation intends to simulate the communication protocol between Alice and Bob until they do the Basis Reconciliation. At this time, it is not taken into account any attack from an eavesdropper. However, as one can learn from theoretical protocol analysis, the attenuation due the fiber losses, dark counts probabilities from single photon detectors and the SOP drift over the quantum channel are all taken into account.

Alice starts by sending a sequence of photons to Bob, and then he measures the photons according to random basis randomly generated by his binary source. After that, he follows the protocol described above until Alice sends to him a string of '0' and '1' where '0' means that both used different basis and '1' means that they used the same basis. Therefore, Alice

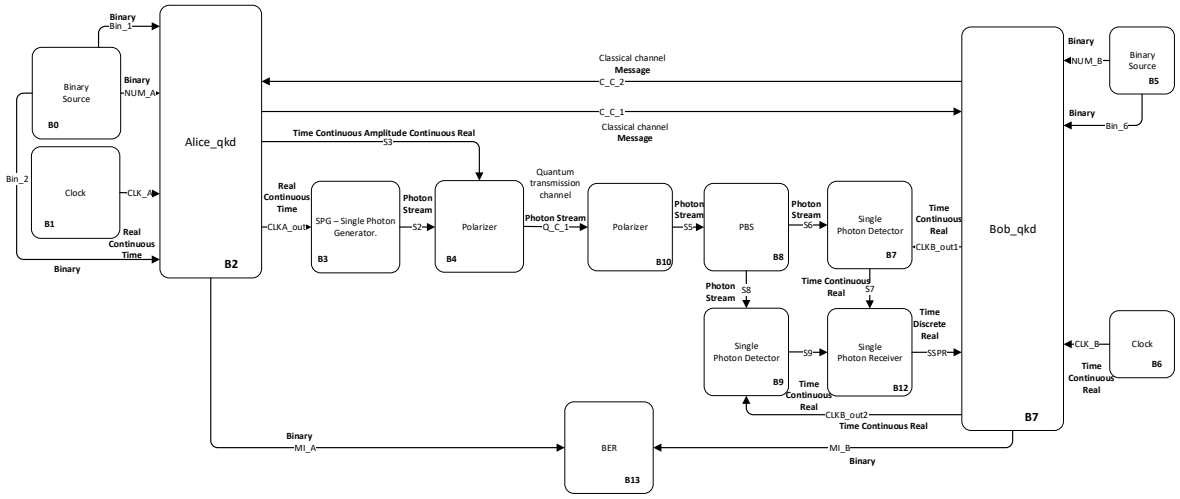

Figure 6.14: Diagram block of simulation performed between Alice and Bob until Basis Reconciliation.

and Bob outputs a binary signal "MI_A" and "MI_B", respectively. In case of no errors occurred in the quantum channel, these signals should be equal in order to both have the same sequence of bits. Furthermore, QBER between the two sequences should be 0. This way, Alice can encode messages using these keys and Bob will be capable of decrypt the message using these symmetric keys. When errors are introduced in quantum channel QBER value will increase as we can see later.

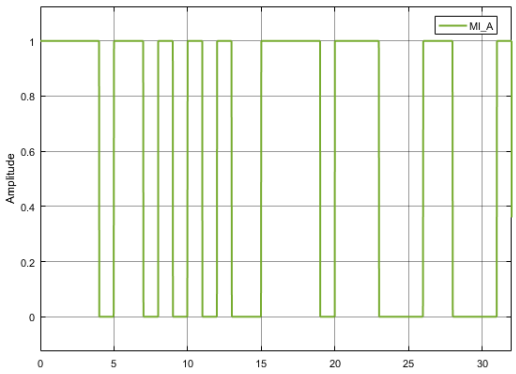

Figure 6.15: MI_A signal.

Figure 6.15 and figure 6.16 represent the sequence of bits which will be used by Alice to encode the messages and the sequence of bits used by Bob to decode the message when no errors in quantum channel are taken into account, respectively. As one can see the two

signals are equal which meets the expected result. In this way, the first step of the protocol has been achieved.

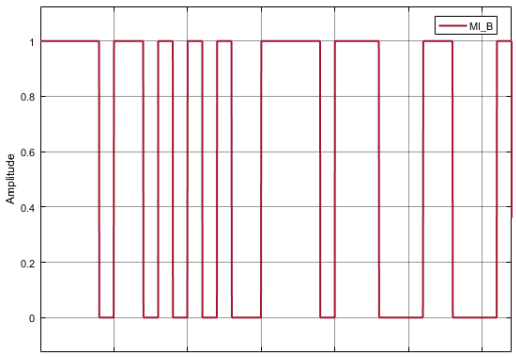

Figure 6.16: MI_B signal.

As one can see in figure 6.28 a block which calculates QBER is connected to Alice and Bob. This block calculates the QBER between the measurements that Bob performed with the same basis as Alice, based on method described in [3]. Thus, as expected, the QBER is 0% when no errors are taken into account.

Next, some errors due the changes in state of polarization of the single photons transmitted between Alice and Bob were added. This way, a polarization rotator in the middle of the quantum channel was added, which is controlled by a SOP modulator block as it is shown in figure 6.17 with modelled with deterministic [4] and stochastic [5] methods. Additional information about the blocks presented in this quantum channel can be found in library chapter.

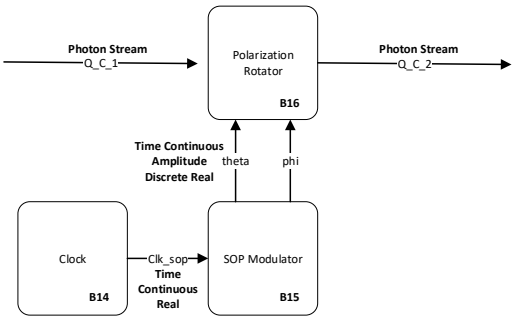

Figure 6.17: Quantum channel diagram.

Now, it is important to calculate the QBER as a function of the rotation angle θ. In order to do that, it was simulated a deterministic SOP modulation, in which the θ angle varies over the time. In figure 6.57 is presented the variation in the value of QBER with respect with theta changes from $0°$ to $45°$. Theoretically, QBER corresponds to the probability of errors in

the channel. Which means that in practice this probability corresponds to the probability of a photon following the wrong path in the polarization beam splitter immediately before the detection circuit.

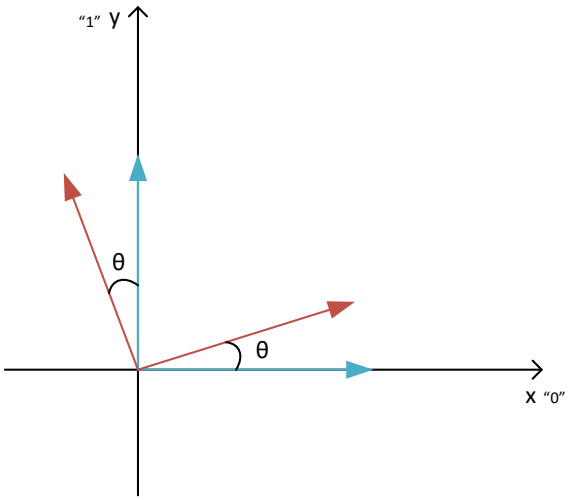

Figure 6.18: Representation of two orthogonal states rotated by an angle θ.

Figure 6.56 presents the graphical representation of two orthogonal states rotated by an angle θ. This rotation is induced by the SOP modulator block which selects a deterministic θ and ϕ angles that do not change over the time. This same rotation is applied for all sequential samples. From figure 6.56 the theoretical QBER can be calculated using the following equation:

$$QBER = P(0)P(1|0) + P(1)P(0|1). \tag{6.13}$$

Since we have been using a polarization beam splitter 50:50,

$$P(0) = P(1) = \frac{1}{2}.$$

This way,

$$QBER = \frac{1}{2}sin^2(\theta) + \frac{1}{2}sin^2(\theta) \tag{6.14}$$

$$QBER = sin^2(\theta). \tag{6.15}$$

In figure 6.57 are represented two curves: QBER calculated from simulated data and QBER calculated using theoretical model from equation 6.33. Furthermore, the cross correlation coefficient between the two signals was calculated using a function from MATLAB *xcorr(x,y,'coeff')* which the result is 99.92%. From that, we can conclude that the QBER calculated from simulated data follows the theoretical curve with high correlation.

Nevertheless, the error bars presented in figure 6.57 were calculated based on a confidence interval of 95%.

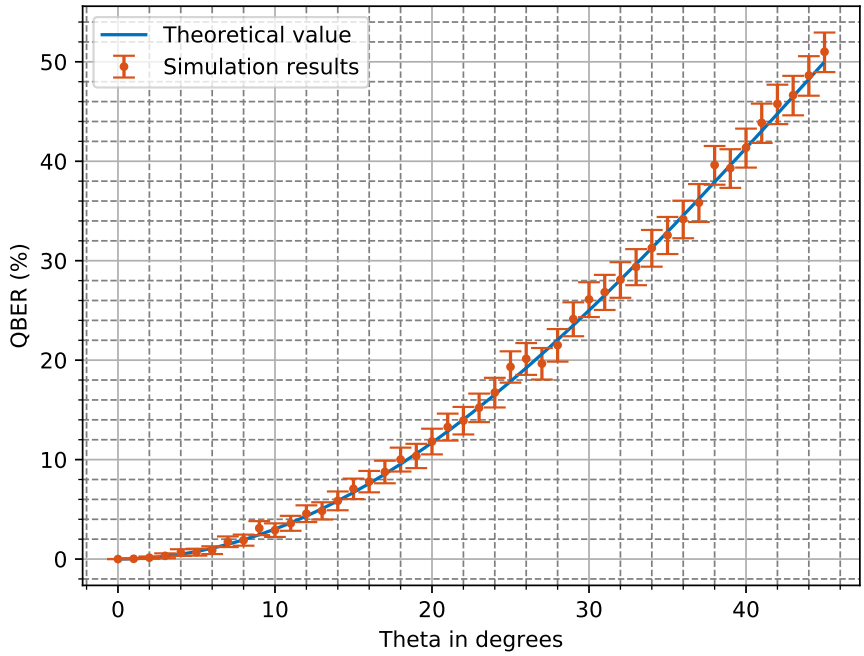

Figure 6.19: QBER evolution in relation with deterministic SOP drift.

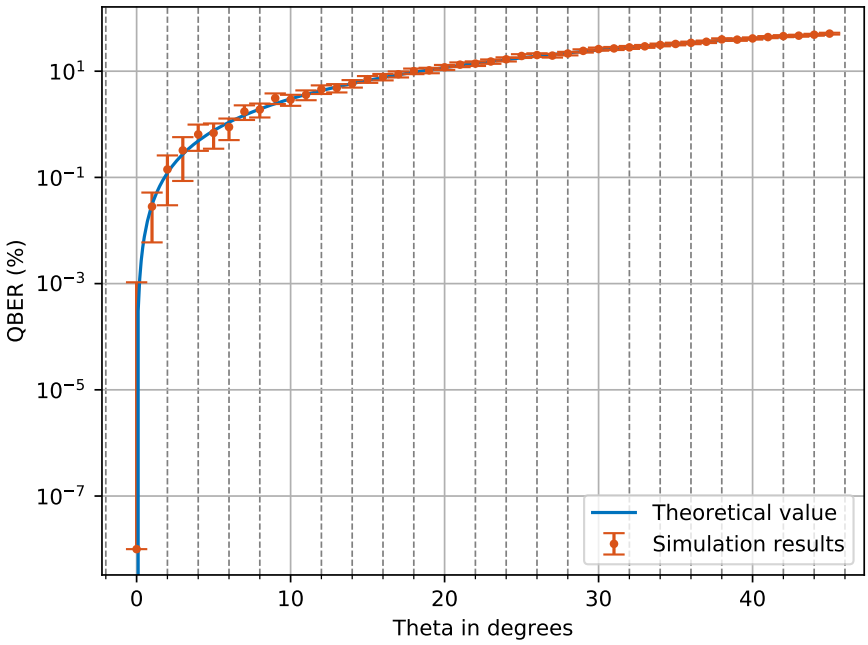

Figure 6.20: QBER evolution in relation with deterministic SOP drift in log scale.

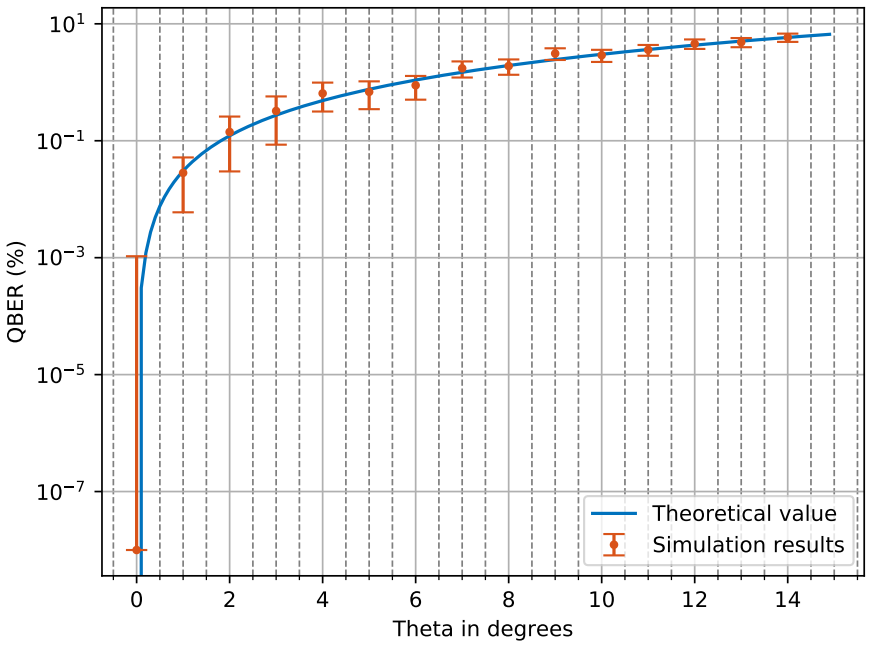

Figure 6.21: QBER evolution in relation with deterministic SOP drift scaled.