1 Hamming Channel Encoder/Decoder

Students Name	:	Luis Almeida (01/06/2018 - ?)
Starting Date	:	November 7, 2017
Goal	:	BB84 implementation with discrete variables.

BB84 is a key distribution protocol which involves three parties, Alice, Bob and Eve. Alice and Bob exchange information between each other by using a quantum channel and a classical channel. The main goal is continuously build keys only known by Alice and Bob, and guarantee that eavesdropper, Eve, does not gain any information about the keys.

1.1 Protocol Analysis

Students Name	:	Kevin Filipe (7/11/2017 - 10/11/2017)
Goal	:	BB84 - Protocol Description

BB84 protocol was created by Charles Bennett and Gilles Brassard in 1984 [**?**]. It involves two parties, Alice and Bob, sharing keys through a quantum channel in which could be accessed by a eavesdropper, Eve. A basic model is depicted in figure **??**.

We are going to analyse the BB84 protocol with bit encoding into photon state polarization. Two non-orthogonal basis are used to encode the information, the rectilinear and diagonal basis, + and x respectively. The following table shows this bit encoding.

The protocol requires the following parameter and it is implemented with the following steps:

1. Alice generates two random bit strings. The random string , R_{A1}, corresponds to the data to be encoded into photon state polarization. R_{A2} is a random string in which 0 and 1 corresponds to the rectilinear, +, and diagonal, $\times$, respectively.

$$R_{A1} = \{0,1,1,0,1,0,0,1,1,0,1,1,1,0,0,1,0,0,0,1\}$$

$$\begin{aligned} R_{A2} &= \{0,0,1,0,1,1,1,0,1,1,1,0,1,0,0,0,1,0,1,0\} \\ &= \{+,+,\times,+,\times,\times,\times,+,\times,\times,\times,+,\times,+,+,+,\times,+,\times,+\} \end{aligned}$$

2. Alice transmits a train of photons, S_{AB}, obtained by encoding the bits, R_{A1} with the respective photon polarization state R_{A2}.

$$S_{AB} = \{\rightarrow,\uparrow,\searrow,\rightarrow,\searrow,\nearrow,\nearrow,\uparrow,\searrow,\nearrow,\searrow,\uparrow,\searrow,\rightarrow,\rightarrow,\uparrow,\nearrow,\rightarrow,\nearrow,\uparrow\}.$$

3. Bob generates a random string, R_B, to receive the photon trains with the correspondent basis.

$$\begin{aligned} R_B &= \{0,1,1,1,0,1,0,0,1,1,0,0,1,1,0,0,1,1,0,0\} \\ &= \{+,\times,\times,\times,+,\times,+,+,\times,\times,+,+,\times,\times,+,+,\times,\times,+,+\} \end{aligned}$$

4. Bob performs the incoming photon states measurement, M_B, with its generated random basis, R_B. If the two photon detectors don't click, means the bit was lost during transference due to attenuation. If both photon detectors click, a false positive was detected. In the measurements, M_B, the no-click in both detectors is represented by a -1 and the false positives to -2. The measurements done in rectilinear or diagonal basis are represented by 0 or 1, respectively. This is represented **??**

$$M_B = \{0, 1, 1, 1, -1, 1, 0, 0, -2, 1, 0, 0, -2, 1, 0, 0, 1, -1, 0, 0\}$$

5. After the measurement, Bob sends to Alice, using the classical channel, the used basis values, R_B with the attenuation, -1, and false positives,-2.

6. Alice performs a modified negated XOR, generating a sequence that detects when the same basis she used B_{AB}.

7. Alice sends the B_{AB} sequence to Bob, in which he can correlate with, M_B, and deduce the key K_{AB}.

$$K_{AB} = \{0, 1, 0, 1, 0, 1, 0, 1, 0, 1\}.$$

8. Alice then by having knowledge of R_{A2} and B_{AB} performs a scrambling algorithm over the deduced key. It is generated a matrix $M \times N$, according to the input parameter. Assuming a scrambling matrix of 3x4, **??**. And being the scramble key represented as KS_{AB}

$$KS_B = \{0, 0, 0, 1, 1, 1, 0, 0, 1, 1\}$$

9. Bob uses the same algorithm as Alice and scrambles his key.

10. Bob then reveals a fixed number of his key to Alice. This number is also an input parameter value, k. With this the Quantum Bit Error Rate (QBER).

To determine the QBER, it is necessary to know the confidence interval parameter, α and the QBER limit, in which states the maximum allowed QBER by the user. Then to verify if the channel is reliable or not, the flowchart presented in figure **??**.

1. Bob will reveals k bits sequence from the scrambled key, SK_{AB} to Alice.

2. Alice then returns to Bob the estimated QBER value, mQBER, with a confidence interval, [qLB, qUB] using the using the equations in the Bit Error Rate section, but applied to this protocol

3. To check if the channel is compromised or not it is necessary to check if the QBER limit is higher than the QBER upper bound. If QBER limit is between the QBER lower and upper bound it is necessary to reveal more k bits from the key. Otherwise the channel is compromised and the key determination process needs to restart.

1.2 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 **??** a top level diagram is presented. Then it will be presented the block diagram of the transmitter block (Alice) in figure **??** and the receiver block (Bob) in figure **??**. In a first approach, we do not consider the existence of eavesdropper.

Figure **??** 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 **??** 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 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 **??** 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 block, which is responsible to en-

code the photons generated from the previous block and send them throughout a quantum channel from Alice to Bob.

In figure **??** 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 **??** presents the system signals as well as them type.

1.2.1 Simulation Results

Figure **??** 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 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 **??** and figure **??** 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.

As one can see in figure **??** a block which calculates QBER is connected

Figure 1: Basic QKD Model. Alice and Bob are connected by 2 communication channels, a public quantum channel and a authenticated classical channel, with an eavesdropper, Eve (figure adapted from [**?**]).

Bit	*Rectilinear Basis,+*	*Diagonal Basis,×*
0	0	-45
1	90	45

Figure 2: Single-Photon Detection block with false-positives, -2, and attenuation, -1, detection depending on D1 and D2 output.

Figure 3: Flowchart to determine if the channel is reliable or not.

Figure 4: Simulation diagram at Alice's side

Table 1: Initial Parameters.

Parameter	**Description**
$M \times N$	Scrambling Matrix M by N
k	Number of revealed bits for BER calculation
α	Confidence level
A	B

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 [**?**]. 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 **??** with modelled with deterministic [**?**] and stochastic [**?**] methods. Additional information about the blocks presented in this quantum channel can be found in library chapter.

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 **??** 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 **??** 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 **??** the theoretical QBER can be calculated using the following equation:

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

Since we have been using a polarization beam splitter 50:50,
P(0) = P(1) = $1_{\overline{2.}}$
This way,

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

$$QBER = sin^2(\theta). \tag{3}$$

In figure **??** are represented two curves: qber calculated from simulated data and qber calculated using theoretical model from equation **??**. 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 **??** were calculated based on a confidence interval of 95%.

1.3 Open Issues

1. Implementation of the scrambling algorithm in order to spread the errors.
2. Implementation of the control system for polarization rotations.
3. Implementation of a QBER estimation protocol.
4. Implementation of the cascade for error correction.
5. Implementation of the output which represents the final key that is built.
6. Introduce EVE in simulation as shown in figure **??**.
7. Experimental Implementation.

R_{A2}	0	0	1	0	1	1	1	0	1	1	1	0	1	0	0	0	1	0	1	0
R_B	0	1	1	1	-1	1	0	0	-2	1	0	0	-2	1	0	0	1	-1	0	0
B_{AB}	1	0	1	0	0	1	0	1	0	1	0	1	0	0	1	1	1	0	0	1

Table 2: Scrambling matrix

0	1	0	1
0	1	0	1
0	1	-	-

[heading=subbibliography]