Numerical Modeling and Simulation of Quantum Key Distribution Systems under Non-Ideal Conditions

Sadman Shafi,[1,*] Md. Serajum Monir,[1] and Md. Saifur Rahman[1]

[1] Department of Electrical and Electronic Engineering, Bangladesh University of Engineering and Technology
Dhaka-1000, Bangladesh

[*]sadmanshafi10@gmail.com

***Abstract*—Quantum key distribution is a very promising technology that can complement the classical cryptographic protocols. However, since the exploitation of the laws of quantum mechanics for any useful purpose is limited by the non-idealities of modern-day devices, researches are required on how these imperfections can be overcome. In this paper, we propose a QKD system and talk about implementation tradeoffs in real world design. We also propose a method for simulating this QKD system including its non-ideal factors. The results obtained by the simulation of the model try to justify a QKD system implementation instead of classical cryptography. The results also show that a real QKD system can be accurately simulated in a classical computer before it is physically set up.**

***Index terms*—Quantum cryptography, quantum key distribution, simulation, modeling, BB84, quantum communication, quantum information**

I. Introduction

Quantum mechanics, although highly counter-intuitive in nature, has proven to be the most successful theory to explain and give predictions about the nature. Its wildest of predictions has had many useful applications in modern civilization. One of the most recent of these is Quantum Key Distribution (QKD). In theory, this works just fine, but the non-idealities that occur in practical implementation severely limit its performances. In this paper we tried to model the non-idealities that arise from different devices and the environment and study how the performance of a QKD system varies with these non-idealities.

There are several approaches to Quantum Key Distribution depending on what type of property is exploited. They can be divided in two categories: prepare and measure protocols, and entanglement based protocols. In 1983, Stephen Wiesner presented the idea how information can be stored or transmitted by encoding in two "conjugate observables" [1], for example, linear and circular polarization states of light. Based on his idea Charles H. Bennett and Gilles Brassard proposed a secure cryptographic protocol which is known as BB84 [2]. Several other protocols have been suggested later, such as B92 [3], E91 [4], MSZ96 [5], SARG04 [6], KMB09 [7] etc. Numerous modifications of these protocols have been developed throughout the course of time, including a particularly significant one named the decoy state protocol [8]. Various experiments have been carried out in many parts of the world to implement QKD systems, and there are several companies that commercially manufacture QKD systems. However, the speed of communication in realized QKD systems has been a limitation. Therefore, efforts are being made to increase the speed so that it can replace classical systems around the world.

Several QKD protocols can be shown to be unconditionally secure in principle. This security is what makes QKD systems a significant and attractive alternative to classical cryptographic systems. However, practical QKD systems suffer from various non-ideal factors which create security vulnerabilities in the systems. Hence much research is being conducted in studying the effects of these non-idealities on QKD systems, and developing possible countermeasures. A utility for simulating QKD systems incorporating these non-ideal conditions can greatly help in these studies, and developing such a simulation utility is our objective.

The remainder of the paper is organized as follows: In section II we talk about the basic principle of the QKD protocol BB84. In section III we give an illustration of the results and error rates that can be theoretically obtained under ideal conditions. In section IV we propose the QKD system based on the BB84 protocol that can be implemented in practice. We also discuss about various devices and components in the QKD system and the sources of non-idealities. We provide mathematical modeling for these non-idealities, and in section V, we define some system parameters necessary for characterization of the system performance. Based on the mathematical models we show the simulation results in section VI. Finally, in section VII we give conclusions and provide future research efforts.

II. Basic Principle

The BB84 protocol requires two parties- Alice, the sender, and Bob, the receiver. Alice prepares two random bit-streams – the message bit-stream a and the basis bit-stream b. She prepares qubits in two bases according to a and b. We assume that she prepares the qubits by "encoding" single photons with four polarization states – horizontal $|H\rangle$, vertical $|V\rangle$, diagonal $|+\rangle$ and antidiagonal $|-\rangle$. She then sends the prepared qubits to Bob through a quantum channel.

TABLE I. Polarization States and Bases

Polarization State	Basis	Dirac Notation Representation	Encoded Bit
Horizontal	Rectilinear	$\|0\rangle = 1 \cdot \|H\rangle + 0 \cdot \|V\rangle$	0
Vertical	Rectilinear	$\|1\rangle = 0 \cdot \|H\rangle + 1 \cdot \|V\rangle$	1
Diagonal	Diagonal	$\|+\rangle = \frac{1}{\sqrt{2}} \cdot \|H\rangle + \frac{1}{\sqrt{2}} \cdot \|V\rangle$	0
Anti-diagonal	Diagonal	$\|-\rangle = \frac{1}{\sqrt{2}} \cdot \|H\rangle - \frac{1}{\sqrt{2}} \cdot \|V\rangle$	1

Bob prepares a random basis bit-stream b' and measures the states of the qubits according to b'. Using the outcome of the measurements, he obtains a raw message bit-stream a'. If the

978-1-5386-3374-8/17/$31.00 ©2017 IEEE

bit-streams are long, about 75% of the bits of a and a' will match, and about 50% of the bits of b and b' will match. Alice and Bob then publicly compare b and b' and discard those bits of a and a' corresponding to the bits of b and b' that do not match. This process is called "sifting", and the message bit-streams thus obtained after sifting are the "sifted keys" a_{sift} and a'_{sift}. Ideally, without any noise and any eavesdropper, $a_{\text{sift}} = a'_{\text{sift}}$. Thus, there will be no error in the sifted keys formed.

Now suppose an eavesdropper, Eve, is present, who tries to intercept the qubits sent by Alice. Eve measures the states of the intercepted qubits. However, this destroys the states of those qubits, and by the "no-cloning theorem" [9], she will not be able to reproduce those states. She then prepares qubits according to the outcomes of her measurements, and sends them to Bob to avoid suspicion. This hacking strategy is called intercept-and-resend attack. If this attack is made, then the error in Bob's a' will be more than 25%, and thus Bob will be able to detect the presence of Eve.

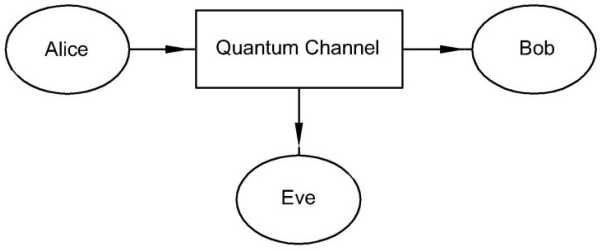

Fig. 1. Schematic diagram of a generic quantum key distribution system

It can be shown that the BB84 protocol is theoretically unconditionally secure under ideal conditions [10].

III. Simulation under Ideal Conditions

We have carried out a simulation of the BB84 protocol under ideal conditions. The simulation was done using MATLAB. We have included the presence of Eve who performs an intercept-and-resend attack in the system. The eavesdropping rate of Eve (the ratio of the number of qubits intercepted by Eve to the total number of qubits transmitted by Alice) is varied and its effects are observed on the error rate and the message match rate of Bob's received message with the transmitted message of Alice before and after sifting. The results are shown in Fig 2.

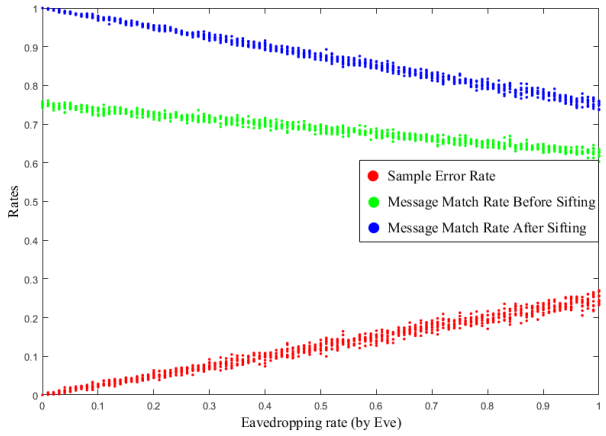

Fig. 2. Sample error rate, message match rates before and after sifting vs. eavesdropping rate by Eve

The results match with those predicted theoretically. The sample error rate (error rate in a sample of bits chosen randomly from the sifted key by Alice and Bob) increases with the increase in eavesdropping rate, because increased eavesdropping causes increased disturbance in the states of the qubits, and thus results in an increased error rate. This also causes the message match rates before and after sifting to decrease.

IV. Implementation of the Proposed Quantum Key Distribution System and Non-Ideality Simulation

The QKD system consists of three parts - Alice's module (transmitter), quantum channel and Bob's module (receiver).

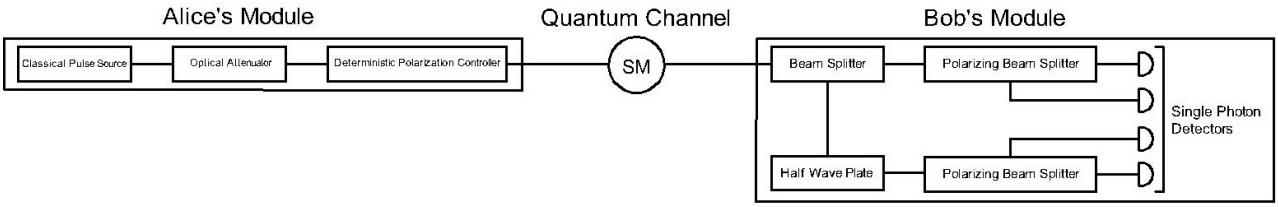

Fig. 3. Schematic diagram of the modelled quantum key distribution system employing the BB84 protocol

A. Alice's Module

Alice's module consists of a classical pulse source, an optical attenuator and a deterministic polarization controller. The classical pulse source produces strong optical pulses of light plane polarized in a particular direction at a certain rate. The optical attenuator strongly attenuates these pulses to "weak coherent pulses" having a very low mean photon number (less than 1). The weak coherent pulses act as "single photons". The deterministic polarization controller sets the polarization states of these pulses according to Alice's message and basis bits.

1) Classical Pulse Source: The classical pulse source consists of a laser diode and a polarizer. The laser diode produces unpolarized light pulses of wavelength 1550 nm. Each pulse has millions or billions of photons and behaves as a "classical" pulse. The polarizer plane-polarizes these pulses at a certain orientation angle.

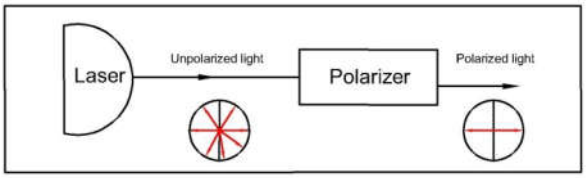

Fig. 4. Schematic diagram of the classical pulse source

Commercially available optical fibers and most other optical devices used in optical fiber communication have been optimized for the wavelength 1550 nm, and so this wavelength has been chosen [11].

2) Optical Attenuator: The optical attenuator block consists of a fixed optical attenuator (FOA) and an electronic variable optical attenuator (EVOA).

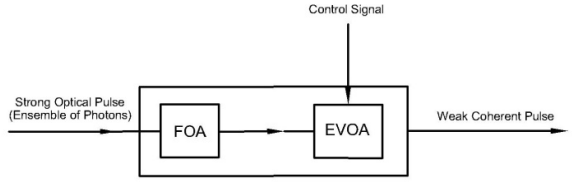

Fig. 5. Schematic diagram of the optical attenuator

The photon numbers in the weak coherent pulses produced obey Poisson statistics [11], [12]. If the mean photon number of the weak coherent pulses is μ, then the probability that a weak coherent pulse will contain n photons is given by

$$P(n) = \frac{\mu^n e^{-\mu}}{n!} \tag{1}$$

If a pulse contains more than 1 photon, it can cause security vulnerabilities. They can be mitigated by several ways, such as the use of decoy states [8].

3) Deterministic Polarization Controller:

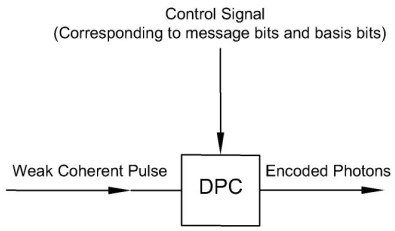

Fig. 6. Schematic diagram of the deterministic polarization controller

The deterministic polarization controller (DPC) can change the polarization state of light passing through it in a known and controlled manner. It is used to "encode" photons by setting their polarization states according to the bit streams a and b of Alice.

B. Quantum Channel

The photons emitted from the source travel through a "quantum channel". A single mode optical fiber can be used as this "quantum channel". We have used photons of wavelength 1550nm since at this value the attenuation through the fiber is very low, about $0.2dB/km$. A real optical fiber can introduce several non-idealities, such as polarization change, depolarization, polarization mode dispersion etc. We have included the polarization change of photons transmitted through the channel in the simulation.

C. Bob's Module

Bob's module consists of a beam splitter, a half wave plate, two polarizing beam splitters and four single photon detectors.

1) Beam splitter: The beam splitter (BS) splits light incident on it into two parts by transmitting a certain portion of the light and reflecting the remaining light in another direction. In this work, we have used a 50:50 beam splitter that transmits half of the incident light and reflects the other half.

Real beam splitters exhibit some non-ideal properties such as attenuation, ghosting, polarization dependent losses etc. Consider a BS with a split ratio $r = T:R$. Let the amplitudes of the incident light, the transmitted light and the reflected light be $E_0 E_T$ and E_R and their intensities be $I_0 I_T$ and I_R respectively. Suppose, their polarization orientation angles are $\theta_0 \theta_T$ and θ_R, the horizontal components of their amplitudes are $E_{0x} E_{Tx} E_{Rx}$ and their vertical components are $E_{0y} E_{Ty} E_{Ry}$ respectively. Let the attenuation of the beam splitter be α (in decibels) and the polarization dependent losses for horizontal and vertical polarization states be PDL_x and PDL_y (in decibels) respectively. Then

$$\alpha + PDL_x = 10\log_{10}\left(\frac{E_{Tx}^2}{E_0^2\cos^2\theta_0}\times\frac{T+R}{T}\right) = 10\log_{10}\left(\frac{E_{Rx}^2}{E_0^2\cos^2\theta_0}\times\frac{T+R}{R}\right) \tag{2}$$

$$\alpha + PDL_y = 10\log_{10}\left(\frac{E_{Ty}^2}{E_0^2\sin^2\theta_0}\times\frac{T+R}{T}\right) = 10\log_{10}\left(\frac{E_{Ry}^2}{E_0^2\sin^2\theta_0}\times\frac{T+R}{R}\right) \tag{3}$$

$$I_T \propto E_T^2 = E_{Tx}^2 + E_{Ty}^2 \tag{4}$$

$$I_R \propto E_R^2 = E_{Rx}^2 + E_{Ry}^2 \tag{5}$$

For a single photon incident on a BS, whether it will be transmitted or reflected is a purely random event - a feature of quantum mechanics. For a real BS, if we incorporate attenuation and polarization dependent losses, then the probability that an incident photon will be transmitted is

$$P(T) = \frac{I_T}{I_0} = \frac{E_T^2}{E_0^2} = \frac{T}{T+R}\cdot 10^{\frac{\alpha}{10}}\left(10^{\frac{PDL_x}{10}}\cos^2\theta_0 + 10^{\frac{PDL_y}{10}}\sin^2\theta_0\right) \tag{6}$$

And the probability that it will be reflected is

$$P(R) = \frac{I_R}{I_0} = \frac{E_R^2}{E_0^2} = \frac{R}{T+R}\cdot 10^{\frac{\alpha}{10}}\left(10^{\frac{PDL_x}{10}}\cos^2\theta_0 + 10^{\frac{PDL_y}{10}}\sin^2\theta_0\right) \tag{7}$$

Thus, a photon passing through a real BS has a finite probability of being "destroyed" (e.g. scattered or absorbed), and that probability is

$$P(\text{destroy}) = 1 - P(T) - P(R) \tag{8}$$

The beam splitter performs a "passive basis selection" for Bob by randomly transmitting or reflecting an incident photon. A transmitted photon will be measured in the horizontal-vertical basis, whereas a reflected photon will be measured in the diagonal-antidiagonal basis.

2) Half wave plate: The half wave plate rotates the plane of polarization of a plane polarized incident beam of light by a specified amount. In our work, the half wave plate is aligned so that it rotates the plane of polarization of the incident light by 45° clockwise.

3) Polarizing Beam Splitter: The polarizing beam splitter (PBS) splits the incident beam of light into two beams of light with different polarization states. Real polarizing beam splitters display several non-idealities, such as attenuation,

polarization dependent losses etc. Using the quantities mentioned in case of the normal beam splitter, we have

$$\alpha + PD\,L_x = 10\log_{10}\left(\frac{E_{Tx}^2}{E_0^2\cos^2\theta_0}\right) \quad (9)$$

$$\alpha + PD\,L_y = 10\log_{10}\left(\frac{E_{Ry}^2}{E_0^2\sin^2\theta_0}\right) \quad (10)$$

$$r_e\ (dB) = 10\log_{10}\left(\frac{E_{Tx}^2}{E_{Ty}^2}\right) = 10\log_{10}\left(\frac{E_{Ry}^2}{E_{Rx}^2}\right) \quad (11)$$

Here, r_e is the extinction ratio of the PBS. Equations (4), (5) also apply here.

Similar to a normal BS, if a single photon is incident on a PBS, whether it will be transmitted or reflected is a random event. The probability that an incident photon will be transmitted is

$$P(T) = \frac{I_T}{I_0} = 10^{-\frac{\alpha + PD\,L_x}{10}}\left(1 + 10^{-\frac{r_e}{10}}\right)\cos^2\theta_0 \quad (12)$$

And the probability that it will be reflected is

$$P(R) = \frac{I_R}{I_0} = 10^{-\frac{\alpha + PD\,L_y}{10}}\left(1 + 10^{-\frac{r_e}{10}}\right)\sin^2\theta_0 \quad (13)$$

The probability that an incident photon will be annihilated is thus similar to (12).

4) Single photon detector: The single photon detector (SPD) can detect and count single photons and weak coherent pulses incident on it. One of the most feasible single photon detectors suitable for quantum communication using photons at the telecommunication wavelength 1550 nm is the InGaAs avalanche photodiode, which has been modeled in our work. Real single photon detectors have several limitations, including dark counts, time jitter, afterpulsing, limited quantum efficiency, lack of ability of photon number resolution etc.

The two PBS's, the half-wave plate and the 4 SPDs "measure" the received photons. In Fig. 3, the upper PBS and the two associated SPDs measure the photons transmitted by the BS in the rectilinear basis. The half-wave plate, the lower PBS and the two associated SPDs measure the photons reflected by the BS in the diagonal basis. The detections in the SPDs determine the outcomes of the measurements.

V. System Parameters and Performance Measures

Three system parameters – the mean photon number (MPN) of the weak coherent pulses, the optical fiber length and the dark count probability of the avalanche photodiodes – are varied in the simulation to observe their effects on the system performance. Several quantities can be used to characterize the system performance, such as the quantum bit error rate (QBER) of the sifted key, the signal gain, the sifted key generation rate etc.

QBER of the sifted key

$$= \frac{\text{Number of correct bits in the sifted key}}{\text{Total number of bits in the sifted key}} \quad (14)$$

Signal gain

$$= \frac{\text{No. of Bob's sifted signal detections}}{\text{No. of Alice's classical signal pulses sent}} \quad (15)$$

The sifted key generation rate is the number of bits in the sifted key generated per unit time. For example, if the sifted key generation rate is 100 kbps, then 100×10^3 bits is obtained in the sifted key in 1 second.

VI. Simulation Results

The entire experimental setup was simulated several times with a certain number of optical pulses generated (e.g. 10^6) in each run. The simulation was performed with MATLAB. The mean photon number, the optical fiber length and the dark count probability of the avalanche photodiodes were varied separately, and their effects on the signal gain, quantum bit error rate (QBER) and the sifted key generation rate were observed. The results are shown in figures 7-12.

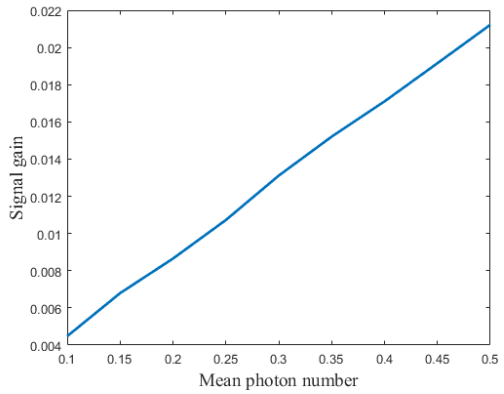

Fig. 7. Signal gain vs. mean photon number

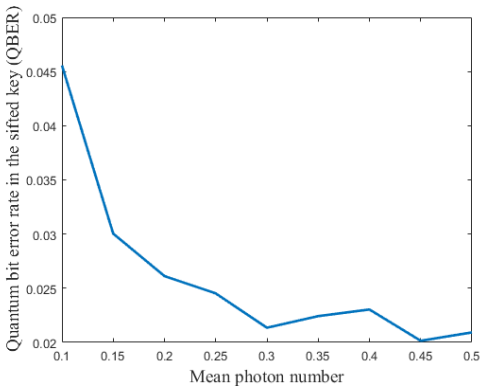

Fig. 8. Quantum bit error rate of the sifted key vs. mean photon number

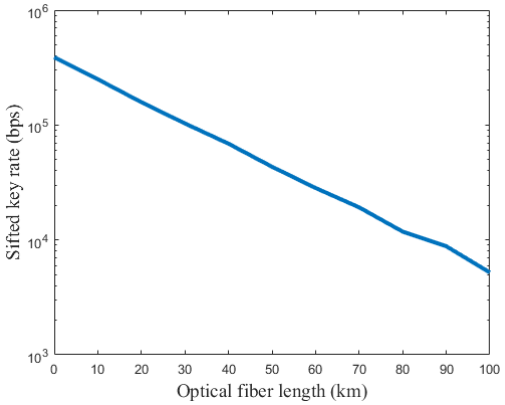

Fig. 9. Sifted key generation rate vs. optical fiber length

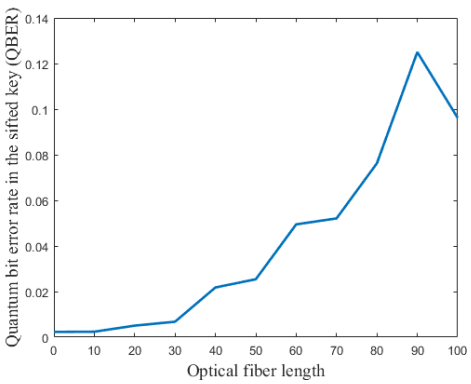

Fig. 10. Quantum bit error rate of the sifted key vs. optical fiber length

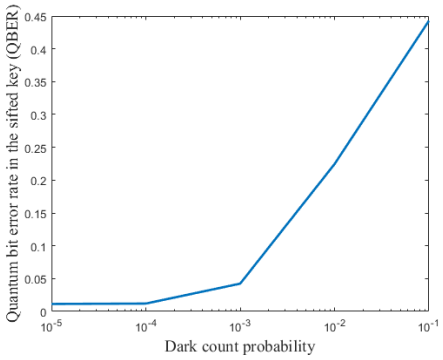

Fig. 11. Quantum bit error rate of the sifted key vs. dark count probability

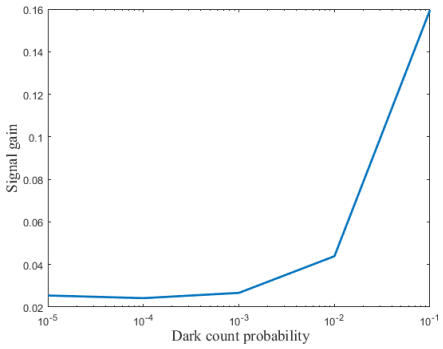

Fig. 12. Signal gain vs. dark count probability

From figures 7 and 8, it is seen that the signal gain increases with the mean photon number, and the QBER decreases, which is expected. Increasing the mean photon number increases the number of non-empty weak coherent pulses and thus the number of pulses received by Bob and so the number of sifted signal detections increases. This increases the signal gain.

Figure 9 shows that the sifted key rate decreases with the increase in optical fiber length. A longer optical fiber results in greater attenuation of the transmitted pulses, and the number of pulses detected by Bob decreases. This causes a reduction in the sifted key rate. Increasing the optical fiber length also increases the change of the polarization states of the photons, which leads to more errors, and thus increases the QBER, as shown in figure 10.

Figure 11 and 12 depict that the QBER and the signal gain increase with the increase in dark count probability. If the dark count probability of the avalanche photodiodes increases, the number of erroneous dark count detections at Bob's module increases, which in turn decreases the message match rate between Alice and Bob before sifting and increases the QBER of the sifted message. Since increased dark count detections increase the number of sifted message bits, so the signal gain also increases with the increase in dark count probability, albeit with more errors in the sifted message. The highest acceptable dark count probability for this experimental setup is about 10^{-3}, above which the QBER increases to unacceptable levels (the maximum theoretical upper limit of QBER for secure key generation is about 11% when privacy amplification and one-way error correction are applied and about 20% when privacy amplification and two-way error correction are used [13], [14], [10]).

VII. Conclusion

The simulation results show the effects of some non-ideal conditions on the performance of a real QKD system, and these effects are realistic and expected. The non-ideal behavior of the system as found in the simulation closely resemble the real-life behavior of the system. Thus, the simulator can reliably simulate a real QKD system and can be used to estimate the performance of the system. The simulator can also be modified to simulate other QKD systems with different QKD protocols. Further research can be done to include more non-ideal factors of the devices used in different QKD systems to make the simulation more accurate.

References

[1] S. Wiesner, "Conjugate Coding," *ACM SIGACT News - A special issue on cryptography,* vol. 15, no. 1, pp. 78-88, 1983.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, 1984.

[3] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.,* vol. 68, no. 21, pp. 3121-3124, 1992.

[4] C. H. Bennett, G. Brassard and A. Ekert, "Quantum cryptography," *Scientific Am.,* no. (int. ed.), pp. 26-33, 1992.

[5] Y. Mu, J. Seberry and Y. Zheng, "Shared cryptographic bits via quantized quadrature phase amplitudes of light," *Optics Communications,* vol. 123, no. 1-3, pp. 344-352, 1996.

[6] C. Branciard, N. Gisin, B. Kraus and V. Scarani, "Security of two quantum cryptography protocols using the same four qubit states," *Phys. Rev. A,* vol. 72, no. 3, p. 032301, 2005.

[7] M. M. Khan, M. Murphy and A. Beige, "High error-rate quantum key distribution for long-distance communication," *New Journal of Physics,* vol. 11, no. 6, p. 063043, 2009.

[8] H. -K. Lo, X. Ma and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.,* vol. 94, no. 3, p. 230504, 2005.

[9] W. Wootters and W. Zurek, "A Single Quantum Cannot be Cloned," *Nature,* no. 299, pp. 802-803, 1982.

[10] P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.,* vol. 85, no. 2, pp. 441-444, 2000.

[11] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography," *Rev. Modern Phys.,* vol. 74, no. 1, p. 12, 2002.

[12] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature Photon.,* vol. 3, p. 698, 2009.

[13] K. Tamaki, M. Koashi and N. Imoto, "Unconditionally Secure Key Distribution Based on Two Nonorthogonal States," *Phys. Rev. Lett.,* vol. 90, no. 16, p. 167904, 2003.

[14] D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, "Security of Quantum Key Distribution with Imperfect Devices," *Quantum Inf. Comp.,* vol. 4, no. 5, pp. 325-360, 2004.

[15] T. F. d. Silva, G. B. Xavier and J. P. v. d. Weid, "Real-Time Characterization of Gated-Mode Single-Photon Detectors," *IEEE Journal of Quantum Electronics,* vol. 47, no. 9, pp. 1251 - 1256, 2011.