www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 9, September 2014 Page No. 8460-8468

Performance Evaluation of Secure Key Distribution Based on Quantum Mechanics Principles Over Free Space.

Lawal Muhammad Aminu[1]
[1]Umaru Musa Yar'adua University,Faculty of Natural and Applied Science,Department of Mathematics and computer Science,
Dutsima Road, Katsina P.M.B 2218, Nigeria
ameenuida@yahoo.*com*

Abstract: ***Quantum key distribution (QKD) provides a perfectly secure coding method which solves the problem of key distribution, it is currently the most mature application in the field of quantum computing. Performance analysis is very important in determining the effectiveness of various QKD protocols. However, Lack of effective simulation tools for evaluating QKD protocols over free space results to use of Analytical (theoretical) and experimental (real equipments) for evaluation, the later is inaccurate while the former is expensive. Optisystem 7.0, a commercial photonic simulator which is widely used in telecommunication was used in modeling and simulating BB84,B92 and Six State QKD protocols. The simulation model emphasizes on the experimental components of quantum key distribution. Results obtained based on the sifted key rate and failure rate shows that Six state protocol has a low sifted key rate and high failure rate which are identical to results from experiments. Lack of detector implementation and assumption of the single photon reduces the accuracy of the results. The simulation can help researchers to test their models before performing experiments.***

Keywords: Quantum key distribution**,** Free Space Optics, Optisystem

1. Introduction

Free Space Optics (FSO) Technology is another transportation technology to link high capacity networking segment [1].It is also a contender to complement current transportation technology because of its cost-effectiveness and high-bandwidth qualities, its significant responsibility or purpose would go a long way in stirring on secure key distribution used in encryption, which is vital for all aspects of telecommunications, networking and its application in Quantum Key Distribution (QKD) [2].

1.1 Quantum key distribution

Quantum key distribution (QKD), widely termed as quantum cryptography provides a perfectly secure coding method which solves the problem of key distribution, it is currently the most mature application in the field of quantum computing [3]. Quantum key distribution (QKD) exploits the fundamental principles of quantum mechanics. First of these principles is the Heisenberg's uncertainty principle which states that one cannot completely determine an unknown quantum state without disturbing it. The second principle is the no-cloning theorem according to which a quantum state cannot be copied [4]. Any attempt to copy will result in the destruction of the original quantum state. These two principles form the basis of all the quantum key distribution protocols and are the key to the major contribution of these protocols, which is the ability to detect any eavesdropping on the channel.

The fundamental model for QKD protocols involves two parties, referred to as Alice and Bob, wishing to exchange a key both with access to a classical public communication channel and a quantum communication channel. This is shown in figure 1. An eavesdropper, called Eve, is assumed to have access to both channels and no assumptions are made about the resources at her disposal. [5]

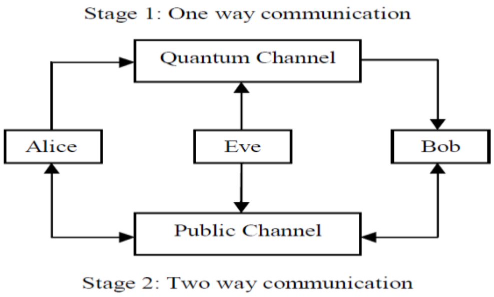

Stage 1: One way communication
Quantum Channel
Alice
Eve
Bob
Public Channel
Stage 2: Two way communication

Figure 1: Model of Quantum Key Distribution communications

In 1984 Charles Bennett and Gilles Brassard published the first QKD protocol [6]. It was based on Heisenberg's Uncertainty Principle and is simply known as the BB84 protocol after the authors' names and the year in which it was published. It is still one of the most important protocols .The fundamental concept for all of this protocol is that Alice can transmit a random secret key to Bob by sending a string of photons where the secret key's bits are encoded in the polarization of the photons. Heisenberg's Uncertainty Principle can be used to guarantee that an Eavesdropper cannot measure these photons and transmit them on to Bob without disturbing the photon's state in a noticeable way thus revealing her existence.

1.2 Description of BB84 Protocol

Figure 2 shows the basis of how a bit can be encoded in the polarization state of a photon in BB84. Binary 0 is characterized as a polarization of 0 Degree in the rectilinear bases or 45 degrees in the diagonal bases [7] [8]. Similarly a binary 1 can be 90 degrees in the rectilinear bases or 135 in diagonal bases. Thus a bit can be represented by polarizing the photon in either one of two bases.

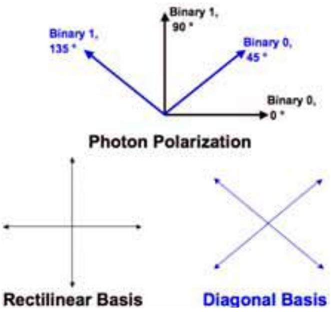
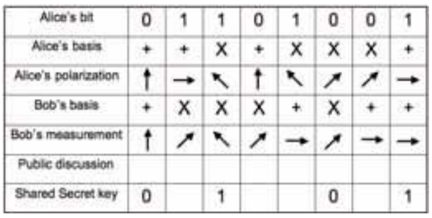


Figure 2: Polarization Basis

In the first stage, Alice will communicate to Bob over a quantum channel. Alice begins by choosing a random string of bits and for each bit, Alice will randomly choose a basis, rectilinear or diagonal, by which to encode the bit. She will transmit a photon for each bit with the corresponding polarization, as just described, to Bob. For every photon Bob receives, he will measure the photon's polarization by a randomly chosen basis. If, for a particular photon, Bob chose the same basis as Alice, then in principle, Bob should measure the same polarization and thus he can correctly deduce the bit that Alice planned to send. If he chose the wrong basis, his result, and thus the bit he reads, will be wrong. In the second stage, Bob will notify Alice over any insecure channel what basis he used to measure each photon. Alice will report back to Bob whether he chose the correct basis for each photon. At this point Alice and Bob will discard the bits corresponding to the photons which Bob measured with a different basis. Provided no errors occurred or no one manipulated the photons, Bob and Alice should now both have an identical string of bits which is called a sifted key. The example below shows the bits Alice chose, the bases she encoded them in, the bases Bob used for measurement, and the resulting sifted key after Bob and Alice discarded their bits as just mentioned [9].



Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Figure 3: Sifted Keys

Prior to the end, Alice and Bob agree upon a random subset of the bits to compare to ensure consistency. If the bits agree, they are discarded and the remaining bits form the shared secret key. In the absence of noise or any other measurement error, a disagreement in any of the bits compared would indicate the presence of an eavesdropper on the quantum channel. This is because the eavesdropper, Eve, were attempting to determine the key, she would have no choice but to measure the photons sent by Alice before sending them on to Bob. This is true because the no cloning theorem assures that she cannot replicate a particle of unknown state [4]. Since Eve will not know what bases Alice used to encoded the bit until after Alice and Bob discuss their measurements, Eve will be forced to guess. If she measures on the incorrect bases, the Heisenberg Uncertainty Principle ensures that the information encoded on the other bases is now lost. Thus when the photon reaches Bob, his measurement will now be random and he will read a bit incorrectly 50% of the time. Given that Eve will choose the measurement basis incorrectly on average 50% of the time, 25% of Bob's measured bits will differ from Alice [10]. The chance that an eavesdropper learned the secret is thus negligible if sufficiently long sequences of the bits are compared.

1.3 Free space QKD

Free space QKD was first demonstrated in 1989 by Bennett and his co-workers over 30 cm optical link [11]. The first experimental implementation of QKD was proposed in [12], since then a lot of research effort has been dedicated by researchers to develop the technology for use in future optical communication systems, to support security critical information flows. While the experimental setup was able to send quantum signal over distances of 100 km [13] in optical fiber link, in free-space quantum signal was sent over a distance of 23.3 km [14]. Recently, advances have led to demonstrations of QKD over point-to-point optical links [13][15][16]. These rather promising transmission distances have stressed the high possibility of obtaining practical QKD systems. In order to implement QKD between any two locations on the globe, a satellite is needed to be used as a secure relay station. Feasibility studies by researchers have shown that the ground-to-satellite, satellite-to-ground and satellite-to-satellite QKD demonstrations are feasible[17][18].In [19] a stratospheric quantum communication model based on the characteristics of the stratosphere was proposed. Besides, a study by [20] on the effect of turbulence on a quantum key distribution system can be found in [21]. Moreover, to improve the transmission bit rate of free space systems, two authors conducted a study on quantum key distribution by free-space MIMO system [20].Furthermore, to evaluate the performance of various QKD systems, the *QBER* and secure communication rate are considered as important criterion [13].

The *QBER* which is indicative of the security and post-error-correction communication key rate is taken in to account when evaluating the link performance. Any information learnt by an unauthorized third party about the exchanged key leads to an increase in the *QBER*. A high *QBER* enables an unauthorized user or more correctly the eavesdropper to learn more information about the transmitted key at the expense of the legitimate recipient. Thus, it should be taken in to account that obtaining high *QBER* values in QKD systems can resultantly lower the secure communication key rate during error correction stage of the protocol. It has been shown that, as long as the *QBER* of the sifted key is below a certain threshold, Alice and Bob can still distill a secure key by means of classical error correction and privacy amplification. Besides, past studies have shown that any *QBERs* of the sifted key above 15 % give room for an eavesdropper to actually learn more information than the intended recipient. When the obtained *QBER* is more than 15 %, no form of classical privacy amplification techniques can be used effectively[22].Thus, any proper design a QKD link should ensure a baseline *QBER* of below 15 % threshold if privacy amplification strategies are to be used to eliminate any knowledge gained by the eavesdropper. If the *QBER* goes above 15% limit value, depending on the restrictions on the eavesdropper's abilities, it will no longer be possible to extract as secure communication bit rate. This baseline *QBER* considers a QKD link in which a one-way classical processing by Alice and Bob is observed.

2 Related work

Quantum Key Distribution is a combination of both hardware and protocols used in achieving unconditional security in key distribution. Most simulation studies concentrate on implementing the software aspect of it.

Qcircuit [41] is a general purpose quantum circuit designer and simulator program. it was developed to design and test quantum algorithms and communication protocols. Qcircuit has the quantum circuit interface with various objects to denote the QKD elements. Quantum circuits are the most general forms of defining quantum algorithms.

Object-Oriented Quantum Cryptography Simulation Model was proposed in [42]. it consist of five layers which can be develop on java platform. The framework can be utilized for quantum computation as well as classical and quantum cryptography.

Event-by-Event Simulation of Quantum Cryptography Protocols was proposed in [43] .it present a new approach to simulate quantum cryptography protocols using event-based processes. The main feature of this approach is that it simulates the transmission of the individual bits by an event-based process .The algorithm that generates the events does not solve any quantum mechanical equation, thereby circumventing the fundamental problems arising from the quantum measurement paradox.

Quantum Cryptography Protocol Simulator proposed in [44] presented a C++ application to evaluate and test quantum cryptography protocols. This application has elegant user-friendly interface and many modules which complete entire QKD operations. It includes BB84 and B92 as a protocol option; two modules for eavesdropping; a noise level module; and privacy amplification. This simulation is suited for understanding overall QKD operations.

QCrypt (A Quantum Cryptography Simulation) , a java based simulator is used in [2]. This software is a practical working model of a QKD system, which implements the BB84 protocol for quantum cryptography involving distribution of information over a quantum channel. The software allows the user to simulate the QKD BB84 protocol and investigate impact of channel efficiency and QKD attacks in order to determine various types of keys.

Charles Bennett and Gilles Brassard [6] invented Quantum Key Distribution in 1984 , based on an earlier idea of unforgeable quantum money by Stephen Wiesner which dates back to the early 1970s although was published a decade later [23], it provides a substitute way out to the key establishment problem. Secret keys in QKD are created in process of key distribution, unlike in classical key distribution where keys are predetermined before distribution. The most significant contribution of quantum cryptography is the detection of eavesdropping. Neither classical cryptography nor public key cryptography has such a capability.

2.1 QKD Protocols

The clear number of QKD protocols is nearly countless following the discovery of Bennett that security can be gained when coding a bit in two non-orthogonal quantum states[24]. The quantum key distribution protocols can be classified into two major categories:
1) Prepare and Measure protocols and
2) Entanglement based protocols.
However, this idea has variety of possibilities which can be further grouped into three classes
i. Discrete-variable coding
ii.Continuous variable coding
iii. Distributed phase-reference coding.

The vital difference is the detection scheme, discrete variable coding and Distributed phase reference coding utilize photon counting and post-select the events in which a detection has effectively been done, while continuous-variable coding utilizes homodyne detection[25].

Discrete-variable coding is the original one. Its major gain is that protocols can be designed such that non existence of errors will allow Alice and Bob to distribute perfect secret key instantly. Most implementation of QKD protocols is based on discrete-variable protocol. Any discrete quantum degree of freedom can be selected in principle, however, a good number of the commonly utilized are polarization for free-space implementations and phase-coding in fiber-based implementations [25].

Continuous-variable coding originates from the study that photon counters usually characterized with low quantum efficiencies, high dark count rates, and rather long dead times, Even as these shortcomings can be solved by employing homodyne detection, the downside is that the protocol provides Alice and Bob with correlated but relatively noisy realization of a continuous random variable, because losses transforms into noise as a result, an important amount of error correction measures must be employed. The trade off is between building up a slow noiseless raw key, or a fast noisy one[25].

Distributed-phase-reference coding stems from the attempt of some experimental groups to bring about realistic practical implementation detection wise. These protocols generate a discrete valued result although the characteristics of the quantum signals is very unlike from the case of discrete-variable protocols which requires , and this prompts further treatment[25].

However, the scope of this project is on the discrete variable coding, protocols under this class are further reviewed below.

2.2 Prepare and Measure Protocols

2.2.1 BB84 Protocol

This protocol was proposed by Bennett et al. [6] and marked the beginning of quantum cryptography. The quantum communication stage encodes the bit in the polarization of the photon. Mathematically, the polarization states of photon are represented by the elements of a two dimensional Hilbert space H. Two unlike orthogonal bases of H are selected by Alice e.g. the linear polarization basis + and the diagonal polarization basis x. Note that the two bases are non-orthogonal with each other. The two states $|0\rangle$ and $|0\rangle x$ represent the bit '0' and the other two states $|1\rangle$ and $|1\rangle x$ represent the bit '1'.Alice, selects at random one out of four states for polarized photons and sends it to Bob. Bob cannot differentiate explicitly among the four states as he does not knowledge of the basis in which Alice encodes the bit. For that reason, he measures randomly along one of the two measurement bases and gets a decisive result in half the cases. When his basis match to Alice's, bits should be perfectly correlated with hers, whereas when his basis is the conjugate, there is no correlation between his result and Alice's original choice. In the second phase, classical communication, Alice and Bob discuss over a public channel and discard all the instances where they did not use the same basis (half of the total on average). The result is called the sifted key, which should be two perfectly correlated strings, but which may contain errors due to Eve's eavesdropping. Alice and Bob can see whether the exchanged key has been eavesdropped by checking if it has been disturbed. In the absence of noise, any discrepancy between Alice's and Bob's raw keys is proof of Eve's intrusion. So to detect Eve, Alice and Bob select a publicly agreed upon random subset of *n* bit locations in the raw key, and publicly compare corresponding bits, making sure to discard from raw key each bit as it is revealed. Should at least one comparison reveal an inconsistency, then Eve's eavesdropping has been detected, in which case the protocol has to be started over again.

2.2.2 B92 Protocol

B92 protocol was proposed by Bennet in 1992 and uses two non orthogonal states in comparison with the four-state BB84 protocol [24]. Alice chooses between only two non-orthogonal states, and sends one to Bob. As the states are not orthogonal, Bob cannot always get a conclusive result. However, by using a measurement called positive operator valued measure or POVM, he can perform a test which will sometimes fail to give an answer, and at all other times give the correct one. In essence, instead of having a binary test (with results 0 or 1), Bob has a ternary system, with possible results: 0, 1, or inconclusive result. For example, if Alice sends a 0, Bob may get either a 0 or an inconclusive result, but he will never get a 1.

2.2.3 Six- State protocol

This protocol was proposed by Brub [26] and is a generalization of the BB84 protocol to six states. The working of the protocol is exactly the same as BB84 protocol with Alice now sending one of the six polarization states. The interest of this protocol lies in the fact that the channel estimation becomes "tomographically complete", that is, the measured parameters completely characterize the channel.

2.2.4 SARG04 Protocol

The SARG04 protocol was proposed by Sacarani et al. in 2004 primarily to overcome the PNS attacks [27]. It is a four state protocol with the quantum phase identical to BB84 protocol. The only difference which makes it resilient to PNS attacks is the difference in encoding and decoding of the classical information bits. The two states $|0\rangle$ and $|1\rangle$ represent the bit '0' and the other two states $|0\rangle x$ and $|1\rangle x$ represent the bit '1'.Alice sends one of the four states to Bob who measures in either of the two bases. In classical communication, Alice does not reveal the basis to Bob as this would reveal the bit with certainty. She discloses the state she has sent and one of the states of the other value of the bit, which is not orthogonal to the first one. Thus Alice can send one of the following sets S11 = $\{|1\rangle , |1\rangle x \}$, S00 = $\{|0\rangle , |0\rangle x \}$, S10= $\{|1\rangle , |0\rangle x \}$ S01 = $\{|0\rangle , |1\rangle x \}$.Bob gets the correct bit if he measured in the correct basis. An error can only happen if the state has been modified by an eavesdropper. In the absence of any errors, the length of the sifted key is ¼ of the original key.

2.2.5 Decoy State Protocol

Decoy state protocol was also proposed as a solution to the PNS attacks on BB84 protocol [28]. It makes use of the fact, that under the PNS attacks, the number of multi-photon pulses received by Bob will be higher than single photon pulses as Eve blocks the single photon pulses. The sender, Alice, intentionally replaces the signal pulses by multi-photon pulses at random locations which serve as decoy states. Since Eve cannot distinguish multi-photon pulses of signal source from those of decoy source, eavesdropping can be detected. Thus the PNS attack can be detected by checking decoy source states. The protocol is aborted if the decoy state are found to be higher than that of other signal pulses. Another important advantage is that decoy state QKD results in larger distance and key generation rate compared to non-decoy protocols [16].

2.2.6 4+2 Protocol

The 4+2 protocol proposed by [40]. combines the advantages of the four state BB84 protocol and the two state B92 protocol [29]. The basic idea is that instead of using two orthonormal bases, two non-orthogonal bases should be used in BB84 protocol. This will make eavesdropping more difficult. The authors also show that the technique is resilient to lossy transmission line as with B92 protocol because of the use of phase encoding compared with polarization used in BB84 protocol. The use of phase encoding offers advantage in eavesdropping detection even when weak pulses containing multiple photons are used.

2.3 Entanglement Based Protocols

It is imperative to first describe the motivation behind entanglement based protocols. In this section, we first explore the question of why entanglement is useful and then proceed on to describe the protocols. As described in the previous section, true single photon sources are difficult to realize experimentally and faint laser pulses are vulnerable to photon number splitting attacks (PNS). The use of entanglement in protocols provides a superior approach to quantum cryptography and was first proposed by Ekert [30]. One of the main conceptual advantages over singlephoton quantum cryptography is the inherent randomness in the results of a quantum-mechanical measurement on an entangled system leading to purely random keys.

Furthermore, the use of entangled pairs eliminates the need for deterministic single photon source, because a pure entangled photon state consists, by definition, of exactly two photons that are sent to different recipients. Multiple-pair emissions are inherently rejected by the protocol, in contrast to the faint pulse case, where a beam splitting attack might be successful. Additionally, high intensity sources would allow longer transmission paths compared to single-photon based systems Moreover, entanglement based QKD offers the advantage that eavesdropping attacks based on multi-photon pulses do not apply in entanglement-based QKD. However, multiphoton pulses lead to errors at Bob, who detects from time to time a photon that is not correlated to Alice's [31]. The creation and transmission over long distances of EPR correlated pairs is technologically more difficult, and it is not clear yet whether this will prove practical [32].

2.3.1 Ekert91 Protocol

The Ekert91 protocol is based on the creation of pairs of EPR correlated photons [30]. A source generates an EPR pair of photons and transmits one photon to Alice and the other to Bob. Alice and Bob both randomly choose a measurement basis and perform the measurements. In the classical communication phase, they compare the measurements and keep the bits in which both had used the same basis and discard the rest. Note, that in the measurements where both Alice and Bob used the same basis, their bit results will be perfectly anti-correlated because of the entanglement properties. The efficiency of EPR protocol is 25% as 50% of the distributed bits are spent on basis negotiation and another 50% are then used in the public discussion for the purpose of eavesdropping detection.

3 Methodology

3.1 Introduction

Experiments in [12],[33],[17],[34],[35],[36] showed that long range QKD is possible on both optical fiber and air medium (FSO), and that either or both mediums can be used depending on the application [2].

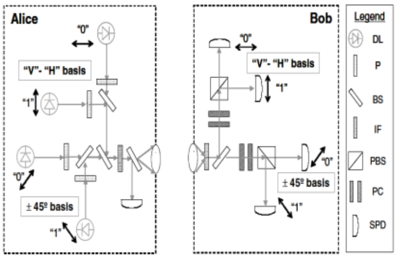


Figure 4: Experimental Setup of QKD

Legend
Data lasers(DL),Linear polarizers (P), Beamsplitters(BS), Polarization controller
(PC),Polarizing beamsplitter (PBS), Interference filter(IF) , Single-photon detectors(SPD).

To evaluate QKD over free space a simulation tool called optisystem is used. OptiSystem™ 7.0 [37] software offers a range photonic telecom components for optical communication modeling and simulation, although the inbuilt components are not in tandem with QKD operation. In modeling QKD experiments using the OptiSystem™ , the telecommunication experimental paradigm which consists of transmitter ,channel and receiver is emulated in relation to QKD experimental setup [38].The QKD set up is divided into these blocks as shown below,

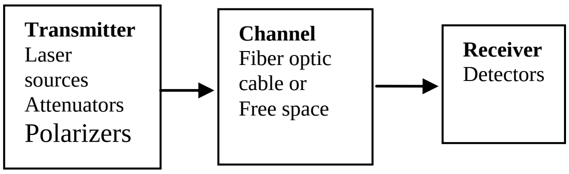


Figure 5: QKD experimental components

3.2 Transmitter Module

Optical Source: OptiSystem provides wide variety of transmitter components for QKD. Most of the components and its features can be utilized for experimental QKD setup . Broad range of components available for optical source laser like coherent wave (CW), light-emitting diode (LED) , pump laser, vertical-cavity surface emitting laser (VSCEL) and its variants, i.e. spatial and laser rate.

Passive Optical Components: Under the "passive library/optical" section, several components available ranges from attenuators, polarization, power combiners, isolators, couplers, circulator, power splitters and delay.

From the "Tools library," we have used fork, select and switch components. Particularly, we swapped experimental QKD vital component called the polarization beam splitter (PBS) with select and switch component. The role of select component is to choose one signal from many signals. Contrast to 'select', 'switch' chooses one of many outputs from one input. On other hand, component 'fork' play duplication of signal. This is used for customization of simulation [39].

3.3 Channel

Under the free space optics library, the FSO component is available. It provides the essential characteristics of free space like the Range between the transmitter and the receiver ,Attenuation, Geometrical loss, Transmitter aperture diameter, Receiver aperture diameter, Beam divergence, Transmitter loss, Receiver loss, Additional losses(atmospheric) and Propagation delay parameters can all be set[39].

3.4 Receiver

The vital component of receivers like photo detectors PIN and APD are provided in the simulator, but we have a synchronize problem with our proposed simulation models. Therefore, we have employed other inbuilt components; i.e. optical spectrum analyzer, polarization analyzer, polarization meter and optical time domain visualize under the "Visualizer" library. Thus, these components are covering the receiver module of our simulation models. However, this set up has a huge impact on the quantum bit error rate (QBER) and acts as an ideal detector [39].

3.5 Simulation Setup

Five sets of experiments on each protocol were conducted. Each set contains 100 iterations to 500 iterations over distance of 1 km to 10km. The data obtained is exported to excel worksheet for further calculations. All simulation models are assumed to be free of eavesdropping attack .Also, detector in the receiver module is considered be a perfect device. In QKD protocols, random selection of bases acts like the critical role, to achieve randomness in our simulation models. The simulator's inbuilt functions was utilized and the results were tested with the NIST test suite [49]. The results passed the frequency test.

Table 1: FSO Transmitter/Receiver Specifications

s/no	Parameter	Value
1	Wave length	1550nm
2	Transmit Power	28 dBm
3	Divergence angle	3 mrad
4	Transmit aperture diameter	0.2m
5	Receive aperture diameter	0.2m
6	Attenuation	0.1

3.6 BB84 simulation model

Simulation setup for BB84 comprises four CW source, four attenuator (0.1 attenuation to attain single photon) and four polarizer. The component 'select' act as polarization beam splitter and configured to choose randomly one of four polarization states on each iteration. On Bob's side, we designed the detector in a way to randomly choose to allow the signal or not. If detector shows signal strokes assumed right polarization base else wrong base[39].

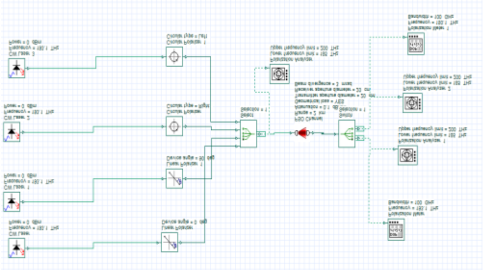


Figure 6: BB84 Simulation Model

3.7 B92 Simulation Model

B92 is a lighter version of BB84. This protocol uses only two states of polarization. The setup requirement is similar to the BB84 setup. In the receiver side, receiver needs to choose between one polarizer. Here, we implemented optical null as differentiation of polarizer. Optical null is equivalent to wrong polarizer. Fig.7 depicts the simulation model[39].

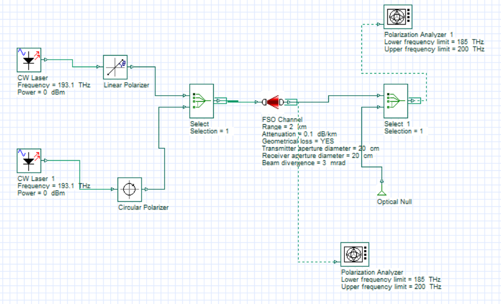


Figure 7: B92 Simulation Model

3.9 Six-state Simulation Model

Fig.8 represents six-state protocol, which applies three conjugate bases for the encoding, but it otherwise identical to the BB84 protocol. The probability for Alice and Bob choosing compatible bases is only 1/3. In our simulation setup, polarization rotator has used to cope with the sixth state. Receiver module is modified in a way each visualizer able to show the right polarization in case of correct base. This is done with help of polarization rotator component [39].

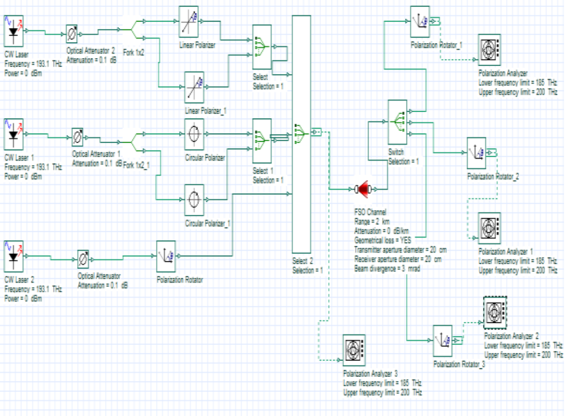


Figure 8:Six State Simulation Model

4 Results and Discussion

To determine the quality of the QKD link and to observe if the generated sifted key can produce secure key, the QBER is computed .It is the performance metric commonly considered, and it is defined as the ratio of the bits received in error to the total number of bits received. A QBER of less than 6% and a sifted key rate of 50% can be obtained in a realistic model without eve attack while less than 11% and a sifted key rate of 25% in the same model with eve attacks. Due to the assumptions made in the simulation setup the QBER is not used as performance criteria, However, in our simulation the performance metrics considered are

1. Sifted key rate which is the number of bits which Alice and Bob choose in common
2. The Failure rate which is the ratio of the wrong sifted bits to the total number of bits.

   These metrics also highlights the performance of the QKD set up.

In general the results of the simulation are superior to the experimental QKD because of the following reasons

1. The inclusion of a single photon source which is not available for experimental QKD. Normally, in QKD experiment, fain-laser is used with high attenuation to produce photons or qubits. Further, emission of photons is based on Poisson distribution. This distribution suffers photon-number splitting (PNS) attacks.
2. The omission of detector's issues. The experimental QKD detector suffers from issues like dark count, low efficiency. Thus, the omission of these factors gives better results in the simulation.

Figure 9 shows the sifted key rate of the BB84,B92 and six state over 100 to 500 iterations, the results show that the sifted key rate has a directly proportional relationship with the number of bits for all the simulated protocols. Six state protocol has the lowest sifted key rate compared to BB84 and B92.This is because Alice is sending one of the six polarization states which will translate 1/3 distribution rate as compared to ½ distribution rate for BB84 and B92.

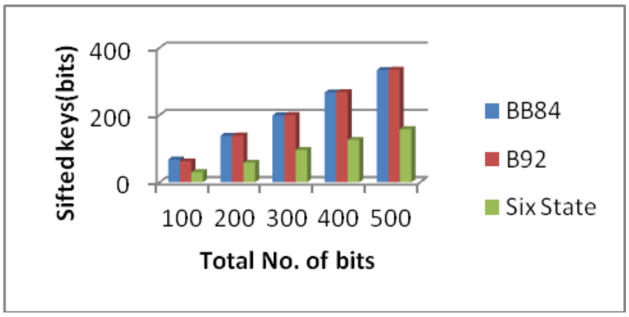


Figure 9: Sifted Key Distribution

Figure 10 shows the Failure rate of the simulated protocols versus the number of iterations. All the simulated have almost the same failure rate irrespective of the number of total number of bits which is 31% to 34% for BB84,31% to 35% for B92 and 56% to 57% for six state ,this is because of the sifted key distribution rate.Six state has the highest failure rate because of the same reason it has the lowest sifted key distribution rate.

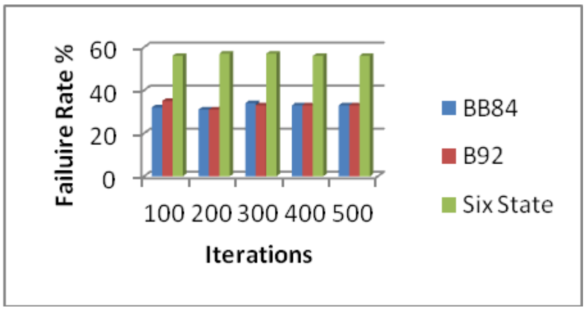


Figure 10: Failure Rate

Figure 11 shows the failure rate of the simulated protocols over distance. As already established from the previous results, all the protocols have the same failure rate irrespective of the total number of bits. With different distance the failure rate tends to increase with 8% to 9% because of losses due to atmospheric conditions, power loss and geometric loss. The power of the signal becomes weak to around -100 dBm, hence the photon cannot be detected thereby contributing to increase in failure rate.

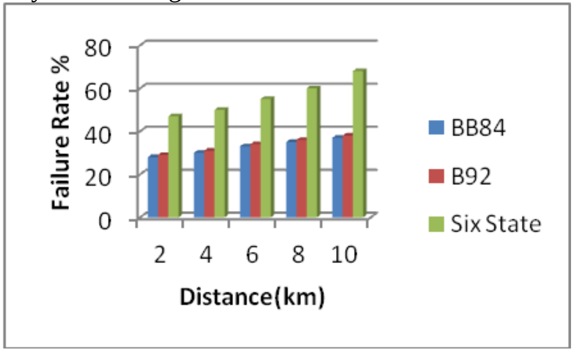


Figure 11: Failure rate with varying Distance

5 Conclusion

Quantum key distribution has the potential to provide solution to key distribution problems in classical cryptography. It does not rely on the assumptions of most classical cryptographic protocols such as computational complexity of certain mathematical problems.

Simulation of QKD protocols (BB84, B92 and Six state) has successfully been carried out using Optisystem 7.0, the simulation focused on the experimental setup using the components available in Optisystem. This gives the true picture of QKD which is a combination of both hardware and protocols used in achieving unconditional security in key distribution. Results obtained shows that Six state protocol has a low sifted key rate and high failure rate which are identical to results from experiments. However, lack of detector implementation and ideal assumption of the single photon reduces the accuracy of the results. The simulation can help researchers to test their models before performing experiments.Modelling and simulating Entanglement based protocols is our future concern.

Author Profile

Lawal Muhammad Aminu received B.Eng in Electrical and Computer Engineering from Federal University of Technology Minna,Nigeria in 2007 and Master of Computer Science from Universiti Putra Malaysia in 2014.He is a Lecturer at Umaru Musa Yar'adua University.His research interest focus on Computer Networks.

References

[1] Carbonneau, T. H. And Wisely, D.R. (1998). Opportunities And Challenges For Optical Wireless; The Competitive Advantage Of Free Space Telecommunications Links In Today's Crowded Market Place. SPIE Conference On Optical Wireless Communications, 3232, 119-128, Dallas, TX.

[2] Alma Husagić-Selman, Wajdi Al-Khateeb And Suhairi Saharudin(2012). Feasibility Of QKD Over FSO Link, International Conference On Computer And Communication Engineering (ICCCE 2012), 3-5 July 2012, Kuala Lumpur, Malaysia.

[3]Etengu, R. Abbou, F. M. Wong, H.Y. Wong, H.Y. Nortiza, N. And Setharaman, A.(2010). Performance Comparison Of Bb84 And B92 Satellite-Based Free Space Quantum Optical Communication Systems In The Presence Of Channel Effects. International Journal Of Engineering And Mathematical Intelligence, Vol. 1 Nos. 1 & 3, 2010

[4] Wootters, W.K., And Zurek, W.H., "A Single Quantum Cannot Be Cloned", Nature 299 (1982), Pp. 802-803.

[5] Mobin Javed And Khurram Aziz.(2009). A Survey Of Quantum Key Distribution Protocols, Proceedings Of The 7th International Conference On Frontiers Of Information Technology, Abbottabad, Pakistan..

[6] Bennett, C. H. And Brassard, G., "Quantum Cryptography: Public Key Distribution And Coin Tossing.", International Conference On Computers, Systems & Signal

Processing, Bangalore, India, 10-12 December 1984, Pp. 175-179.

[7] The BB84 Quantum Coding Scheme", June 2001. Http://Www.Cki.Au.Dk/Experiment/Qrypto/Doc/Qucrypt/Bb84coding.Html

[8] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., "Quantum Cryptography", Reviews Of Modern Physics, Vol. 74, January 2002, Pp. 146 - 195.

[9] Wikipedia-SIFT: Http://En.Wikipedia.Org/Wiki/Quantum_Cryptography

[10] Rieffel, E., "An Introduction To Quantum Computing For Non-Physicists.", ACM Computing Surveys, Vol. 32, No. 3, Pp. 300-335., September 2000.

[11] Bennet C. H., Bessette F., Brassard G., Salvail L. And Smolin J. (1992). Experimental Quantum Cryptography. Journal Of Cryptology 5, 3-38.

[12] Ott E., Grebogi C. And York J. A. (1990). Controlling Chaos. Physical Review Lett. 64, 1996-1199.

[13] Buttler W. T., Hunhes R. J., Kwiat P. G., Lamoreaux S. K., Luther G. G., Et Al (1998). Practical Free-Space Quantum Key Distribution Over 1 Km. Physical Rev. Lett., 81 (15), 3283-3286.

[14] Hatcher M. (2003 June 5). Cryptography Beats 100 Km Barrier [Online]. Available At Http://Optics.Org/Articles/News/9/6/3/1.

[15] Rarity J. G., Gorman P. M. And Tapster P. R. (2001). Electronics Letter, 37 512.

[16] Kurtsiefer C., Zarda P., Halder M., Weinfurter H., Gorman P. M., Et Al (2002). Nature, 419, 450.

[17] Nordholt J. E., Hunghes J. E., Derkacs D. And Peterson C. G. (2002). Practical Free-Space Quantum Key Distribution Over 10 Km In Daylight And At Night. Los Alamos: Physics Division, Los Alamos National Laboratory.New Journal Of Physics, 4 43.1.

[18] Rarity J. G., Tapster P. R., Gorman P. M. And Knight P. (2002). New Journal Of Physics, 4 82.1.

[19] Zhiu, J. And Zeng G. (2005). Attenuation Of Quantum Optical Signal In Stratospheric Quantum Communication IEEE.

[20] Gabay, M. And Arnon, S. (2006). Quantum Key Distribution By A Free-Space MIMO System. Journal Of Light Technology, 24, 8.

[21] Gabay M., Arnon S., Zhiu S. J. And Zeng G. (2005). Effect Of Turbulence On A Quantum-Key Distribution Scheme Based On Transformation From The Polarization To The Time Domain: Laboratory Experiment. Optical Engineering 44 (4), 045002.

[22] Kumavor P. D., Beal A. C., Yelin S., Donkor E. And Wang B. C. (2005). Comparison Of Four Multi-User Quantum Key Distribuion Schemes Over Passive Optical Networks. Journal Of Light Wave Technology, 23, 1.

[23] Wiesner, S., "Conjugate Coding", Sigact News, Vol. 15, No. 1, 1983, Pp. 78 – 88

[24] Bennett, C.H., 1992, "Quantum Cryptography Using Any Two Nonorthogonal States" Phys. Rev. Lett. 68, 3121.

[25] Valerio Scarani , Helle Bechmann-Pasquinucci , Nicolas J. Cerf , Miloslav DuˇSek , Norbert L¨Utkenhaus ,Momtchil Peev The Security Of Practical Quantum Key Distribution. Rev. Mod. Phys. 81 , 1301–1350 (2009).

[26] Brub, D.,“Optimal Eavesdropping In Quantum Cryptography With Six States,” Physical Review Letters, Vol. 81, 1998, Pp. 3018

[27] Scarani, V., Acin, A., Ribordy, G., And Gisin, N., “Quantum Cryptography Protocols Robust Against Photon Number Splitting Attacks For Weak Laser Pulse Implementations”, Physical Review Letters, Vol. 92, 2004, Pp. 057901

[28] Hwang , W.Y., “Quantum Key Distribution With High Loss: Toward Global Secure Communication”, Physical Review Letters,Vol. 91, 2003, Pp. 057901

[29] Huttner, B., Imoto, N., Gisin, N., And Mor, T., Quantum Cryptography With Coherent States”, Physical Review Letters,Vol.51, 1995, Pp. 1863-1869

[30] Ekert, A. K., "Quantum Cryptography Based On Bell's Theorem", Physical Review Letters, Vol. 67, No. 6, 5 August 1991,Pp. 661 - 663.

[31] Marcikic, I., Reidmatten, H., Tittel, W., Scarani, V. , Zbinden, H., And Gisin, N. , Time-Bin Entangled Qubits For Quantum Communication Created By Femtosecond Pulses Physical Review Letters, Vol. A 66, No. 6 , 2002 , Pp. 062308-0623124.

[32] Ekert, A.K., Rarity, J.G., Tapster, P.R., And Palma, G.M., “Practical Quantum Cryptography Based On Two-Photon Interferometry ”, Physical Review Letters, Vol. 69, No. 9, 1992, Pp. 1293-1295.

[33] Buttler W. T. And Wisely, D. R. (2000). Daylight Quantum Key Distribution Over 1.6 Km. Los Alamos: Physics Division, Los Alamos National Laboratory.

[34] Kurtsiefer, C., Zarda, P., Halder, M., Gorman, Ph. M., Tapster, Paul R., Rarity, J. G. And Weinfurter, Harald (2002). Long Distance Free Space Quantum Cryptography. Proc. SPIE, 4917, 25-31, Quantum Optics In Computing And Communications. Ludwig-Maximilian University, Munich, Germany.

[35] Resch, K. J., Resch K., Lindenthal M., Blauensteiner B., Bhm H., Fedrizzi A., Kurtsiefer C., Poppe A., Schmitt-Manderbach T., Taraba M., Ursin R., Walther P., Weier H., Weinfurter H. And Zeilinger A. (2005). Distributing Entanglement And Single Photons Through An Intracity, Free-Space Quantum Channel. Optics Express, 13 (1), 202-209.

[36] Schmitt-Manderbach, Weier, H., Furst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, Ch., Rarity, J., Zeilinger, A., Weinfurter, H. (2007). Experimental Demonstration Of Free-Space Decoy-State Quantum Key Distribution Over 144 Km. Physical Review Letters, 98 (1), Pp.1- 6.

[37] Http://Www.Optiwave.Com/

[38] Abudhahir. Buhari, Zuriati. Ahmad Zukarnai, Shamala. K.Subramaniam, Hisham. Zainuddin, And Suhairi. Saharudin.(2012). BB84 And Noise Immune Quantum Key Distribution Protocols Simulation: An Approach Using Photonic Simulator, International Conference On Computer And Intelligent Systems (ICCIS’2012) & International Conference Of Electrical, Electronics, Instrumentation And Biomedical Engineering (ICEEIB’2012) Dec. 28-29, 2012 Bangkok (Thailand)

[39] Abudhahir. Buhari, Zuriati. Ahmad Zukarnai, Shamala. K.Subramaniam, Hisham. Zainuddin, And Suhairi. Saharudin.(2012), A Discrete Event Simulation Approach On Polarizedbased Quantum Key Distribution Protocols Usingoptisystem, (IJCSIS) International Journal Of Computer Science And Information Security,Vol. 10, No.12, 2012

[40] Huttner, B., Imoto, N., Gisin, N., And Mor, T., Quantum Cryptography With Coherent States", Physical Review Letters, Vol.51, 1995, Pp. 1863-1869

[41] A. Pereszlenyi, "Simulation Of Quantum Key Distribution With Noisy Channels."

[42] X. Zhang, Q. Wen, And F. Zhu, "Object-Oriented Quantum Cryptography Simulation Model," IEEE, Pp. 599-602.

[43] S. Zhao, And H. De Raedt, "Event-By-Event Simulation Of Quantum Cryptography Protocols," Journal Of Computational And Theoretical Nanoscience, Vol. 5, No. 4, 2008, Pp. 490-504.

[44] M. Niemiec, Ł. Romański, And M. Święty, "Quantum Cryptography Protocol Simulator," Multimedia Communications, Services And Security, 2011, Pp. 286-292.