4th International Conference on Science, Technology and Management
India International Centre, New Delhi (ICSTM-16)
15th May 2016, www.conferenceworld.in ISBN: 978-81-932074-8-2

BIT ERROR RATIO ANALYSIS OF A QKD SYSTEM HAVING MULTIPLE EAVESDROPPERS – REALIZATION USING QUANTUM PACKAGE FOR MATHEMATICA

K.Elampari[1], B.Ramakrishnan[2]

[1] *Department of Physics, S.T. Hindu College, Nagercoil, (India)*

[2]*Department of Computer Science, S.T. Hindu College, Nagercoil, (India)*

ABSTRACT

Cryptography plays a very important role in secure communication and almost all the cryptographic protocols exists today are based on computational complexity. Theoretically Quantum cryptography provides unconditional security based on the underlining quantum physical laws. But because of the limitations of technology, it is impossible to build the ideal system described in theory. For example, currently, the only practicable quantum particle that can be used in cryptography systems is the photon and the original QKD protocol required a single photon source. However, due to the limitation of technology, perfect single photon source is still far from practical and in case if multiple eavesdroppers are working on a QKD channel, and Alice has non-single photon source, the state changed by one eavesdropper may be restored by the next and so Bob has no way of catch-up the disturbances. Based on this idea, in this work, bit error rate is analysed for the simple BB84 protocol with multiple eavesdropping using the Quantum Package in Mathematica.

Keywords: Multiple Eavesdroppers, QKD Protocols, Quantum Cryptography, Quantum Package, Simulation.

I. INTRODUCTION

The secrecy of communication over a network usually involves using algorithms that have a key to encrypt and decrypt the information. In classical crypto systems, a secret key K1 is used to encrypt a plain text or message M into a cipher text or message C, sent over a non-secure classical communication channel and decrypted back into original form using a secret key K2.A key in this context typically means a string of ones and zeros. In a crypto system, conventionally, the sender is referred as Alice, the receiver as Bob and the code breaker is often referred to as an eavesdropper or Eve.

Efficient private key ciphers were developed in the 1970s, and the difficulty of establishing a shared secret key at a distance was solved by the invention of public-key cryptography. One of the most commonly used public-key encryption schemes today is the Rivest-Shamir-Adleman (RSA) scheme [1], the almost universal implementation of the public key system today.

II. WHY QUANTUM CRYPTOGRAPHY?

The security of public key cryptosystems is based on computational complexity. The security of the RSA scheme is actually based on the factorization of large integers (i.e.) based on the presumed difficulty of factoring a large product of two primes (a semiprime) into its two constituent primes. In spite of its elegance suffers from a major flaw. Whether factoring is "difficult" or not could never be proven. This implies that the existence of a fast algorithm for factorization cannot be ruled out. In addition, the discovery in 1994 by Peter Shor of a polynomial algorithm allowing fast factorization of integers with a quantum computer puts additional doubts on the nonexistence of a polynomial algorithm for classical computers. Similarly, all public-key cryptosystems rely on unproven assumptions for their security, which could themselves be weakened or suppressed by theoretical or practical advances. So far, no one has proved the existence of any one-way function with a trapdoor. In other words, the existence of secure asymmetric cryptosystems is not proven. This casts an intolerable threat on these cryptosystems.

A new major development in cryptography arrived in the form of quantum cryptography. Quantum cryptography (QC), or more precisely quantum key distribution (QKD) offers an alternative and elegant solution to the key distribution problem. A paper published by Charles Bennett and Gilles Brassard in 1984 [2] proposed a way to encode information onto photons and distribute a secret key to a distant recipient by sending these photons. The scheme is set up in such a way that the security of the key is based on laws of quantum physics. A fibre optic cable system or the free space may act as a quantum channel for key distribution and the public classical channel may be any way of transferring information.

The strength of quantum cryptography is its unconditional security. It allows two parties to establish a secret random key at a distance, without having to rely on any computational assumptions. Unlike conventional cryptography, in QC security is based on the fundamental law of quantum mechanics, namely the Heisenberg Uncertainty principle which states that 'it is not possible to measure the quantum state of any system without disturbing that system'. Thus information gain over a quantum state generally implies disturbance on the original quantum state. If an eavesdropper attempts to intercept the information through a quantum channel, a measurement is necessary on the signal states and the measurement always disturbs the original state of the signal. Thus if Alice and Bob wish to communicate secretly, they can detect the presence of an eavesdropper Eve by using cleverly chosen quantum states and testing them to check whether they were disturbed during transmission. The absence of disturbance assures Alice and Bob that Eve almost surely does not have any information about the transmitted quantum signals [3].

III. PRACTICAL DIFFICULTIES IN QC

A fundamental truth about QKD technology is that, because of the limitations of technology, it is impossible to build the ideal system described in theory. For example, currently, the only practicable quantum particle that can be used in cryptography systems is the photon and the original QKD protocol required a single photon source. However, due to the limitation of technology, perfect single photon source is still far from practical [4]. The proofs for QKD generally make a large number of idealized assumptions to describe the behaviour of the physical devices used to perform QKD, such as light sources and detectors. Since real physical devices are far

from ideal, these assumptions are usually not valid in experimental implementations of QKD [5]. For this reason, each QKD implementation is only an approximation of the ideal apparatus described in theory [3]. Because of the limitations, the theoretical concepts may fail in actual implementations. Therefore, researchers make effort in the development of a QKD modelling and simulation framework that will allow system implementation non-idealities to be included in the system analysis so their impact on overall system performance and security can be better understood [6].

QKD has been rigorously proved to be secure [7][8][9]. As long as quantum mechanics is a valid theory that correctly describes Nature, QKD itself can never be broken.

IV. QKD PROTOCOLS

Literature study shows that there are several QKD protocols available and as nearly any set of non-orthogonal signal states together with a set of non-commuting measurement devices will allow secure QKD [10]. The BB84 protocol is the first QKD protocol. These protocols differ, however, in their symmetry that simplifies the security analysis, in the ease of their experimental realization and in their tolerance to channel noise and loss. Independent of Bennett and Brassard's work, Ekert proposed a QKD protocol (Ekert 91) based on Bell's inequalities [11] . In 1992, Bennett proposed a simple protocol (B92) [12] that involves only two non-orthogonal states. A protocol of particularly high symmetry is the six-state protocol [13].

V. ERROR STATISTICS

During the key distribution between Alice and Bob, error could have occurred even without eavesdropping because of channel, source and detector characteristics. Error correction allows Alice and Bob to determine all the "error bits" among their shared, sifted bits, and correct them so that Alice and Bob share the same sequence of error-corrected bits. Error bits are ones that Alice transmitted as a 0 but Bob received as a 1, or vice versa. These bit errors can be caused by noise or by eavesdropping. Optical quantum cryptography is based on the use of single photon Fock states. Unfortunately, these states are difficult to realize experimentally. Now a days, practical implementations rely on faint laser pulses or entangled photon pairs, where both the photon as well as the photon-pair number distribution obeys Poisson statistics. Hence, both possibilities suffer from a small probability of generating more than one photon or photon pair at the same time. Even small fractions of these multi-photons can have important consequences on the security of the key [14].

In case if multiple eavesdroppers are working, and Alice has non-single photon source, the state changed by one eavesdropper may be restored by the next and so Bob has no way of catch-up the disturbances. Based on this idea, in this work, bit error rate is analysed for the simple BB84 protocol with multiple eavesdropping using the Quantum Package in Mathematica.

VI. DESCRIPTION OF BB84

The basic idea in QKD is that Alice generates a sequence of truly random bits, each with a value zero or one, code the information into single photons and transmit these photons to Bob. Bits encoded in a quantum mechanic way is referred to as a quantum bit or qubit. Alice sends a large number of single photons to Bob

through the quantum channel. For each one, Alice picks from choice of four equally –likely random polarization states (Table 1).

Table 1. Qubits and Polarization States

Qubits	States
$\|\rightarrow\rangle$	Horizontal (H)
$\|\uparrow\rangle$	Vertical (V)
$\|\nwarrow\|$	Diagonal ($+45^o$)
$\|\nearrow\|$	Anti-diagonal (-45^o)

Alice encodes each photon with one these states and sends it to Bob. Each polarization state represents a bit value: V and +45 represent bit value 1, H and -45 represent bit value 0. The states representing each bit are non orthogonal.

$$|\nearrow| = \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\uparrow\rangle) \text{ and}$$
$$|\nwarrow| = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle) \quad (1)$$

For each arriving photon, Bob randomly chooses one of two possible measurement bases: rectilinear basis + = {H,V} or the diagonal basis x ={$+45^o$,-45^o}. Bob has four single-photon detectors, two for each basis. One of them will click depending on the basic choice and polarization of the incoming state. If Bob used the same basis as Alice, he should measure the state Alice sent. If Bob used the wrong basis, one of the two detectors in that basis would click randomly with 50% probability. Each detector in each basis represent a bit value, either 1 or 0, corresponding to the encoding of the incoming photons. As photons arrive and detectors click, a string of 1s and 0s is formed which constitutes the raw key. Table 2 demonstrates the sifted key construction.

Table 2. Sifted Key Construction

Alice Bit value	1	0	0	1	1	0	1	0
Alice State	$\uparrow$	$\rightarrow$	$\nwarrow$	$\nearrow$	$\uparrow$	$\rightarrow$	$\uparrow$	$\nwarrow$
Bob Basis	+	X	X	X	X	+	X	X
Raw Key	1	0	0	1	1	0	1	0
Basis Matched?	Y	N	Y	y	N	Y	N	Y
Sifted Key	1		0	1		0		0

Since no measurement operator of '+' is compatible with any measurement operator of 'x', it follows from the Heisenberg uncertainty principle that no one, not even Bob or Eve, can receive Alice's transmission with an accuracy greater than 75% [15].

This can be seen as follows. For each bit transmitted by Alice, one can choose a measurement operator compatible with either + or x, but not both. Because of incompatibility, there is no simultaneous measurement operator for both + and x. Since one has no knowledge of Alice's secret choice of quantum state, 50% of the time (i.e., with probability 1/2) one will guess correctly, i.e., choose a measurement operator compatible with Alice's choice, and 50% of the time (i.e., with probability 1/2) one will guess incorrectly. If one guesses correctly, then Alice's transmitted bit is received with probability 1. On the other hand, if one guesses incorrectly, then Alice's transmitted bit is received correctly with probability 1/2. Thus in general, the probability of correctly receiving Alice's transmitted bit is

$$P = 1/2.\ 1 + 1/2\ .\ 1/2\ = ¾ \quad (2)$$

For each bit transmitted by Alice, we assume that Eve performs one of two actions, opaque eavesdropping with probability λ, $0 \leq \lambda \leq 1$, or no eavesdropping with probability $1- \lambda$. Thus, if $\lambda = 1$, Eve is eavesdropping on each transmitted bit; and if $\lambda = 0$, Eve is not eavesdropping at all. Because Bob's and Eve's choice of measurement operators are stochastically independent of each other and of Alice's choice of state, Eve's eavesdropping has an immediate and detectable impact on Bob's received bits. Eve's eavesdropping causes Bob's error rate to jump from 1/4 to

$$1/4(1- \lambda) + 3/8\ \lambda = 1/4 + \lambda/8 \quad (3)$$

Thus, if Eve eavesdrops on every bit, i.e., if $\lambda = 1$, then Bob's error rate jumps from 1/4 (.25) to 3/8 (0.375), a 50% increase.). That is, Bob's probability of reception of the correct bit is decreased to 0.625. In the second stage, Alice and Bob communicate in two phases over a public channel to check for Eve's presence by analyzing Bob's error rate. The two phases of the scheme is explained below.

VII. PHASE 1 . EXTRACTION OF RAW KEY

Phase 1 of stage 2 is dedicated to eliminating the bit locations (and hence the bits at these locations) at which error could have occurred without Eves eavesdropping. Bob begins by publicly communicating to Alice which measurement operators he used for each of the received bits. Alice then in turn publicly communicates to Bob which of his measurement operator choices were correct. After this two way communication, Alice and Bob delete the bits corresponding to the incompatible measurement choices to produce shorter sequences of bits which we call respectively Alice's raw key and Bob's raw key. If there is no intrusion, then Alice's and Bob's raw keys will be in total agreement. However, if Eve has been at work, then corresponding bits of Alice's and Bob's raw keys will not agree with probability

$$0.(1- \lambda) + 1/4.\lambda = \lambda/4 \quad (4)$$

VIII. PHASE 2 . DETECTION OF EVE'S INTRUSION VIA ERROR DETECTION

Alice and Bob now initiate a two way conversation over the public channel to test for Eve's presence. 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 m 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 Alice and Bob

return to stage 1 and start over. On the other hand, if no inconsistencies are uncovered, then the probability that Eve escapes detection is:

$$P_{false} = (1 - \lambda/4)^m \quad (5)$$

For example, if $\lambda = 1$ and m= 200, then

$$P_{false} = (3/4)^{200} \approx 10^{-25}$$

Thus, if P_{false} is sufficiently small, Alice and Bob agree that Eve has not eavesdropped, and accordingly adopt the remnant raw key as their final secret key.

IX. MULTIPLE EAVESDROPPERS WITH NON-SINGLE PHOTON SOURCE

In case if multiple eavesdroppers are working, and Alice has non-single photon source, the state changed by one eavesdropper may be restored by the next and so Bob has no way of catch-up the disturbances. Based on this idea, in this work, bit error rate is analysed for the BB84 protocol with multiple eavesdropping using the simulation program written in Quantum Package for Mathematica.

ASSUMPTIONS

Alice sends Bob a stream of qubits.

For each qubit, before sending it to Bob, she randomly chooses a bit |0> or |1>

And randomly either applies Hadamard operator H to the qubit or not

Send the qubit to Bob,

Bob receives a random sequence of qubits, each of which is in one of the four states.

|0>, |1>, ½(|0> + |1>), ½(|0> - |1>)

The three important terms in the context of quantum cryptography are

Bit values – {0, 1}

Bases – H/V = {0^o, 90^o} or D/A = {45^o,135^o or -45^o}

States – {0, 90, 45, 135}

MEASUREMENT

A measurement can be regarded as a quantum mechanic operation projecting the state of the photon onto the chosen basis and giving the eigenvalues of the state in that basis. Due to the overlap of the states the probability of measuring the correct state given the wrong basis is 1/2. The calculation of the probability is denoted $|\langle State|Basis\rangle|^2$.

Suppose if a qubit ‘q1’ is in an initial state of |0>, then we will get the following observation for the output of |0>, using different measurement operators.

Meausrement	Probability
$\langle 0_i \mid \cdot q1$	1
$\langle 1_i \mid \cdot q1$	0
$\langle +_i \mid \cdot q1$	$\frac{1}{\sqrt{2}}$
$\langle -_i \mid \cdot q1$	$\frac{1}{\sqrt{2}}$

After the measurement the system is in the new measured state.

X. SIMULATION USING QUANTUM PACKAGE

The simulation contains the following steps.

1. Alice has a source of random (classical) bits
2. Alice can produce qubits in states |0> and |1>
3. Alice can apply a Hadamard operator H to the qubits
4. Bob can measure income qubits either in the basis |0>, |1> (i.e.) + or in the basis $1/\sqrt{2}$ (|0> + |1>), $1/\sqrt{2}$ (|0> - |1>) (i.e.) X
5. Alice generates a stream of qubits (photons)
6. For each qubit, before sending it to Bob, Alice randomly chooses a bit |0> or |1>
7. Randomly either applies H to the qubit or not
8. And finally sends it to Bob

Therefore, Bob receives a random sequence of qubits, each of which is in one of the four states.

|0>, |1>, H|0> = $1/\sqrt{2}$ (|0> + |1>), H|1> = $1/\sqrt{2}$ (|0> - |1>)

For each qubit, Bob randomly chooses either the basis |0>, |1> or the basis H|0>, H|1> and measures the qubit in the chosen basis.

Bob announces which basis he used for each measurement over a classical channel.

Alice tells Bob which measurements were made in the correct basis

The qubits which were measured in the wrong basis are discarded, while the rest form a shared key.

XI. SIMULATION OUTPUT AND CONCLUSION

The simulation is carried out for different number of Qubits and for each case the Bob's capture percentage (i.e.) bit error ratio is calculated. The bit error ratio (BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. A sample output of the simulation program is shown in Table 3.

Table 3. Simulation Result

Number of Qubits (n)	Bob's Capture Percentage (BER)		
	Without Eavesdropper	Single Eavesdropper	Two Eavesdroppers
20	11/20 =55%	8/20 = 40%	6/20=30%
50	31/50=62%	24/50 = 48%	17/50=34%

100	61/100=67%	41/100 = 41%	36/100=36%
200	96/200=48%	89/200 = 44.5%	52/200=26%

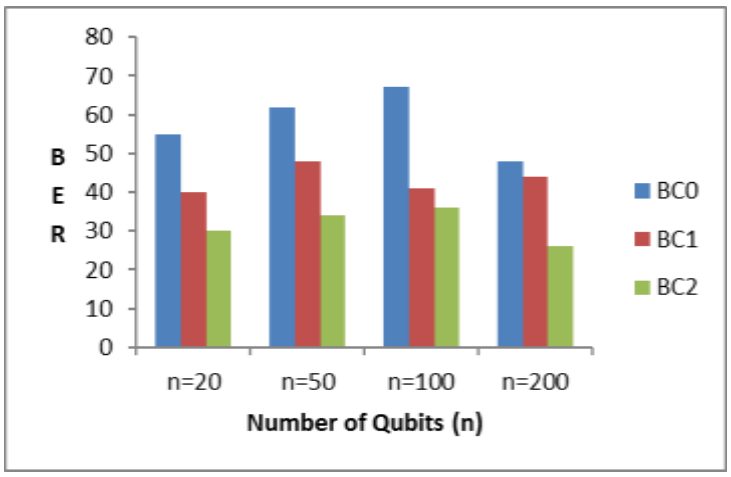

Figure 1. BER for different 'n' values

The simulation output shows that even in the case of multiple eavesdroppers with non-single photon source, the bob's qubit capture percentage decreases. The decrease in percentage indicates one or more eaves are working on the channel and hence Alice and Bob can terminate the session safely.

XII. ACKNOWLEDGEMENT

The authors acknowledges José Luis Gómez-Muñoz and Francisco Delgado, Tecnologico de Monterrey, State University of Mexico, the developers of Quantum Package for Mathematica.

REFERENCES

[1] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21, 1978, 120-126.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, 1984, 175.

[3] Jeffrey D. Morris, Douglas D. Hodson, Michael R. Grimaila, David R. Jacques, Gerald Baumgartner "Towards the Modelling and Simulation of Quantum Key Distribution Systems International Journal of Emerging Technology and Advanced Engineering, 4(2), 2014.

[4] Hui Qiao, Xiao-yu Chen, Proceedings of 14th Youth Conference on Communication, 978-1-935068-01-3, scientific research, 2009.

[5] Viacheslav Burenkov, Security Issues of Quantum Cryptographic Systems with Imperfect Detectors, doctoral diss., Department of Physics,University of Toronto, 2015

[6] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M., The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301, 2009

[7] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances," Science 283, 1999, 2050-2056.

[8] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. 85, 2000, 441-444.

[9] D. Mayers, "Unconditional security in quantum cryptography," J. ACM 48, 2001, 351-406.

[10] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 2002, 145.

[11] Artur K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. 67, 1991, 661.

[12] Charles H. Bennett, Quantum cryptography using any two no orthogonal states Phys. Rev. Lett. **68**, 1992, 3121.

[13] Lo, Hoi-Kwong, and Norbert Lütkenhaus. "Quantum cryptography: from theory to practice." *arXiv preprint quant-ph/0702202*, 2007.

[14] Nicolas Gisin, Gregoire Ribordly, Wolfgang Tittel and Hugo Zbinden, Quantum Cryptography, Group of Applied Physics, University of Geneva, Reviews of Modern Physics, 2008

[15] Samuel J. Lomonaco, A Quick Glance at Quantum Cryptography, arXiv:quant-ph/9811056v1, 1998.