METHODS TO COUNTER ATTACKS ON QUANTUM CRYPTOGRAPHY PROTOCOLS

By

SINDHU CHITIKELA

Bachelor of Technology in Computer Science

Jawaharlal Nehru Technological University

Hyderabad, AP, India

2011

Submitted to the Faculty of the Graduate College of the
Oklahoma State University in partial fulfillment of the
requirements for the Degree of
MASTER OF SCIENCE
May 2013

METHODS TO COUNTER ATTACKS ON

QUANTUM CRYPTOGRAPHY PROTOCOLS

Thesis Approved:

Subhash Kak

Thesis Adviser

Eric Chan-Tin

Tingting Chen

ACKNOWLEDGEMENTS

I dedicate my thesis work to my parents, Chitikela Venkata Krishna Reddy and Chitikela Anuradha and my brother, Chitikela Arun Kumar Reddy for their support, love and encouragement throughout my life.

I am grateful to Dr. Subhash Kak for providing a chance to contribute to his research. I appreciate his encouragement and support throughout the period of my MS. I also thank Dr. Eric Chan-Tin and Dr. Tingting Chen for their advices in completing my thesis work successfully.

Acknowledgements reflect the views of the author and are not endorsed by committee members or Oklahoma State University.

Name: SINDHU CHITIKELA

Date of Degree: MAY 2013

Title of Study: METHODS TO COUNTER ATTACKS ON QUANTUM
CRYPTOGRAPHY PROTOCOLS

Major Field: COMPUTER SCIENCE

Abstract: The need for secure transmission in the fields of banking and defense has led to the interest in quantum cryptographic protocols which are theoretically more secure than any classical cryptographic protocol. However, the current implementations of the quantum cryptographic protocols have weaknesses. The main goal of this work is to find ways to strengthen quantum cryptographic protocols by using new implementation schemes. We present a method to improve the randomness of the sequence of polarization states used in BB84, the two-stage and the three-stage protocols. An analysis of quantum cryptography in the presence of noise is given. We also study a variant of the three-stage protocol where the intensity of the photons is tracked. We have developed a further improvement to this protocol where the state of the photons is also estimated.

TABLE OF CONTENTS

Chapter Page

Chapter Page

LIST OF TABLES

Table Page

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Overview of quantum cryptography

In quantum cryptography information is transmitted in the form of photons or light particles. These information carriers obey laws of quantum physics. A photon which is a quantum state exhibits the property that in general it is a superposition of mutually exclusive attributes and the unknown polarization of a photon cannot be cloned.

Quantum cryptography is a secure way to distribute a random secret key between two parties. Once the key is shared through a quantum channel, the information is then transferred through a public channel using classical cryptographic techniques.

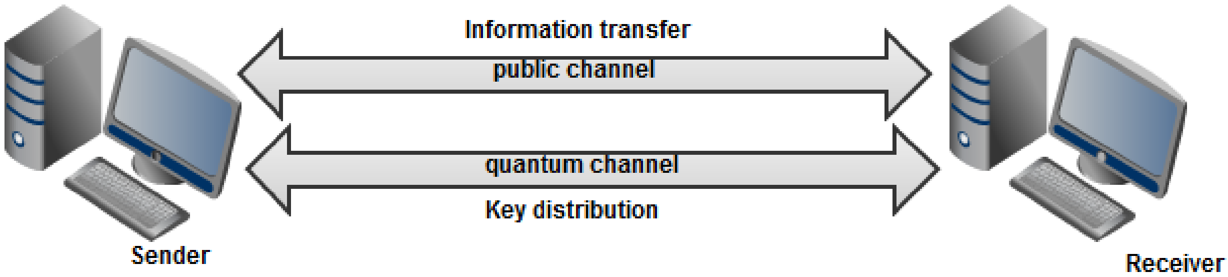


Figure 1 Quantum key distribution

Quantum cryptography makes it possible to implement a one-time pad under certain conditions. BB84 Protocol, two-stage protocol and the three-stage protocol are the best known quantum cryptographic protocols.

1.2 Research in quantum cryptography

The research in quantum cryptographic system can be put in categories of the application, key management, physical quantum cryptographic transformation, and generation of random sequences. The various levels of the cryptographic system are as shown in the Figure 2. In this thesis, we have worked on cryptographic hardening of random sequences and also made a contribution to the methods used for the quantum cryptographic transformation.

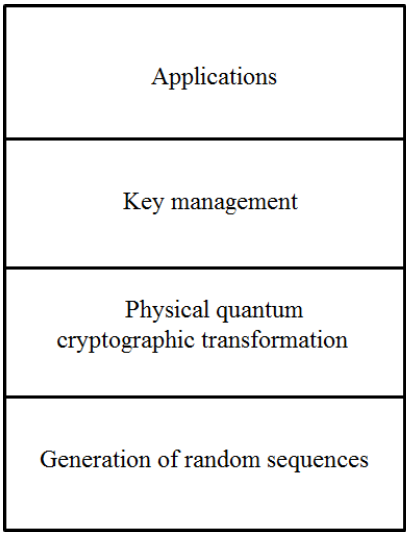

Applications
Key management
Physical quantum cryptographic transformation
Generation of random sequences

Figure 2 Cryptographic system

1.3 Organization of thesis

Towards the first goal of improving the randomness of a sequence, we have investigated the effect of introducing permutations on blocks of a candidate random sequence. This work is discussed in detail in chapter III.

In the study of quantum cryptography protocols, we have investigated a drawback of the iAQC protocol which tracks the intensity of the transmitted photons to ensure that Eve has not siphoned off some of the photons. Since Eve can theoretically inject photons to compensate for the ones she has siphoned off, we have investigated a new protocol that is intensity and state aware (chapter IV).

CHAPTER II

REVIEW OF RELATED LITERATURE

The following sections give an overview of information representation in quantum mechanics, quantum cryptographic protocols like BB84 protocol, the two-stage protocol, the three-stage protocol and noise analysis on these protocols.

2.1 Representation of information by photons

A single photon is a qubit. Let us consider the information associated with the photon. Represented as a qubit $(a|0\rangle + b|1\rangle)$, the photon will collapse to $|0\rangle$ or $|1\rangle$ but since this collapse is random, it would not communicate any useful information to the receiver. Maximum information will be communicated to the receiver if the sender prepares the photon in one of the two orthogonal states $|0\rangle$ or $|1\rangle$, which the receiver will be able to determine upon observation.

In the BB84 protocol, the photon is polarized using either rectilinear bases (horizontal and vertical bases) or diagonal bases (-45^0 and 45^0 bases) to represent qubits. A photon generated represents a qubit after it is passed through a linear polarizer as shown in Figure 3. A horizontally polarized photon or a photon that is polarized by -45^0 represents a qubit 1. Similarly a vertically polarized photon or a photon that is polarized by +45^0

represents a qubit 0. Table 1 summarizes the representation of qubits. This process of generation of qubits is done at the sender's site. At the receiver's site, the stream of polarized photons are passed through polarizing beam splitters and then through photon detectors to know the qubits.

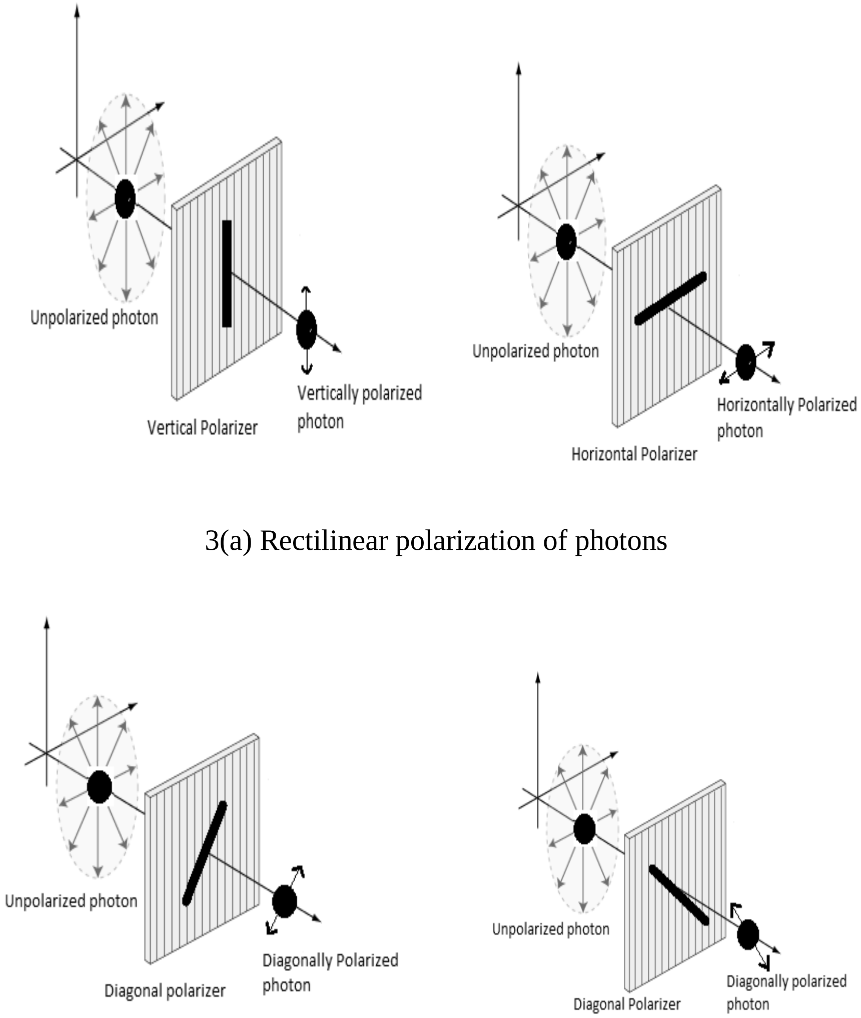
When a horizontally polarized photon passes through a rectilinear polarizing beam-splitter, it is found at the refracted output (horizontally polarized photons) exit of the beam splitter. Similarly when a vertically polarized photon passes through a rectilinearly oriented beam splitter, it is found at the refracted output (vertically polarized photons) exit of the beam-splitter as shown in the Figure 3(a). But when a horizontally polarized photon passes through a diagonally oriented beam-splitter, the photon has 50% probability to be found at each exit. Furthermore, the photon will have a corresponding diagonal polarization afterwards as shown in the Figure 3(b).

Table 1 Representation of qubits in quantum cryptography

Polarization	**Quantum bit value**
Horizontal Polarization	0
Vertical Polarization	1
-45^0	1
$+45^0$	0

2.2 BB84 protocol

As it is customary, we name the sender as Alice, the receiver as Bob and the eavesdropper as Eve. In the BB84 protocol, the key distribution takes place in a quantum channel and the further transmission of information takes place in a public channel.



3(a) Rectilinear polarization of photons

3(b) Diagonal polarization of photons

Figure 3 Linear polarization of a photon at the sender site to represent a quantum bit

At the sender's site, a single photon at a time is sent through linear polarizer as explained previously to generate polarized photons that represent a bit 0 or 1 of information. Alice codes a quantum bit using either a rectilinear base state or a diagonal base state. The base states are chosen randomly. The resultant stream comprises of horizontally, vertically polarized photons and diagonally polarized photons each representing a qubit of the information that Alice wants to send to Bob. In this case of key distribution, the information sent is a pseudorandom sequence that is used to compose a key.

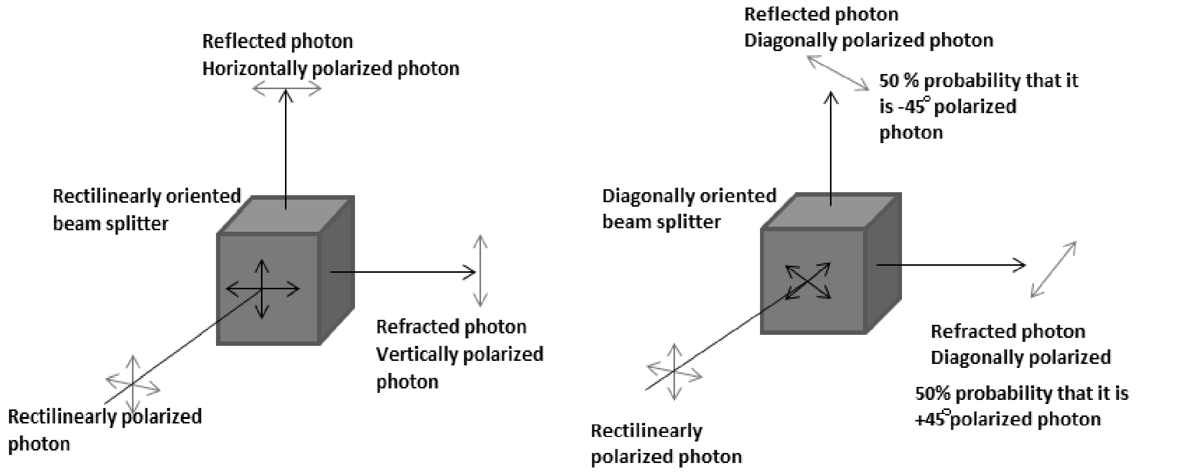

Reflected photon
Horizontally polarized photon
Rectilinearly oriented beam splitter
Refracted photon
Vertically polarized photon
Rectilinearly polarized photon
Reflected photon
Diagonally polarized photon
50 % probability that it is -45° polarized photon
Diagonally oriented beam splitter
Refracted photon
Diagonally polarized
50% probability that it is +45° polarized photon
Rectilinearly polarized photon

Figure 4(a) A rectilinearly polarized photon passing through a rectilinear beamsplitter

Figure 4(b) A rectilinearly polarized photon passing through a diagonal beamsplitter

Figure 4 Photons through beamsplitters

On receiving the stream of polarized photons, Bob measures the property of the photon by using two interchangeable polarizing beam splitters where one of them allows Bob to distinguish between the horizontal and vertical polarization, the other allows him to distinguish between -45^{0}and +45^0 polarization. He then uses photon detectors to know the arrival of the photon. The choice of polarizing beamsplitters is randomly made. If Bob uses a polarizing beamsplitter compatible with the polarization choice of Alice, he can read the bit as either 0 or 1 based on the polarization. If Bob uses a polarizing beamsplitter incompatible with the polarization choice of Alice, he cannot get any information about the state of polarization. As stated earlier, here the quantum state is a superposition of two mutually exclusive properties. There is a 50% probability of it being a bit that represents 0 or 1.

Once Alice is done with sending the information, Bob announces the sequence of polarizing beamsplitters that he used. Alice then compares this sequence with the sequences of bases that she used and tells Bob to note the beamsplitters that he used correctly. Finally those bits that are obtained from the correctly selected beamsplitters are considered and this forms the key called the Sifted key. The working of BB84 protocol is explained in the Figure 5.

2.3 The two-stage protocol

At an abstract level, the two-stage protocol can be explained in a simple scenario of exchange of a bag of money between Alice and Bob. Imagine a situation where Alice sends an amount of money to Bob, say X dollars. Bob either adds or subtracts some amount to this, say (X+Y) dollars and sends this to Alice. Alice now subtracts her amount from the bag and knows the value added by Bob. If the money in the bag is not counted in passage in both directions, then the protocol is secure.

This situation can be related to the two-stage protocol [2] as a scenario where Alice sends a linearly polarized photon that is randomly rotated through an angle θ to Bob. It is Bob who has to decide on the key to be shared and he either rotates the photon further by 90^0 or by 0^0 that is no rotation. In the third step, Alice rotates the photon by -θ and knows the rotation performed by Bob and hence knows the data chosen by Bob same as Alice knows the amount added by Bob. So, by knowing the rotation made by Bob, Alice knows the binary value decided by Bob to form a key. Hence the key negotiation can be done in just two stages.

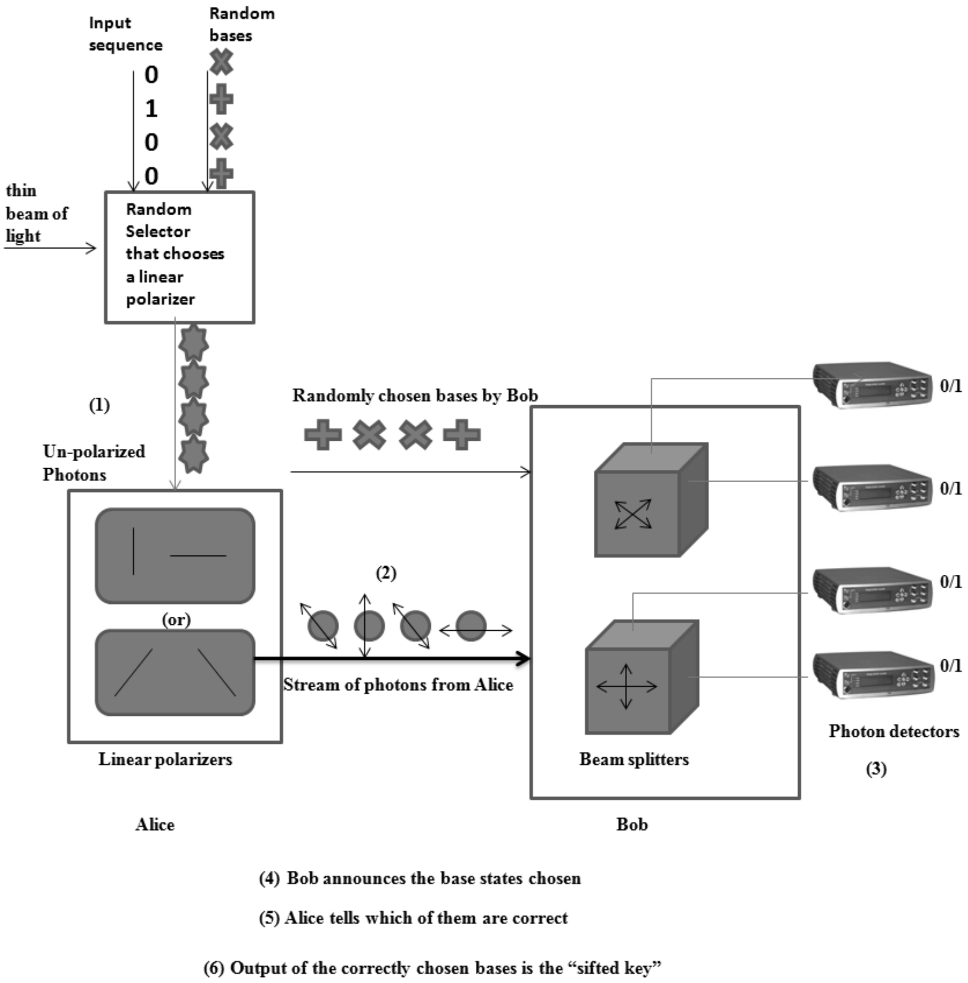

Input sequence
Random bases
0
1
0
0
thin beam of light
Random Selector that chooses a linear polarizer
(1)
Un-polarized Photons
Randomly chosen bases by Bob
(2)
(or)
Stream of photons from Alice
Linear polarizers
Alice
Beam splitters
Bob
0/1
0/1
0/1
0/1
Photon detectors
(3)
(4) Bob announces the base states chosen
(5) Alice tells which of them are correct
(6) Output of the correctly chosen bases is the "sifted key"

Figure 5 Working of BB84 protocol (1) Un-polarized photons are sent through randomly chosen linear polarizer to represent the qubits to be sent to Bob (2) The stream of polarized photons are sent from Alice to Bob (3) Bob detects the qubits by passing these linearly polarized photons through beamsplitters and then through photon detectors (4) Bob announces the base states chosen by him (5) Alice then tells which of these are correct (6) The shared key which is called the 'sifted key' is formed by the bits obtained from these correct bases told by Alice.

Once the key bits are known by Alice, Bob computes the hash value of the key and sends it to Alice. Similarly Alice computes the hash value of the key received and sends it to Bob. They compare the hash values received with the one they have computed and verify that the correct key is shared. This step ensures the secure distribution of secret keys. The working of the two-stage protocol is shown in Figure 6.

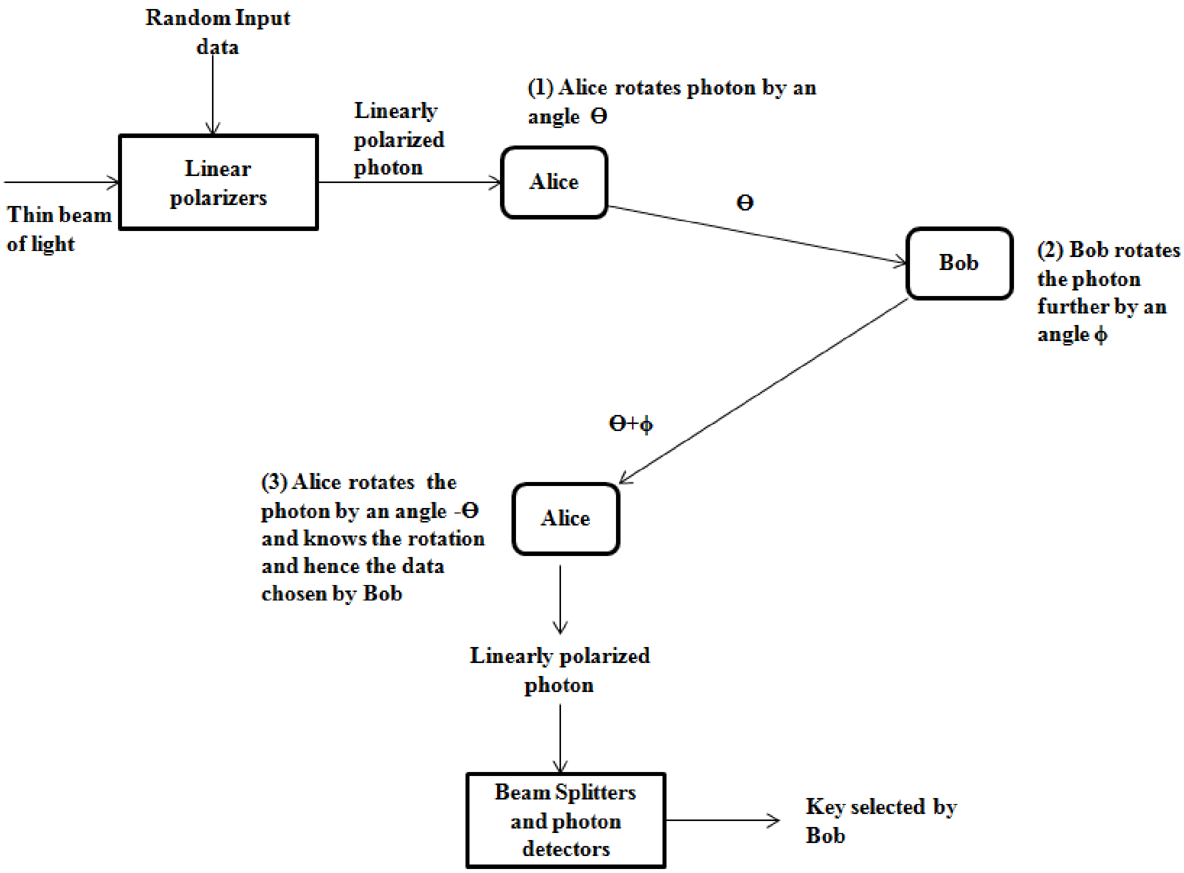

Random Input data
Linear polarizers
Thin beam of light
Linearly polarized photon
(1) Alice rotates photon by an angle ϴ
Alice
ϴ
Bob
(2) Bob rotates the photon further by an angle ϕ
ϴ+ϕ
(3) Alice rotates the photon by an angle -ϴ and knows the rotation and hence the data chosen by Bob
Alice
Linearly polarized photon
Beam Splitters and photon detectors
Key selected by Bob

Figure 6 Implementation of the two-stage protocol

2.4 The three-stage protocol

Unlike BB84 protocol, the entire communication between Alice and Bob remains quantum at each stage that is both the key distribution and the further information transfer takes place in a quantum channel. The working of the three-stage protocol [2] is based on the idea of both Alice and Bob using personal keys on the data that is being exchanged.

Consider a situation in which Alice puts her own lock on a box and sends it to Bob. Bob then puts his own lock on the box and sends it to Alice. Now, Alice removes her lock from the box and sends it to Bob. Bob now removes his own lock from the box and finally he can open and see what is in the box. In the three-stage protocol the locks are nothing but the secret transformations of each party.

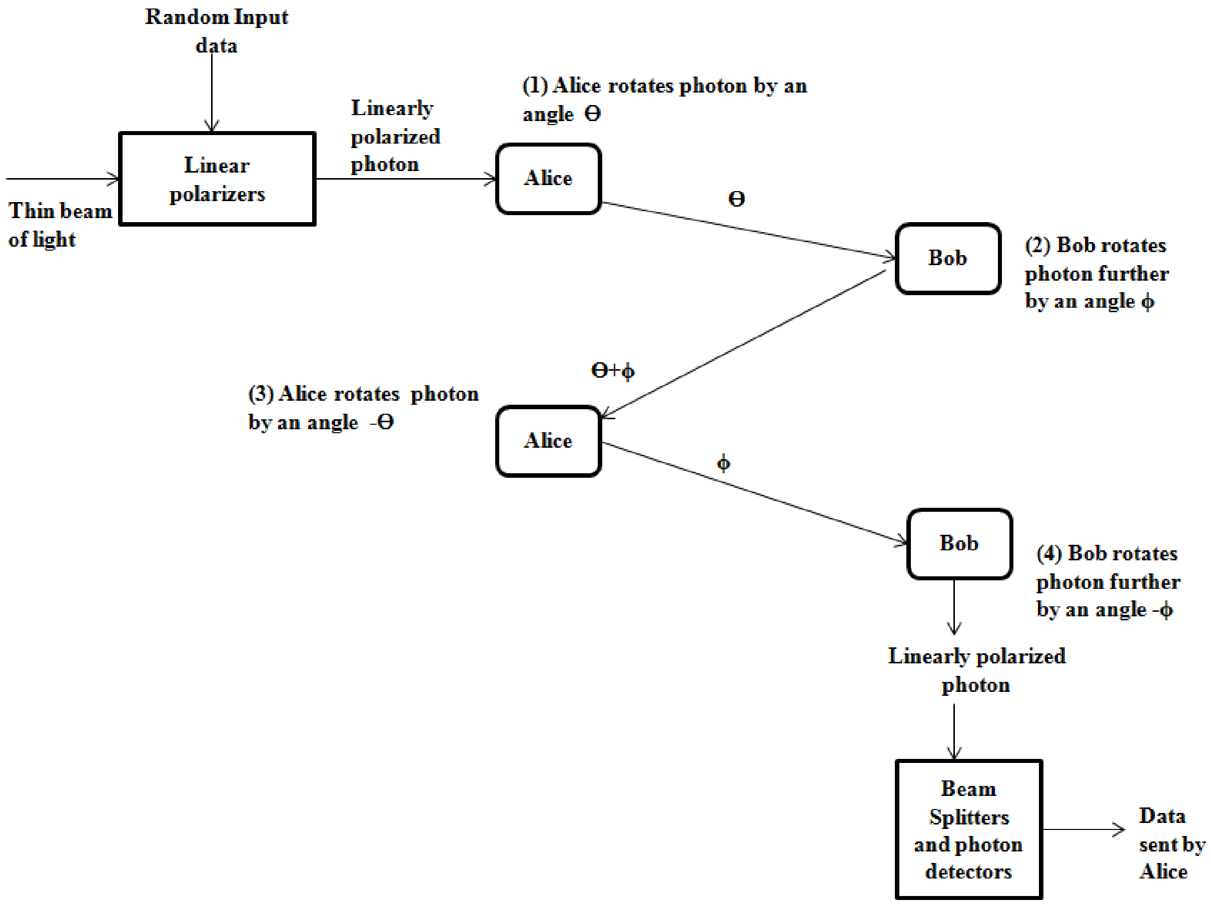

Random Input data
Linear polarizers
Thin beam of light
Linearly polarized photon
(1) Alice rotates photon by an angle Θ
Alice
Θ
Bob
(2) Bob rotates photon further by an angle ϕ
Θ+ϕ
(3) Alice rotates photon by an angle -Θ
Alice
ϕ
Bob
(4) Bob rotates photon further by an angle -ϕ
Linearly polarized photon
Beam Splitters and photon detectors
Data sent by Alice

Figure 7 Implementation of the three-stage protocol

The three-stage protocol involves secret rotation transformations on the photons. Alice codes a quantum bit by applying a secret transformation of some random angle on a polarized photon. In the initial stage, Alice rotates the polarized photon, X through a secret, random angle θ and sends it to Bob. In the second stage, Bob further rotates this photon through an angle ϕ. In the final stage, Alice inverses the transformation by re-rotating this photon by the same angle θ and sends it to Bob. Bob inverses the transformation that he applied on the photon by re-rotating by angle ϕ . Finally Bob receives the photon X that Alice intended to send (Figure 7).

2.5 Quantum cryptography in the presence of noise

2.5.1 Noise analysis on BB84 protocol

In the BB84 protocol, the effect of noise is combated by first estimating the noise rate on the public channel and then extracting the reconciled key from the raw key. First, Alice and Bob apply an agreed upon random permutation to their respective raw keys. The raw key is broken into blocks of length *x*, where the value of x is chosen so that it is most likely that the block contains no more than one error. For each of these blocks, and for other sub-blocks, Alice and Bob publicly compare parity checks, in a process so that erroneous bits are located and deleted. Each time parities are compared, an agreed upon bit is deleted from the chosen key sample. If the parity should not agree, a binary search strategy is used to locate and delete the error.

The correctness of the raw key can also be communicated between Alice and Bob by the use of cryptographically strong hash functions of their respective raw keys. The ideas of obtaining reconciled key starting from a raw key can be used for non-BB84 protocols also.

2.5.2 Noise analysis on the two-stage protocol and the three-stage protocol

In both the two-stage and three-stage protocols, there is a possibility that the equipment that rotates the photon through certain angle is working erroneously. The error can be at Alice's site or at Bob's site or it can be at both the sites. The error can also be in the quantum channel through which the photon is transferred. We will lump the error from various sources to a uniform probability distribution function in each communication link. The probability density function of error at Alice's or Bob's site is uniform with the measure of angle *x* ranging from -0.1 to +0.1 radians and is represented in the Figure 8.

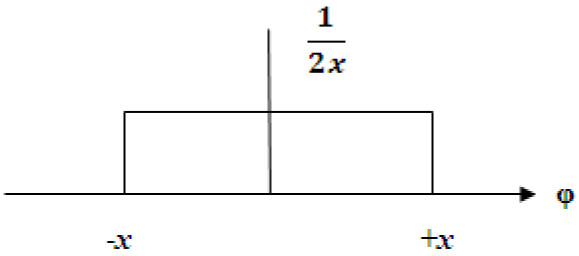


Figure 8 Probability density function of Error

Therefore, the probability of error is obtained by the following expression where φ ranges from –*x* to +*x* radians. We have

$$\int_{-x}^{+x} \frac{1}{2x} sin^2 \varphi \ d\varphi \ = \ \frac{1}{2} - \frac{1}{4x} sin\, 2x$$

which is approximately equal to $\frac{1}{3}x^2 - \frac{1}{15}x^4$ where *x* ranges from -0.1 to +0.1 . The graph obtained by taking different values is shown in the Figure 9. The y-axis represents the probability of error and the x-axis represents the value of *x* in radians.

When the error exists at both the sites, then the cumulative effective of noise is as shown in the Figure 10. Therefore, the probability of error is obtained by the following expression where φ ranges from –*x* to +*x* radians.

$$2\int_{0}^{2x}(-\frac{1}{4x^2}\varphi + \frac{1}{2x})\left(sin\varphi\right)^2 d\varphi \ = \frac{2x^2}{3}$$

where *x* ranges from -0.1 to +0.1 .

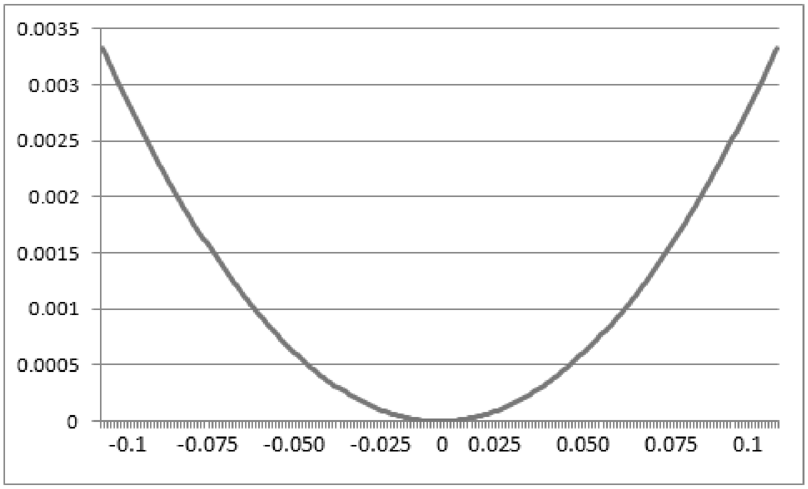


Figure 9 Probability of error with the noise at single site based on the value of *x* in radians

The graph obtained by taking different values of error angle is shown in the Figure 11. The y-axis represents the probability of error and the x-axis represents the value of *x*.

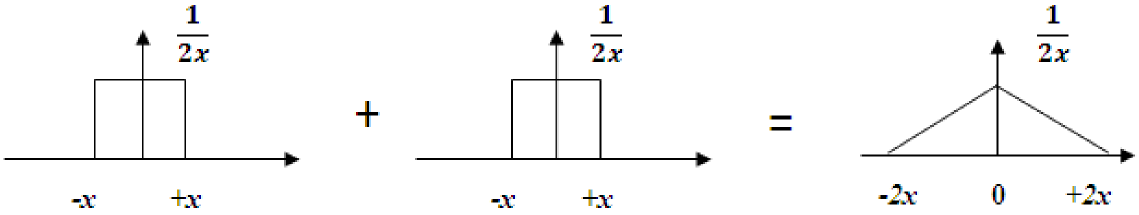


Figure 10 Cumulative effective of noise at both the sites

We notice that the probability of error in two stages is roughly equal to twice of that in one stage. Likewise, the probability of error in three stages is roughly three times the error in a single stage. Given this error rate, one can use standard methods of key purification to obtain the reconciled key from the raw copy.

2.6 Comparison of BB84 protocol with the two-stage and the three-stage protocols

Apart from the faked-state attack [18], [19], the main weakness of BB84 protocol is that it is difficult to produce single photon at a time and the duplicate photons can be used by the eavesdropper to reconstruct the key. Hence, the attacker can siphon off the photons when they are transferred between Alice and Bob. Moreover, as the photons are siphoned off only at one step, the intensity of the output at the receiver's end is not affected. There is also the problem in generating single photons [20] as well as having single photon detectors.

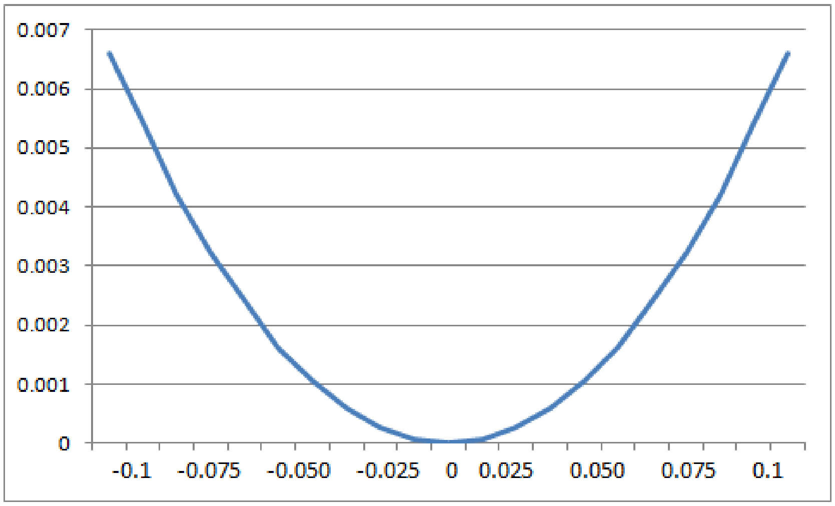


Figure 11 Probability of error with the noise at two sites based on the value of *x* in radians

This is not the case with Kak's multistage protocols. In order to know the angles θ and ϕ, Eve has to siphon off the photons in all the stages which can result in significant decrease in the intensity of the output. Hence, the receiver can easily identify the attack. Nevertheless, practical implementation of this system creates its own difficulties [21]-[23]. The security of single-photon rotation system has recently been presented [24]. A modification of the three-stage protocol to catch active eavesdroppers was recently presented [25]. Although it is generally claimed that quantum key distribution is unconditionally secure, Yuen has argued against that position [26].

2.7 Conclusion

This chapter presents overview of quantum cryptography protocols and the noise analysis on these protocols. The noise model used is that of uniform distribution of error over a certain small range that is associated with each link without regard for the source of the error. The noise in different links is taken to be independent.

In every cryptographic protocol, a random sequence plays a vital role. In the BB84 protocol, the bases are chosen randomly at both the parties. This shows the role of a random sequence in BB84 protocol. Similarly, in three-stage protocol, the polarization angles θ and ϕ are chosen randomly. In the two-stage protocol, the polarization angle θ is randomly chosen and the value of ϕ being 0^0 or 90^0 is also random. Therefore, if the random sequence is cryptographically strong, the strength of the protocol increases. In chapter III we discuss a new technique to improve the randomness of a sequence.

CHAPTER III

CRYPTOGRAPHIC HARDENENING OF RANDOM SEQUENCES

3.1 Introduction

Pseudorandom sequences that are algorithmically produced have limited cryptographic applications because the eavesdropper can readily generate them. The complexity of the generation process and the lack of correlation amongst the bits (or digits) of the sequence are important in determining the usefulness of a pseudorandom sequence. A quantum mechanical process can be used to generate a true random sequence but the problem with such an approach is that such sequences cannot be replicated. Classical random sequences also find use in quantum cryptography applications since the random base choices or rotations there, either in the BB84 protocol or the three-stage protocol [2]-[4], must be generated by an algorithmic process.

To develop a method of improving the quality of pseudorandom sequences, the question of a metric for the degree of randomness must be addressed. There are several ways the randomness of a binary sequence is defined statistically [5] and from a computational complexity point of view [6]. The problem of randomness is complicated by entanglement in quantum systems [7],[8] and it shall not be considered here. One popular method of defining randomness of an *n*-bit long sequence *a(i)* is given by the following formula

$$R(sequence) = 1 - \frac{1}{n-1}\sum_{k=1}^{n-1}(|c(k)|)$$

where *c(k)* is the autocorrelation function $c(k) = 1/n\sum_{j=1}^{n}(a_j a_{j+k})$, where the sequence is represented in terms of +1s and -1s. This is intuitively satisfactory since for a completely random binary sequence this randomness measure is equal to 1 and for a constant sequence the randomness measure is 0. For a maximul length shift-register sequence of period 2^k [9], the randomness measure is *1-1/n*. For good pseudo-random sequences, the randomness measure will be a number just less than 1.

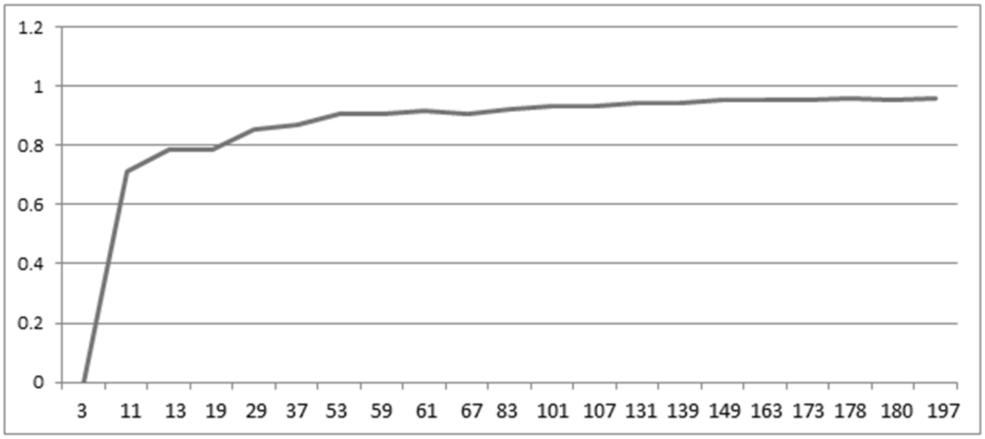


Figure 12 Randomness measure of prime reciprocal sequences to 200

Prime reciprocal sequences or d-sequences [10]-[14] have many applications and any pseudo-random sequence can be mapped to a suitable d-sequence. As seen in Figure 12, the randomness measure gets closer to 1 as the period of the d-sequence increases which is perfectly consistent with the theorem that prime reciprocal sequences are normal sequences.

A number *x* is simply normal in base *r* if in the decimal of *x* each of the *r* possible digits occur with a frequency *1/r,* i.e.,$\lim_{n\to\infty}\frac{n_b}{n} = \frac{1}{r}$ for all *b,* where the digit *b* occurs n_b times in the first n places and a number x is normal in base r if all of the numbers $x, rx, r^2x,\ldots$ are simply normal in all of bases $r, r^2, r^3,\ldots$ It follows that when x is expressed as a decimal in the scale of r, every combination $b_1, b_2, b_3, \ldots$ of digits occurs with the proper frequencies. Thus, the property that a number is normal in base r may be reiterated by saying that all the digits 0 to $(r - 1)$ occur with equal probability, and that each digit of the sequence is independent of every other digit. Almost all numbers are normal in any base.

Nevertheless, from a practical point of view, given prime reciprocal sequences are not entirely satisfactory. To see this first note that the prime reciprocal sequence $a(i)$, $i = 1,2,3,\ldots$ for prime p (that is the sequence $1/p$ in base 2) can be generated as $a(i) = 2^i \bmod p \bmod 2$ (Reference [12]):

$b(0)= 1$

$b(i+1) = 2b(i) \bmod p$

$a(i)=b(i) \bmod 2$

Maximum length (with period p-1) prime reciprocal sequences are generated when 2 is primitive root of p. Although maximum length binary prime reciprocal sequences have excellent autocorrelation properties they have the negative peak of -1 for half the period that reflects the fact that the sequence after half the period is a complementary image of the first half. As example, the binary d-sequence for 1/13 is 000100111011 where the last 6 bits are complements of the first 6 bits. This means that although the randomness measure of such sequences is high, it is not very useful in this context.

We suggest performing another transformation on the given sequence. In contrast to an earlier preliminary study [15] where groups of bits were mapped to a single bit based on plurality of 0s or 1s to improve autocorrelation properties, here we consider the effect of block permutations on autocorrelation. A number of different random permutations are applied to the blocks of the candidate pseudorandom sequence. We will show that doing so improves the autocorrelation performance considerably.

3.2 Choosing blocks for permutations

A d-sequence can be divided into either even number of blocks or odd number of blocks. The performance of the permutation for the d-sequences does depend on whether the number of blocks is even or odd. For example, the d-sequence of the prime number 1277 can be divided into blocks in a variety of ways as 1276 has factors 2, 4, 11, and 29. Here we will consider the division of 1276 into 58 blocks of size 22 bits or 319 blocks of size 4 bits.

In the general case, the sequence *S* can be represented as the concatenation of blocks $S_1S_2S_3S_4$... We represent an n-permutation by the operator $P_n = P_1P_2P_3$... so that the permutations P_1, P_2, $P_{3,}$… are applied in sequence. For example, 3-permutation P_3 will work as follows:

$$P_3(S) = P_1(S_1)\, P_2\, (S_2)\, P_3(S_3)\, P_1(S_4)\, P_2(S_5)\ \ldots$$

3.2.1 Experiments

In the first experiment, we consider the d-sequence of length 1276 which is divided into 58 blocks that is S_1, S_2, S_3… S_{58}. We generated a random permutation, P, of size 22. This permutation,P is applied on all the 58 blocks of the d-sequence. If the position of each digit is represented with the help of an alphabet as follows.

1	0	1	0	1	0	0	1	1	0	1	1	0	1	1	1	1	0	1	1	1	1
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v

P is the permutation “hajblcfedgikovusrqnpmt” and it transforms the given block to 1100110100111111011101. This random permutation “hajblcfedgikovusrqnpmt” is applied on each of 58 blocks of the sequence. We have conducted this experiment many times where the permutation P varies in each experiment. The average of all auto-correlation values is plotted in the graph shown in Figure 13.

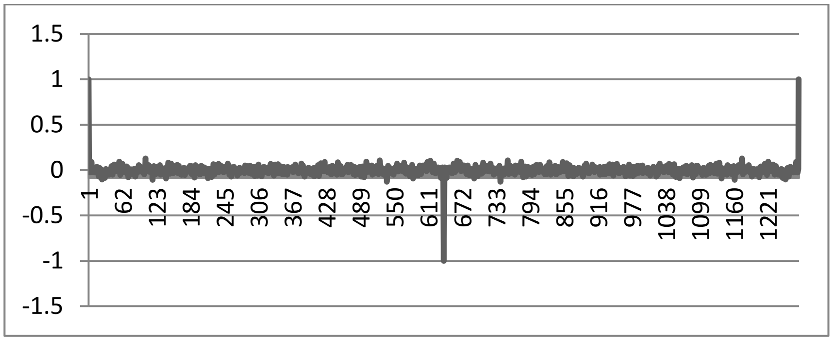


Figure 13 Autocorrelation of the d-sequence with a single permutation applied on its 58 blocks of size 22 digits each

To stress the difference with odd number of blocks, we next consider 319 blocks of size 4 digits each of the d-sequence of 1277. We applied a single permutation P, on all the 319 blocks as we did in the case of even number of blocks. The graph in Figure 14 shows the auto-correlation values of the d-sequence for odd number of blocks. As the autocorrelation function for half the period is less than what it was for the case of even number of blocks, this clearly shows that the performance of permutation process varies for even and odd number of blocks.

Next, as a continuation of the first experiment on the d-sequence for even number of blocks, we generated two random permutations P_1, P_2 of length 22 each. The permutation P_1 is applied on block1 and the permutation P_2 is applied on block2. Then the same two permutations P_1 and P_2 are applied on block3 and block4 respectively. This is repeated for all the 58 blocks of the d-sequence. We conducted the experiment many times where the permutations P1 and P2 are different every time and plotted the average of the autocorrelation values in the graph shown in Figure 14.

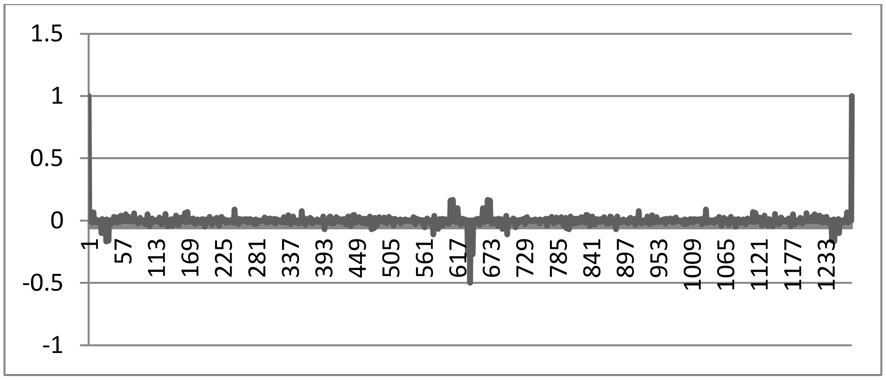


Figure 14 Autocorrelation of the d-sequence with a single permutation applied on its 319 blocks of size 4 digits each

Next we consider four random permutations P_1, P_2, P_3 and P_4. We applied the permutations P1, P2, P3 and P4 on block1, block2, block3 and block4 of the d-sequence of period 1276. Then, we applied the same four permutations, P1, P2, P3 and P4 on block5, block6, block7 and block8 respectively and this process was repeated till the end of the 58 blocks.

Similarly we considered five, six, seven, eight, nine and ten different permutations on the 58 blocks of the d-sequence of 1277. As a final step, we generated 58 random permutations P_1, P_2…P_{58} on block1, block2…block58 respectively. We conducted the experiment many times where the permutations are different every time and plotted the average of the autocorrelation values in the graph shown in Figure 17.

3.2.2 Off Peak autocorrelation for different number of permutations performed on the d-sequence of 1277

Table 2 represents the maximum auto-correlation values of the d-sequence of the prime number, 1277. These are the results observed when the above experiments of different permutations are performed on the d-sequence of 1277 which is divided into 58 blocks of size 22 digits each. Table 3 represents the maximum auto-correlation values of the d-sequence of the prime number 1277 for odd number of blocks that is 319 blocks of size 4 digits each.

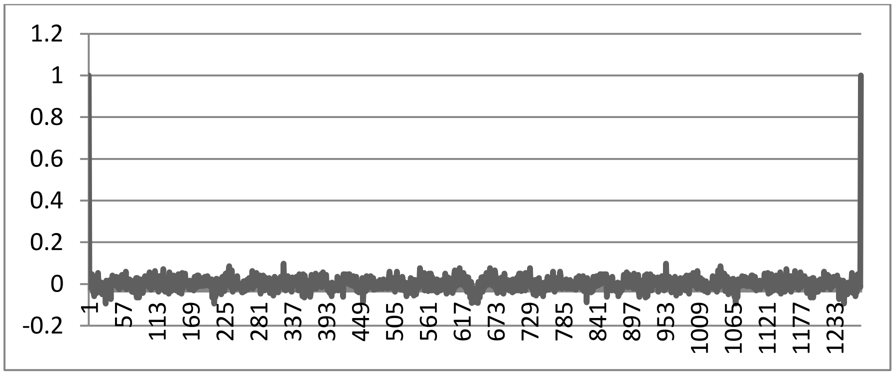


Figure 15 Autocorrelation of the d-sequence of 1277 with two different permutations on 58 blocks of size 22 digits each

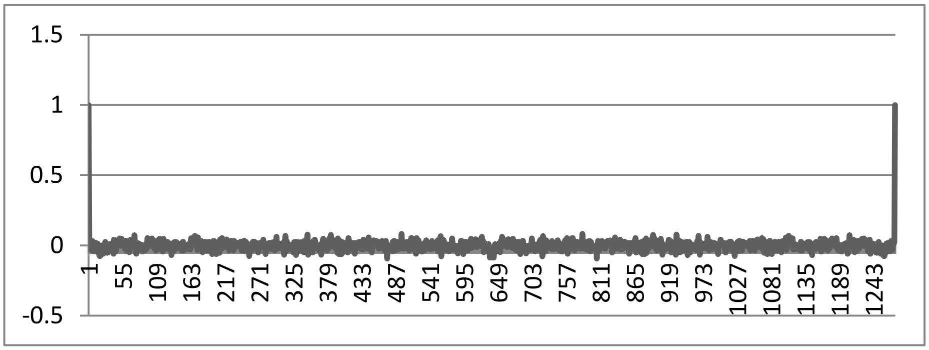


Figure 16 Autocorrelation of the d-sequence of 1277 with four different permutations on its 58 blocks of size 22 digits each

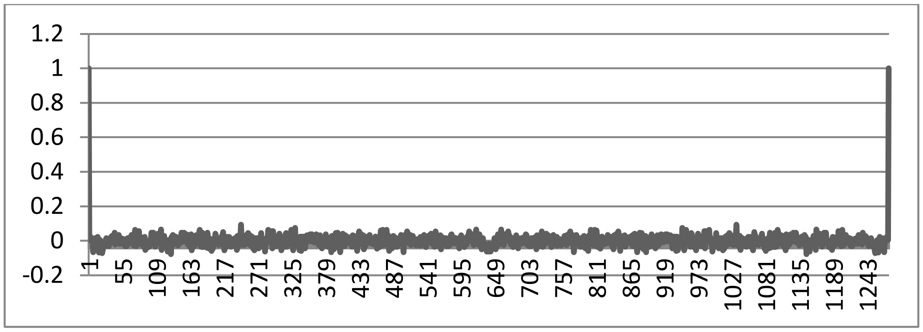


Figure 17 Autocorrelation of the d-sequence of 1277 with 58 different permutations on its 58 blocks of size 22 digits each

Table 2 Absolute maximum of the autocorrelation values of the d-sequence of 1277 which is divided into 58 blocks of size 22 digits each that is even number of blocks

Number of different permutations	Maximum auto-correlation value
0	1.0
1	1.0
2	0.10
3	0.09
4	0.10
5	0.10
6	0.09
7	0.10
8	0.24
9	0.10
10	0.13
58	0.08

The striking difference between the two Tables if for the value at 1-permutation where for obvious reasons it makes for no improvement if the number of blocks is even. Also if the size of the blocks is small, the reduction in the value of the off-peak autocorrelation is small.

3.3 Improvement factor

The Improvement factor in the off-peak autocorrelation function of any d-sequence may be measured by the following formula.

$$\textit{Improvement factor, } I = 1/\text{maximum}\ (|c(k|),\ k \neq 0$$

Table 3 Absolute maximum of the autocorrelation values of the d-sequence of 1277 which is divided into 319 blocks of size 4 digits each that is odd number of blocks

Number of different permutations	Maximum auto-correlation value
0	1.0
1	0.47
2	0.38
3	0.41
4	0.24
5	0.64
6	0.31
7	0.32
8	0.37
9	0.26
10	0.34
319	0.19

We considered the improvement factor as a measure of randomness in our experiments. Figures 18 and 19 show the improvement factor for the d-sequence of prime 1277 for different number of permutations.

We conducted the above experiments for a large number of primes that lead to maximum length d-sequences. Figures 20 and 21 show the improvement factor of the permuted d-sequence of 1787. Figure 20 shows the improvement factor of the d-sequence of 1787 where it is divided into even number of blocks that is 94 blocks of size 19 digits each. Figure 21 shows the improvement factor of the d-sequence of 1787 where it is divided into odd number of blocks that is 47 blocks of size 38 binary digits each.

From all the above experiments it is found that the randomness of a d-sequence increases by applying permutations on its blocks. Similar results are obtained for a random sequence that is generated on a Windows PC. The above graphs show that the improvement factor is quite impressive if the block size is not too small. Several statistical tests of randomness [5] were performed on the sequences and the results were supportive of the conclusion that the sequences are cryptographically strong.

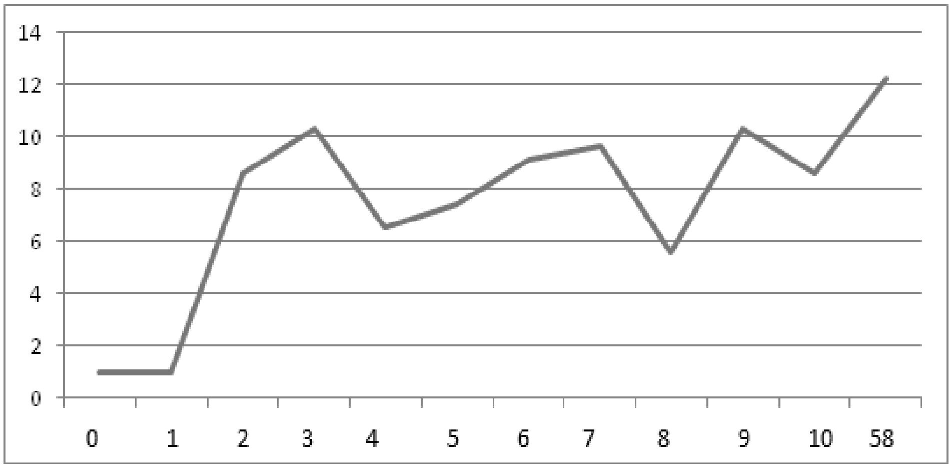


Figure 18 Improvement factor of the d-sequence of 1277 when divided into 58 blocks of size 22 digits each that is even number of blocks

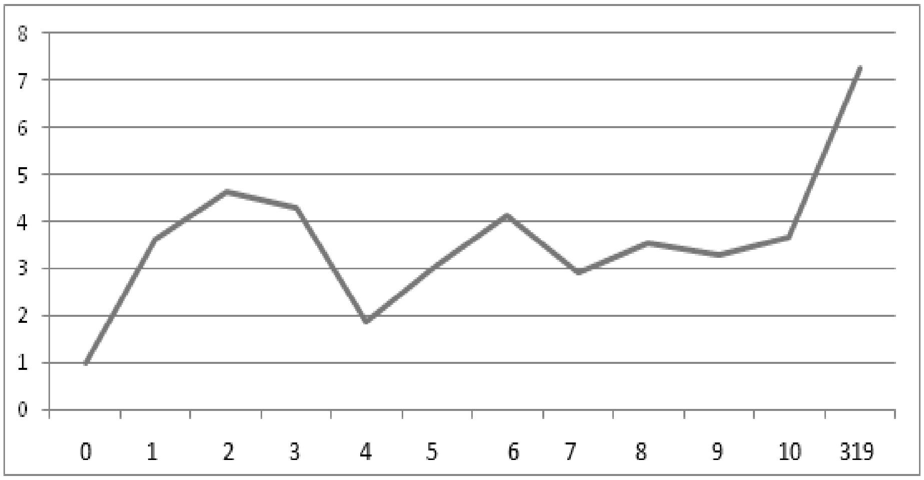


Figure 19 Improvement factor of the d-sequence of 1277 when divided into 319 blocks of size 4 digits each that is odd number of blocks

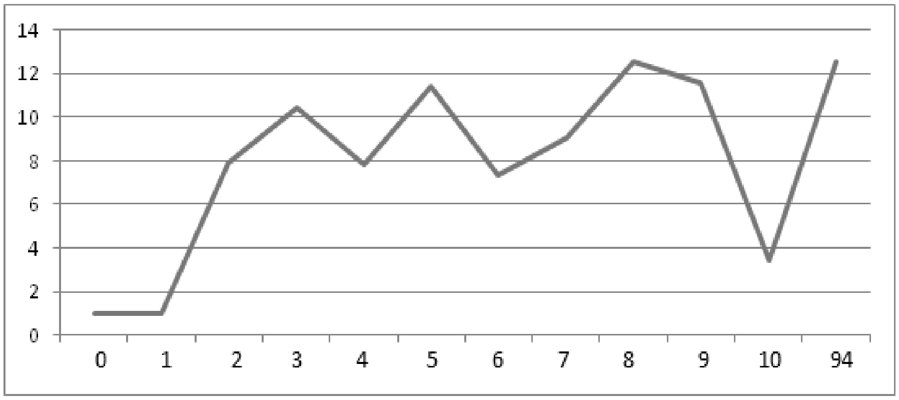


Figure 20 Improvement factor of the d-sequence of 1787 when divided into 94 blocks of size 19 digits each that is odd number of blocks

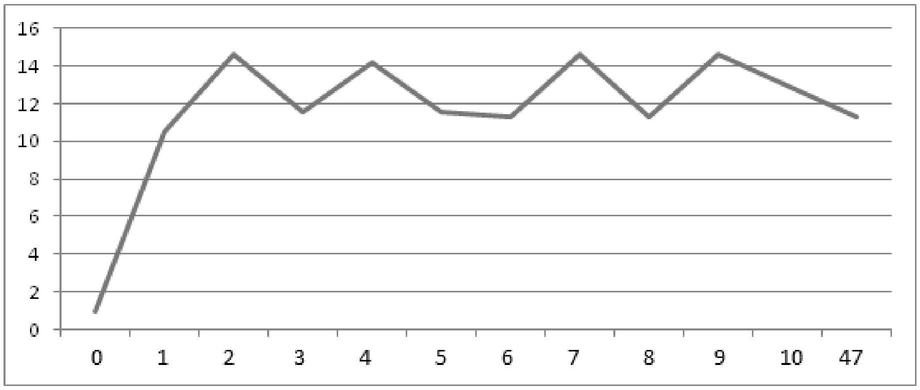


Figure 21 Improvement factor of the d-sequence of 1787 when divided into 47 blocks of size 38 digits each that is odd number of blocks

3.4 Conclusion

We show that permutations on blocks of random sequences improve their randomness. The improvement presented in the graphs is typical of the performance of d-sequences. The specific conclusion is that two or three permutations on blocks that are not too small suffice to improve the autocorrelation function of the sequence.

CHAPTER IV

INTENSITY AND STATE ESTIMATION IN QUANTUM CRYPTOGRAPHY

4.1 Introduction

The drawbacks of BB84 protocol are PNS attack, Trojan horse attack and faked states attack [31], [32], [39]. In Kak's multistage protocols [2],[4],[25] a bunch of photons can represent a single bit. Though these protocols are theoretically proven to be secure, they have the loophole that Eve can siphon off photons at multiple stages and obtain the information.

In the iAQC (Intensity Aware Quantum Cryptography) protocol [25] is a variant of three-stage where Alice and Bob track the intensity of the laser beam at each stage making it possible to detect the intruder. But the drawback of iAQC lies in the scenario when Eve removes some photons and replaces them with the same number of photons with random polarization back into the stream where the intensity remains constant. Such siphoning can be done by fiber tapping [35] or using half silvered mirrors if the communication media is free space. In this case the intensity is not changed and hence Eve will not be discovered and the changes in the state will be ascribed to noise. In order to overcome this threat from Eve, an additional step of detecting the state of photons using tomography [36] is considered. This new protocol is called ISA (intensity and state aware) quantum cryptography. A certain fraction of the received photons are examined for their intensity and state to determine if Eve has siphoned off photons and replaced them with other photons.

The ISA system can be used for the standard three-stage protocol or its many variations [3], [4], [17], [37] including the one-stage protocol [27]. We illustrate the process of state determination by examining only one transmission that is the two-stage protocol.

4.2 Intensity and state aware protocol (ISA)

In the ISA protocol, Alice keeps track of the state of the photons in addition to the intensity of the photons. If Eve introduces some photons with different polarization than that of Alice, then the resultant stream of photons sent to Bob is mixed state. Thus, Eve is caught if the state is detected to be mixed.

The density operator is a convenient way of representing a mixed state. Assuming that a quantum system is in one of the number of states $\left|\psi_i\right\rangle$, where i is an index with probabilities p_i, $\{ p_i \mid \psi_i \}$ is an ensemble of pure states. The density operator of the system is defined as $\rho = \sum_i p_i \left|\psi_i\right\rangle\left\langle\psi_i\right|$.

The main criterion to decide if a state is pure or mixed is considering the trace (*tr*) of the density matrix. If the *tr* is less than one then the state is said to be a mixed state else it is pure state.

Suppose that Eve siphons off *x* number of photons in the first stage and puts *x* number of photons with different polarization back into the stream. Therefore, a total of *2x* photons are siphoned off throughout the transmission. Eve will not be caught by the techniques that detect intruders unless the value of *2x* reaches a substantial fraction of the total number of photons sent by Alice. Alice has to use this technique of computation and comparison of density matrices to catch the eavesdropper. It is assumed that Alice picks up a random polarization angle, θ and sends pure state photons to Bob. In addition, Alice computes two density matrices, imagining that Bob makes a rotation of 0^{o} in one case and 90^{o} in the other case. Assuming that Bob makes a 0^{o} rotation on the photons that he receives, Alice computes the density matrix, ρ. Similarly, assuming that Bob makes a 90^{o} rotation, Alice computes the density matrix as ρ'.

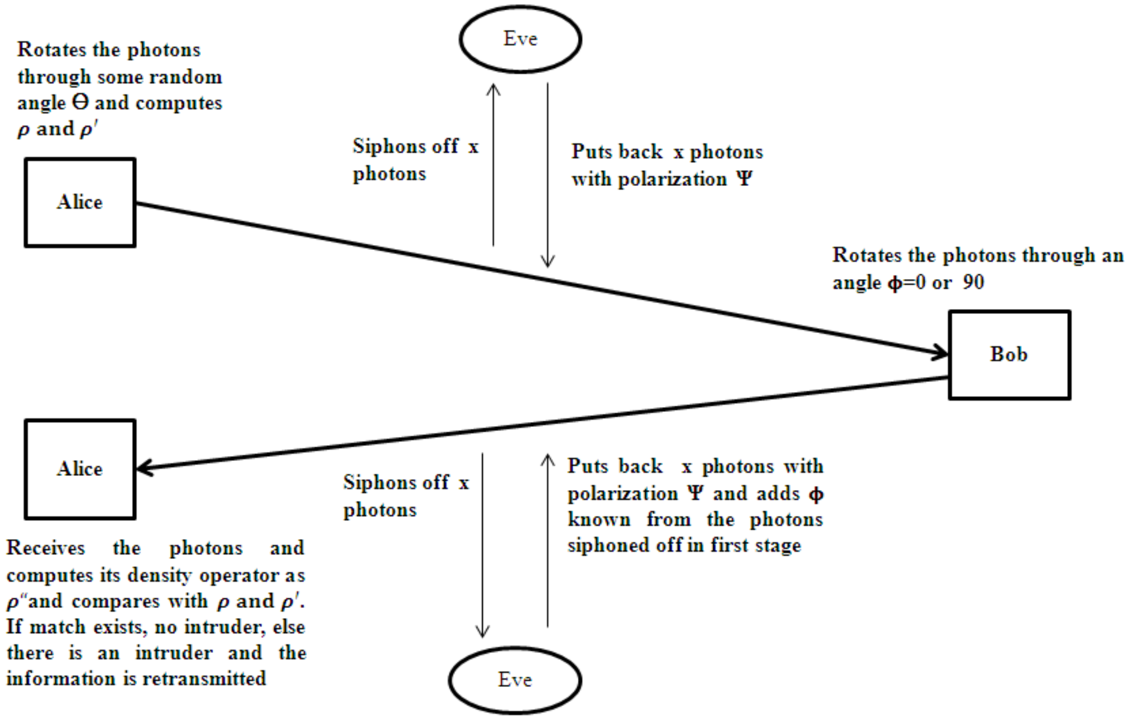

Eve
Rotates the photons through some random angle Θ and computes ρ and ρ'
Siphons off x photons
Puts back x photons with polarization Ψ
Alice
Rotates the photons through an angle ϕ=0 or 90
Bob
Alice
Siphons off x photons
Puts back x photons with polarization Ψ and adds ϕ known from the photons siphoned off in first stage
Receives the photons and computes its density operator as ρ“and compares with ρ and ρ'. If match exists, no intruder, else there is an intruder and the information is retransmitted
Eve

Figure 22 Intensity and State Aware Quantum Cryptography

Once Alice receives the photons from Bob in the second stage, she computes a new density matrix for that photon state as ρ'' and then compares it with ρ and ρ'. If there is no match, then Alice assumes that the state that she received is not pure and she makes sure by verifying if the trace of $(\rho'')^2$ is less than one which means that it is mixed state. This is how Eve is detected in this approach. Let the polarization of photons added by

Eve be φ. The following calculations show how Eve's interference is discovered. It is assumed that Alice sends a total of 100 photons with the polarization angle θ =30^{o}. Suppose that Eve siphons off 5 photons and injects 5 other photons with a random polarization, φ of about 45^{o} in the first stage. Then Bob rotates the photons by θ =0^{0}. Then in the second stage Eve takes 5 more photons and injects 5 photons with the same polarization, φ. That means 80 photons are with the state $\sqrt{3}/2|0\rangle + 1/2|1\rangle$ and 20 with state $1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle$. Now the density matrices ρ, $\rho'$and ρ'' computed by Alice are

$$\rho= \begin{bmatrix} 3/4 & \sqrt{3}/4 \\ \sqrt{3}/4 & 1/4 \end{bmatrix}; \rho' = \begin{bmatrix} 3/4 & \sqrt{3}/4 \\ \sqrt{3}/4 & 1/4 \end{bmatrix}; \rho'' = \begin{bmatrix} 0.7 & 0.4464 \\ 0.4464 & 0.3 \end{bmatrix}$$

which is quite different from that of ρ and ρ' and the trace of $(\rho'')^{2}$ is less than 1. Therefore, Eve is caught. If Alice finds that the photons are in pure state, she uses quantum tomography to find the unknown state. Figure 22 shows the ISA protocol. The next sections give a brief idea of the photon generation and detection process for better understanding of the quantum tomography.

4.3 Photon generation process

A set of photons are generated to represent a bit of information. We need a set of photons instead of a single photon for tomography purposes. A laser beam or a semiconductor Schottky diode device is used as a photon source. All the linearly polarized photons are sent through the polarizing equipment to obtain photons with required polarization angle. Alice and Bob negotiate on the set of polarization bases to be used and the notation each bit using the polarization angle, θ. A brief outlook of the photon generation process can be obtained from the Figure 23. There may be an error in the polarizing equipment which causes error in the information transfer. This category of error and the tolerance of the protocol to this error are explained in the next section.

4.4 Photon detection process

The photon detection process at the receiver site involves beamsplitters, half silvered mirrors and filters that contribute to the quantum tomography process. When the set of photons are received, they are sent through the beam splitters or half silvered mirrors to send them through different filters set up at required angles. The intensities at these filters are taken to construct the intensity vector, *v*. Now the nearest neighbor search algorithm is used to find the match in the stored vectors. Once the match is found the corresponding angle is said to be the polarization of the set of photons sent by Alice. Thus, the unknown state is determined. The process flow of the detection process at receiver's site is shown in the Figure 24.

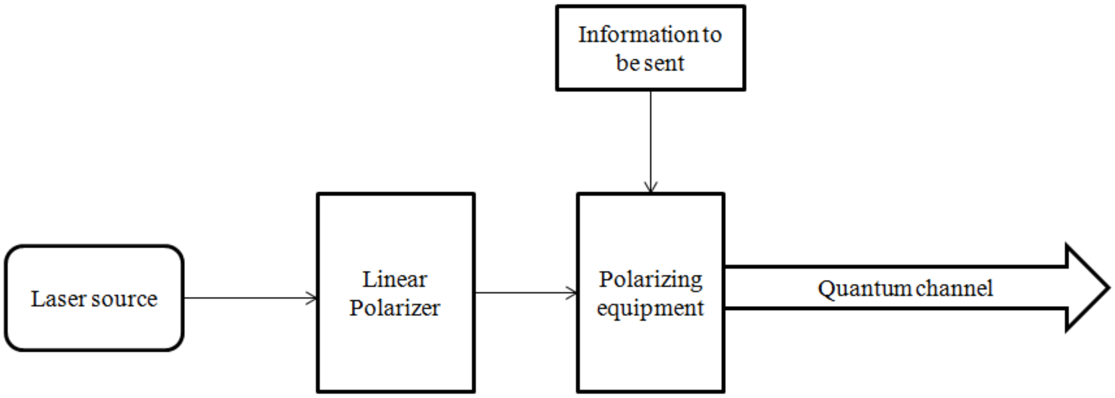


Figure 23 Photon generation process at the Sender's site

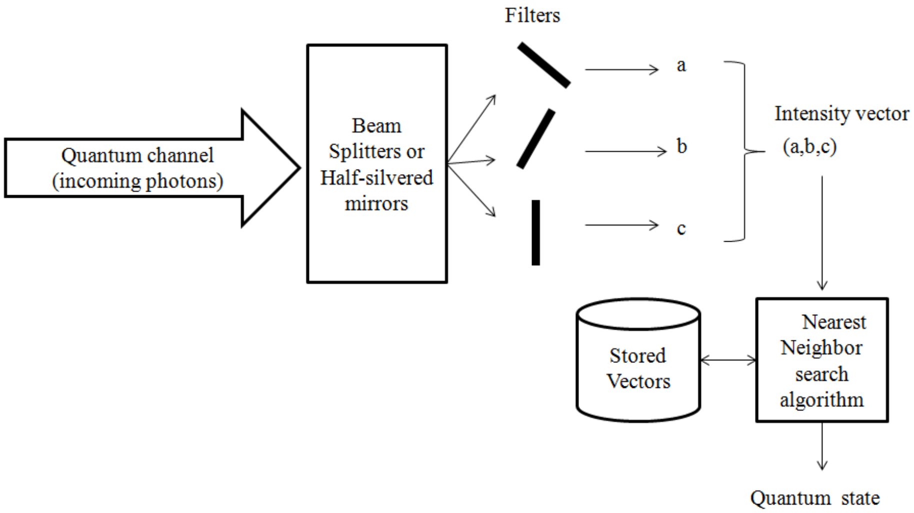

Filters
Quantum channel (incoming photons)
Beam Splitters or Half-silvered mirrors
a
b
c
Intensity vector (a,b,c)
Stored Vectors
Nearest Neighbor search algorithm
Quantum state

Figure 24 Photon detection and quantum tomography at receiver's site

4.5 Quantum state tomography

Alice has to measure the unknown quantum state to get the information sent by Bob. The process of estimating the unknown quantum state is quantum state tomography. The following section gives an overview of the existing theory on quantum state tomography. Then, my work on quantum state tomography is given in detail.

4.5.1 Overview of quantum state tomography

Initially, all the photons pairs are filtered using the spatial filters and frequency filters. After the filtering process, the unknown states are measured by the process of projection [36]. An arbitrary polarization measurement can be realized using a quarter-wave plate, a half-waveplate and a polarizing beam splitter (PBS) in an order. The quarter-wave plate and the half-waveplate are used to rotate the state to $|H\rangle$. Then the PBS will transmit the projected state and reflect its orthogonal compliment. The resultant measurement state is sent through the detectors and a photon counting circuit is implemented to maintain the coincidental counts. Using the likelihood function, the T matrix is obtained and using the T matrix density operator can be calculated as ρ= $T^{-1}T$ / Tr{ $T^{-1}T$} [36].

Once the density operator or matrix ρ is obtained, any single-qubit density matrix, ρ can be uniquely represented by three parameters {S_1, S_2, S_3} are the Stokes parameters such that $\rho = \sum_{i=1}^{3}(S_i\sigma_i)$ such that $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Measurements can also be made in any non-orthogonal bases. The following computation illustrates how Stokes parameters which correspond the measurement in the D/A (diagonal), H/V (rectilinear) and R/L (right-circular and left-circular) basis are calculated and their representation on the Poincaré sphere is shown. Note that in our case, the Stokes parameter (S_2) corresponding to the R/L basis is always zero. Suppose Alice receives a bunch of photons from Bob and obtains the density matrix as $\rho = \begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix}$. By the equation $S_i \equiv Tr\{\sigma_i \rho\}$, the Stokes parameters can be calculated as $S_0=1$, $S_1=1$, $S_2=0$, $S_3=0$. Since $\sum_{i=0}^{3} S_i = 1$, it indicates that the obtained state is pure state. Figure 26 shows the representation of these values in the Poincaré sphere. Since the state is on the surface, it is a pure state.

Any physical density matrix can be diagonalized and its corresponding eigenvalues and eigenvectors can be computed. The eigenvalues of ρ are {0.0000, 1.0000} and the corresponding eigenvectors are (-0.5000, 0.8660) and (0.8660, 0.5000) respectively. The eigenvalues of ρ'' are {0.0108, 0.9892} and corresponding eigenvectors calculated are (-0.5437, 0.8393) and (0.8393, 0.5437) respectively. The eigenvalues of any density matrix give the intensities and their corresponding eigenvector gives the angle at each intensity.

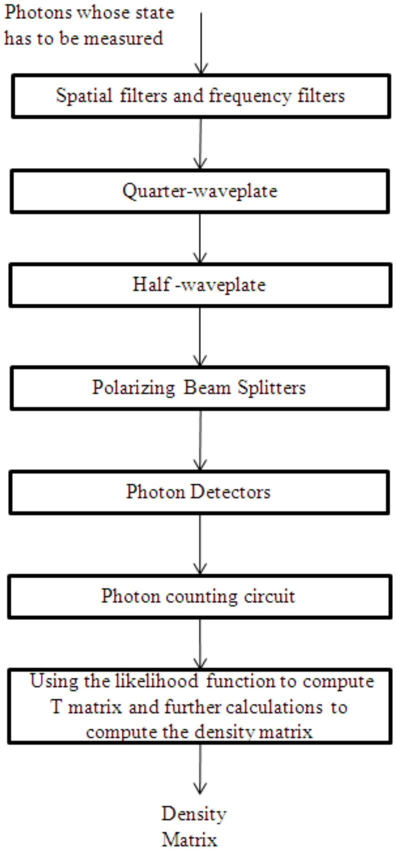

Photons whose state has to be measured
Spatial filters and frequency filters
Quarter-waveplate
Half -waveplate
Polarizing Beam Splitters
Photon Detectors
Photon counting circuit
Using the likelihood function to compute T matrix and further calculations to compute the density matrix
Density Matrix

Figure 25 Quantum tomography

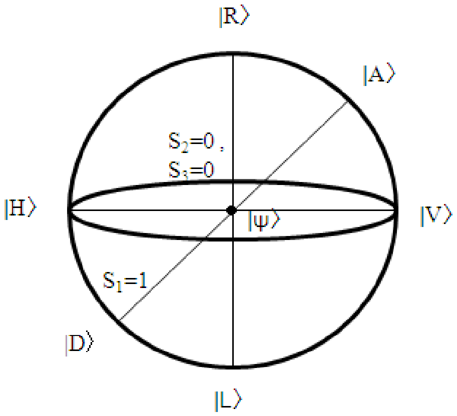


Figure 26 Poincaré sphere

4.5.2 Quantum state tomography for constrained polarization

Here we present a conceptually easy approach to quantum tomography where the polarization angles are defined on a fixed plane which is true of our protocols.

It is assumed that Alice and Bob negotiate on the number of polarization angles that should be used in their communication process. At Bob's site, the received photons are sent into a set of filters. These filters are aligned at certain angles chosen from the set of polarization angles. A peak exists at a particular filter whose angle is equal to that of the polarization of the photon. We now consider the question of how many photons do we need to determine an unknown state. Our experiments lead us to the following conjecture:

> *If there are n number of polarization angles equal to 2^m in a fixed plane, we need m number of filters and m^2 number of photons through each filter. Calculations starting with the base case are provided in the following paragraphs.*

For 4 polarization angles, we need 2 filters and a total of 2^3 photons. This is concluded from a set of experiments done. At the receivers end the photons are sent through filters aligned at different angles. The peaks obtained at these filters are put together to form an intensity vector as shown in Figure 24. Initially, we used one filter in the detection process, but it was not possible to determine the polarization angle of the photons since the vectors obtained were not unique. Then in the next trial, 2 filters are considered and the intensity vectors are found to be unique.

Further, the point of number of photons needed at each filter to get a convincing value of intensity is considered. Since an integer value of the intensity peak has to be obtained we keep on increasing the number of photons passed through each filter until we get an integer value of the component of the intensity vector. Thus, the trials began with passing one photon through each filter and then increasing the number by one each time. It is found that at the point where we sent 2 photons to each filter, we obtained integer values of intensity vectors that were precisely unique. The uniqueness of the vectors helps us to determine the unknown state. The vectors obtained by passing the photons with polarization angle chosen from the set of four polarization angles, {0^0, 45^0, 90^0, 135^0 } are stored at the receiver's database. Thus, whenever a new set of photons arrive at receiver's site, they are sent through the filters with the help of beamsplitters or half-silvered mirrors. The output of these filters forms a new vector which is then compared with the stored vectors following the Nearest neighbor search algorithm to get the nearest match and therefore to get the unknown state of the photons.

For example, the vectors for each possible value of θ for a protocol which uses 8 polarization angles are stored at the Bob's site in the form of Table 5. When Alice sends a set of photons with polarization θ= {0, 22.5, 45, 67.5, 90, 112.5, 135, 157.5}, at Bob's site, they are sent through the three filters to get the intensity vector, V. This V is compared with the existing vectors {(3 3 2), (3 3 3), (1 3 3), (0 2 3), (0 0 1), (0 0 0), (2 0 0), (3 2 0)}. When a match is found, the polarization is determined which gives the state of the photons. Even if there is slight deviation in the vector obtained, then the Nearest neighbor search algorithm is applied to find the closest vector that matches. The Euclidean distance between two vectors, (a_1, b_1, c_1) and (a_2, b_2, c_2) is calculated as $\sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2 + (c_1 - c_2)^2}$ where (a_1, b_1, c_1) is the stored vector and (a_2, b_2, c_2) is the vector that is obtained when the photons sent by Alice are passed through filters.

Once the matching vector is found, the corresponding angle determines the unknown state of the photons sent by Alice. Similarly, the experiment is done for 8, 16, 32, 64 and 128 polarization angles and the results are shown in Table 5 which support the conjecture.

Table 4 Possible intensity vectors for a setting with 8 polarization angles

Polarization of the photon sent by Alice	Filter at 0^0	Filter at 22.5^0	Filter at 45^0	Intensity Vectors (Stored Vectors)
0^0	3	3	2	(3, 3, 2)
22.5	3	3	3	(3, 3, 3)
45	1	3	3	(1, 3, 3)
67.5	0	2	3	(0, 2, 3)
90	0	0	1	(0, 0, 1)
112.5	0	0	0	(0, 0, 0)
135	2	0	0	(2, 0, 0)
157.5	3	2	0	(3, 2, 0)

For some choice of filters, we might need lesser number of photons than m^2. Figure 27 shows a graph where the dotted line indicates the number of photons that suffice to measure the polarization angle for some optimal combination of filters. The square line indicates the at most number of photons needed in general for 4 through 64 polarization angles.

The graphs in the following section show the change in intensities as the number of photons siphoned off by Eve changes. The angle by which Alice rotates the photons is denoted by θ and the polarization of photons inserted by Eve as φ. The graph in Figure 28 indicates the intensities of photons at the highest peak obtained when $\theta = 22.5^0$ and φ $=30^0$.

Table 5 Number of photons and filters required in the tomography process

Number of polarization angles	Number of filters	Total number of photons
4	2	8
8	3	27
16	4	64
32	5	125
64	6	216
128	7	343

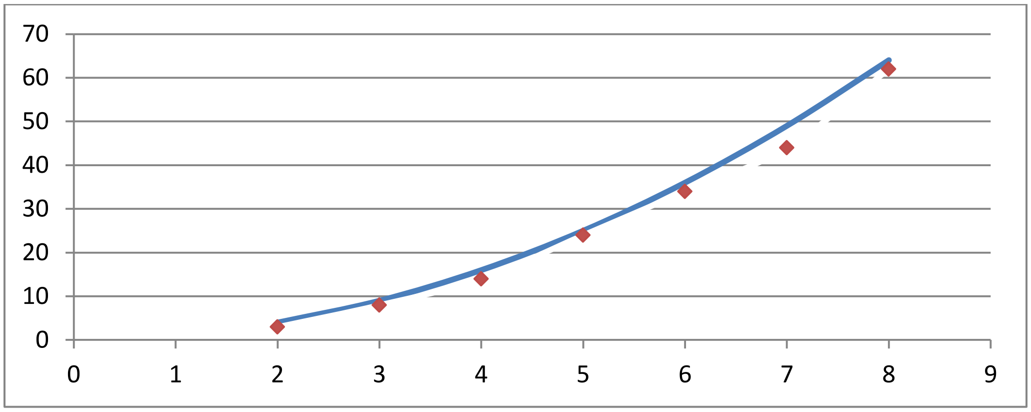


Figure 27 Graph to show the number of filters varying for each set of polarization angles

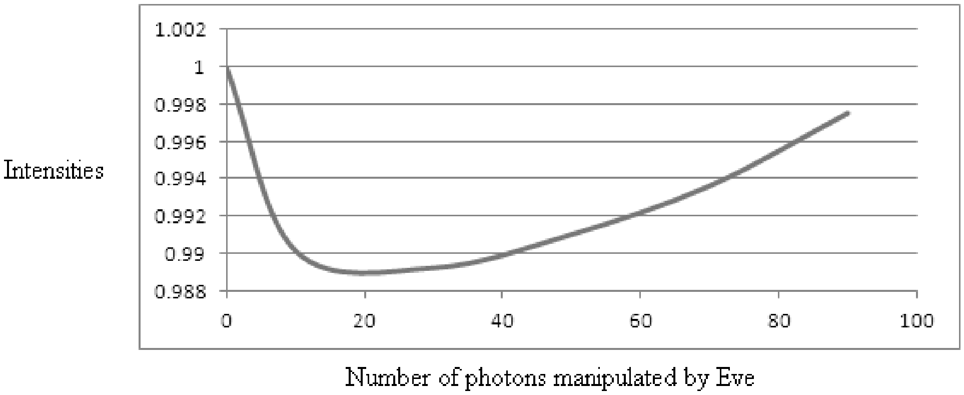


Figure 28 Graph showing the varying peak intensities with change in number of photons manipulated by Eve when $\theta = 22.5^0$ and $\varphi = 30^0$

Figure 29 to Figure 35 indicate the angle at which the intensity is high and the peak intensities varying with the number of photons manipulated by Eve. The examples are considered with difference between angle used by Alice and Eve that is (θ-φ) as 7.5^0, 15^0, 30^0 and 60^0. The intensities and the values of angle are obtained by the computation of eigenvalues and eigenvectors.

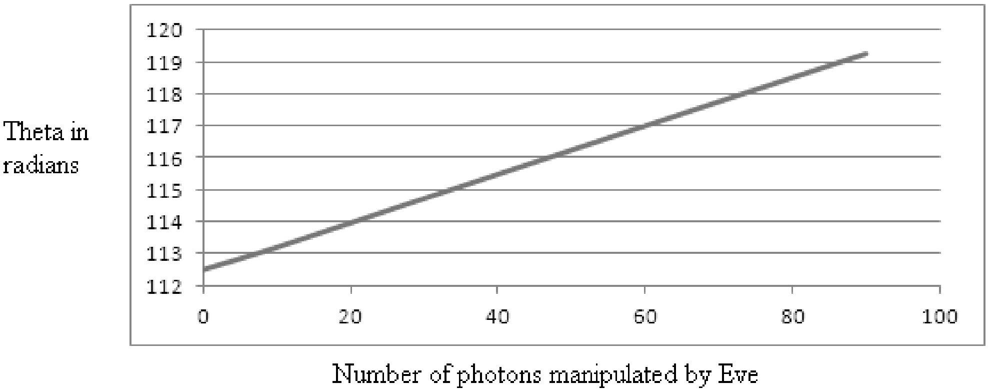


Figure 29 Graph showing the varying values of angle whose intensities are high with change in number of photons manipulated by Eve when $\theta = 22.5^0$ and φ $=30^0$

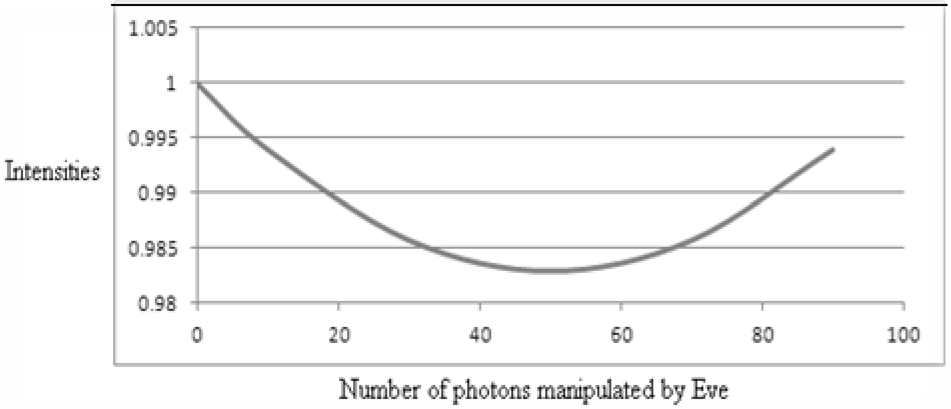


Figure 30 Graph showing the varying peak intensities with change in number of photons manipulated by Eve when $\theta = 45^0$ and φ $=60^0$

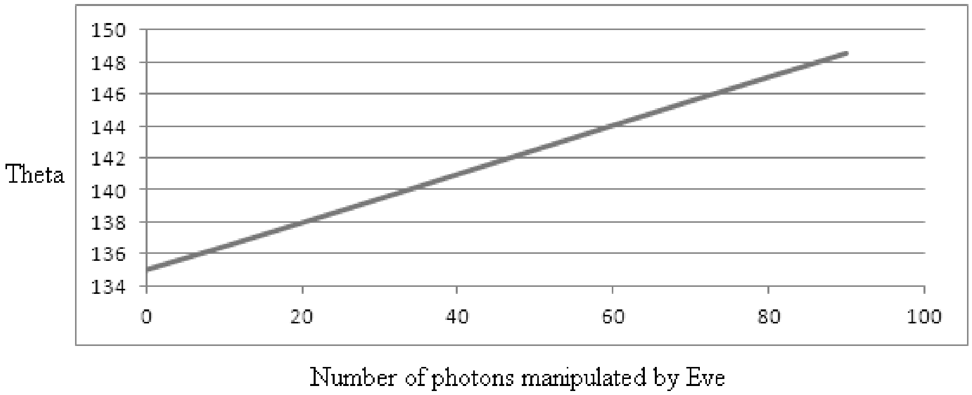


Figure 31 Graph showing the varying values of angle whose intensities are high with change in number of photons manipulated by Eve when $\theta = 45^0$ and φ $=60^0$

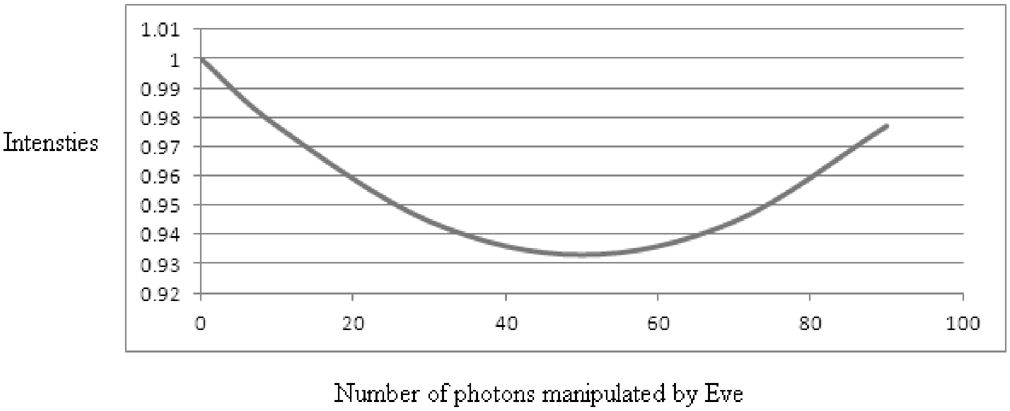


Figure 32 Graph showing the varying peak intensities with change in number of photons manipulated by Eve when $\theta = 30^0$ and φ $=60^0$

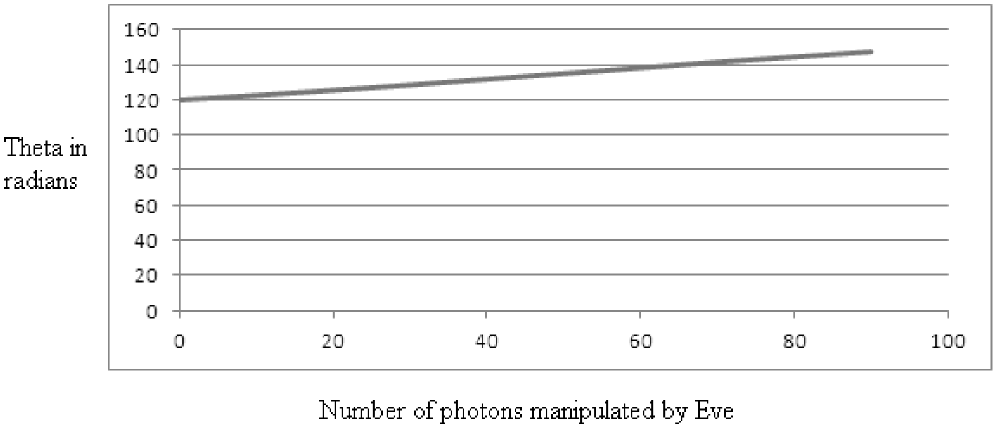


Figure 33 Graph showing the varying values of angle whose intensities are high with change in number of photons manipulated by Eve when $\theta = 30^0$ and φ $=60^0$

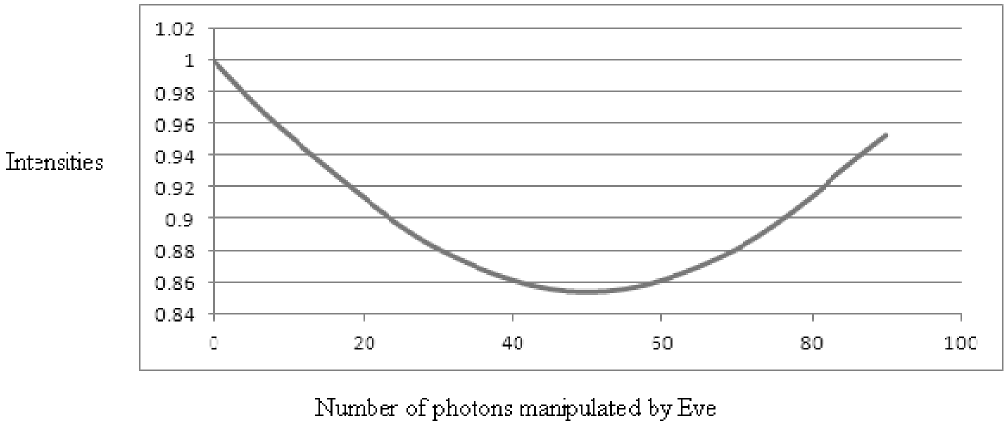


Figure 34 Graph showing the varying peak intensities with change in number of photons manipulated by Eve when $\theta = 30^0$ and φ =90^0

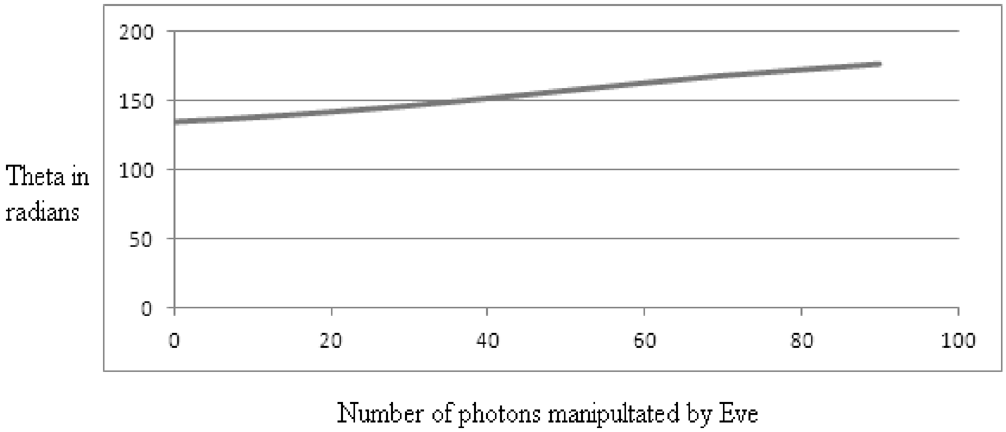


Figure 35 Graph showing the varying values of angle whose intensities are high with change in number of photons manipulated by Eve when $\theta = 30^0$ and φ =90^0

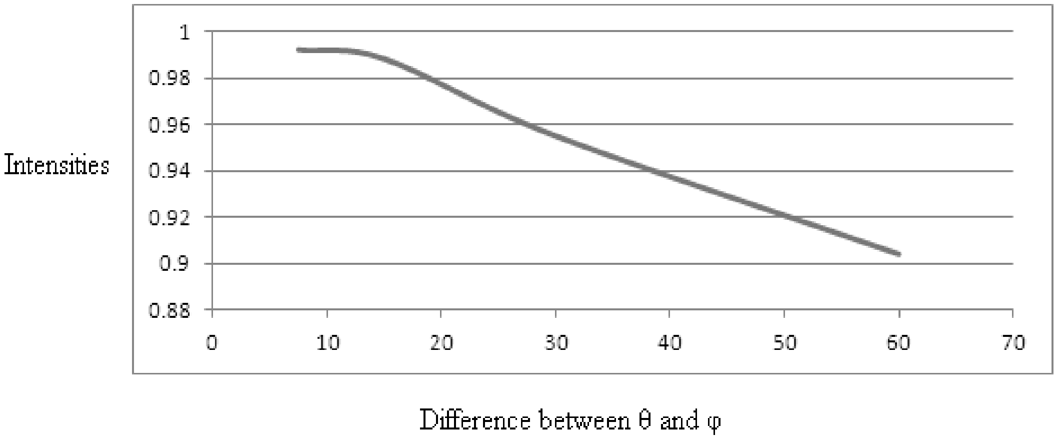


Figure 36 Graph showing the varying values peak intensities with the difference between θ and φ equals 7.5^0, 15^0, 30^0 and 60^0

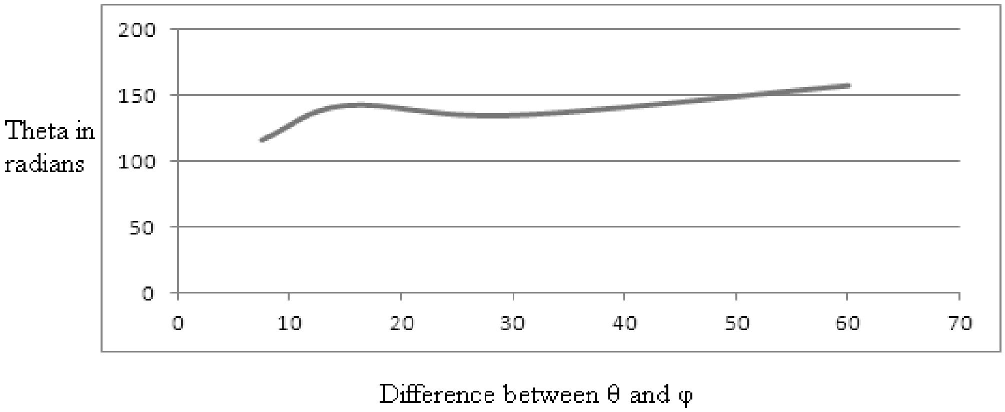


Figure 37 Graph showing the varying values of angles at peak intensities with the difference between θ and φ equals 7.5^0, 15^0, 30^0 and 60^0

Combining the results from all the above experiments, the graphs in Figure 36 and Figure 37 are obtained. The Figure 36 shows the varying peak intensities as the difference between θ and φ varies. Similarly Figure 37 shows the varying angle at the peak intensities as the difference between θ and φ varies.

4.6 Noise analysis on ISA quantum cryptography protocol

4.6.1 Types of noise

The existence of noise can be in any of the three possible ways. The first type of noise can be due to an error in the equipment that rotates the photons. This causes an error in the polarization of the photons which affects the quantum state on the whole. The next type of noise can occur in the photon generation process where the number of photons generated is affected. Another type of error that is possible is the error in the detectors that detect the photons.

4.6.2 Relating noise to the ISA quantum cryptography protocol

We consider the first type of error that is, a flaw in the rotation equipment. Chapter III considered the presence of this type of noise in the two stage and three stage protocols. Let the angle of polarization is θ and the error introduced be φ.

We assume that the error angle, φ introduced by the faulty equipment ranges from -4^0 to +4^0. Let us now try to understand the effect of this type of error on ISA protocol by the following example.

Consider a protocol with 8 polarization angles. Assume that the filters used are at angles 0^0, 22.5^0, 45^0 and the vectors stored at the receiver's site are as shown in the Table 6. If the angle of polarization is 0^0, then the expected intensity vector is found to be (3, 3, 2). From the following table it is found that the match exists for all $\theta+\varphi$ and the vectors are exactly the same as the intensity vector for θ=0^0. Similarly when φ ranges from 0^0 to +4^0, match exists in all the cases. Therefore, this theoretical experiment is done for all the cases of angle, θ with error, φ ranging from -4^0 to +4^0 that is φ ={-4.0, -3.5, -3.0, -2.5, -2.0, -1.5, -1.0,-0.5, 0, +0.5, +1.0, +1.5, +2.0, +2.5, +3.0, +3.5, +4.0}.

Table 6 Probability of error for each polarization angle

Possible Polarization Angles	Probability of error
0^0	0
22.5^0	13/16
45^0	13/16
67.5^0	1
90^0	0
112.5^0	13/16
135^0	13/16
157.5^0	13/16

The impact of error on the protocol in the case of $\theta=0^0$ and $\theta=90^0$ is zero. This indicates that the effect of noise due to error in the polarizing equipment is zero in case of the photons with polarization $\theta=0^0$ and $\theta=90^0$

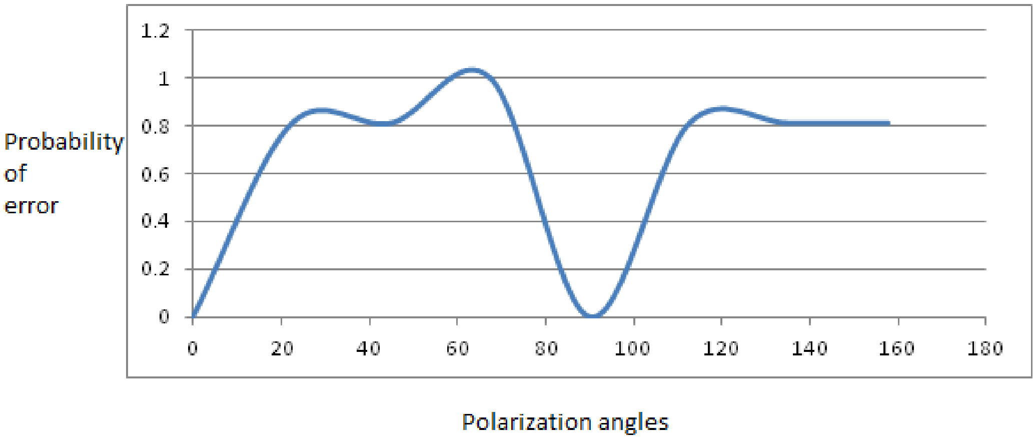


Figure 38 Probability of error in the vectors when there is a noise in the polarizing equipment

The second possible error is in the photon generation process. If the number of photons generated is not up to the threshold, then there might be an error in the tomography process. The following paragraphs explain this category of noise in detail.

Table 3 shows the number of filters required in the tomography process for different number of polarization angles. For some choices of filters, if the number of photons is less than the required, then the resultant vector might match with more than one stored vector which makes it difficult to determine the polarization state of the photons. Let us consider the case of 8 polarization angles of a protocol. In this case, the number of photons required is less than or equal to 9 photons at each filter. Here, we consider the filters chosen in table 4. Let us consider the cases where the photons generated are 8, 7, 6 and 5 due to the error in generation process. If 8 photons are generated, still the vector can find a unique match with the stored vectors and there is no error found in the tomography process. Similar is the case with 7, 6 photons generated due to error. But if the number of photons generated is less than 6 then the vector obtained matches with more than one stored vector. 5 out of 9 possibilities result in error. Similar experiment is done for the 16 through 64 polarization angles and the results are shown in the Table 7. In the case of 16 polarization angles, ISA protocol has good tolerance till the number of photons is not less the actual required number of photons minus two. Otherwise the vector obtained would have more than one match with the stored vectors.

Table 7 Uniqueness of the vectors as the number of photons generated decreases

Number of photons generated and sent through each filter	Choice of filters		
	0, 45, 90, 135	22.5,45,67.5,90	45, 90, 135, 168.75
16	Unique match	Unique match	Unique match
15	Unique match	Unique match	Unique match
14	No unique match	No unique match	No unique match
13	No unique match	No unique match	No unique match
Probability of error	14/16	14/16	14/16

In the case of 16 polarization angles, the best choice of filters in an error prone protocol is a set of filters with a difference of 22.5^0. Similarly when this experiment is run for the set of 32, 64 and 128 polarization angles, 13 out of 16 cases are found to be error prone. If the number of photons sent is more than the required, then the newly computed vector may deviate from the existing vectors. But in this case, the Nearest neighbor search algorithm can be used to find out the match.

Therefore, we can conclude that any protocol which defines n polarization angles and that requires m number of photons at each filter has an error tolerance of about m-1. It might reach m-2 with some other choice of filters.

The third type of noise is caused due to the error in the detection process. The fault may be in any of the detecting equipment like beam splitters, half-silvered mirrors or the orientation of the filters. The tolerance to the noise in the protocol is similar to that of the generation process as the effect is on the number of photons.

4.7 Conclusion

The ISA protocol overcomes one of the drawbacks of iAQC and helps to detect the intruder by tracking the state of the photons. Detection of mixed state shows the presence of Eve in the communication link. The polarization angles are defined on a fixed plane in our protocols. A conceptually easy way to approach quantum tomography in these protocols is explained. The tolerance of the intensity and state aware protocol is investigated for various noise environments.

CHAPTER V

CONCLUSION

This thesis is on improving the randomness of a sequence and developing a protocol for quantum cryptography that estimates both intensity and state. Our proposed ISA protocol adds state estimation to the iAQC protocol. Our work is also applicable to the one-stage and the multi-stage protocols.

Since random sequences play a vital role in choice of bases in BB84 protocol and choice of polarization of states in multistage protocol, the improvement in randomness of the sequence strengthens the protocols. The randomness of the sequence can be improved by applying permutations on its blocks and the randomness is measured with the autocorrelation graphs and randomness measure formula.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175–179 (IEEE, New York, 1984).

[2] S. Kak, A three-stage quantum cryptography protocol. Foundations of Physics Letters 19: 293-296, 2006.

[3] Y. Chen, P. Verma, and S. Kak, Embedded security framework for integrated classical and quantum cryptography in optical burst switching networks. Security and Communication Networks 2: 546-554, 2009.

[4] S. Kak, Quantum information and entropy, International Journal of Theoretical Physics 46: 860-876, 2007.

[5] A. Rukhin et al, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST, 2010.

[6] A.N. Kolmogorov, Three approaches to the quantitative definition of information. Problems Inform. Transmission 1 (1): 1–7, 1965.

[7] S. Kak, Active agents, intelligence, and quantum computing. Information Sciences 128: 1-17, 2000.

[8] S. Kak, The universe, quantum physics, and consciousness. Journal of Cosmology 3: 500-510, 2009.

[9] S. Golomb, Shift Register Sequences. San Francisco, Holden–Day, 1967

[10] S. Kak and A. Chatterjee, On decimal sequences. IEEE Transactions on Information Theory, IT-27: 647 – 652, 1981.

[11] S. Kak, Encryption and error-correction coding using D sequences. IEEE Transactions on Computers C-34: 803-809, 1985.

[12] S. Kak, New results on d-sequences. Electronics Letters 23: 617, 1987.

[13] D. Mandelbaum, On subsequences of arithmetic sequences. IEEE Trans on Computers 37: 1314-1315, 1988.

[14] S Kak, Prime reciprocal digit frequencies and the Euler zeta function. http://arxiv.org/ftp/arxiv/papers/0903/0903.3904.pdf

[15] S. Rangineni, Cryptographic hardening of d-sequences. http://arxiv.org/abs/1106.3574

[16] D. R. Hjelme, L. Lydersen, V. Makarov, Quantum cryptography. arXiv:1108.1718

[17] S. Kak, P. Verma, and G. MacDonald, Cryptography and state estimation using polarization states. SPIE Conference on The Nature of Light: What are Photons IV? August 2011.

[18] Gerhardt, Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., and Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nat. Commun. 2, 349 (2011)

[19] L. Lydersen, Wiechers, C., Wittman, C., Elser, D., Skaar, J. and Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. Nat. Photonics 4, 686 (2010)

[20] T. Usuki, Y. Sakuma, S. Hirose, K. Takemoto, N. Yokoyama, T. Miyazawa, M. Takatsu, Y. Arakawa, Single-photon generator for optical telecommunication wavelength. Journal of Physics: Conference series, vol. 38 140, 2006.

[21] S. Kak, Quantum information in a distributed apparatus. Foundations of Physics 28: 1005-1012, 1998.

[22] S. Kak, Information, physics and computation. Foundations of Physics 26: 127-137, 1996.

[23] S. Kak, The initialization problem in quantum computing. Foundations of Physics 29: 267-279, 1999.

[24] U. Seyfarth, G.M. Nikolopoulos, G.Alber, Symmetries and security of a quantum-public key encryption based on single-qubit rotations. Phys. Rev. A 85, 022342, 2012.

[25] S. Kak, The intensity-aware quantum cryptography protocol. arXiv:1206.6778

[26] H.P. Yuen, Problems of Existing Unconditional Security Proofs in Quantum Key Distribution. arXiv:1109.1051.

[27] J.H. Thomas, Variations on Kak’s three stage quantum cryptography protocol. arXiv:0706.2888

[28] W. Perkins, Trusted Certificates in Quantum Cryptography. arXiv:cs/0603046

[29] Basuchowdhuri, Classical Authentication Aided Three-Stage Quantum Protocol. arXiv:cs/0605083

[30] S. Chitikela, Noise analysis for two quantum cryptography protocols. arXiv:1207.7281

[31] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nat. Commun. 2: 349-352, 2011.

[32] IL. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination. Nat. Photonics 4: 686-689, 2010.

[33] T. Usuki, Y. Sakuma, S. Hirose, K. Takemoto, N. Yokoyama, T. Miyazawa, M. Takatsu, Y. Arakawa, Single-photon generator for optical telecommunication wavelength. Journal of Physics: Conference Series 38: 140-143, 2006.

[34] S. Kak, The piggy bank cryptographic trope. arXiv:1301.0313

[35] K. Shaneman, S. Gray, Optical network security: technical analysis of fiber tapping mechanisms and methods for detection & prevention. Military Communications Conference, 2: 711-716, 2004.

[36] J.B. Altepeter, E.R. Jeffrey and P.G Kwiat, Photonic state tomography. vol. 52 of Advances in Atomic, Molecular, and Optical Physics, pp. 105-159, Academic Press, 2005.

[37] S. Mandal et al., Multi-photon implementation of three-stage quantum cryptography protocol. International Conference on Information Networking, 2013.

[38] Arya, S., D. M. Mount, N. S. Netanyahu, R. Silverman, and A. Y. Wu. An Optimal Algorithm for Approximate Nearest Neighbor Searching in Fixed Dimensions. Journal of the ACM, vol. 45, no. 6, pp. 891–923.

[39] Rahul Agarwal, Heeren Sharma, Deepak Gupta, Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol, International Journal of Computer Applications, Volume 20.

VITA

SINDHU CHITIKELA

Candidate for the Degree of

Master of Science

Thesis: METHODS TO COUNTER ATTACKS ON QUANTUM CRYPTOGRAPHY PROTOCOLS

Major Field: Computer Science

Biographical:

Education:

- Master of Science in Computer Science at Oklahoma State University, Stillwater, Oklahoma, May, 2013.
- Bachelor of Technology in Computer Science and Engineering at Jawaharlal Nehru Technological University, Hyderabad, Andhra Pradesh/India, 2011.

Experience:

- Graduate Research Assistant at CS department, OSU from August 2011 to May 2013
- Computer Assistant at ITLabs, OSU from August 2011 to May 2013
- Software developer Intern at TMW Systems, Oklahoma city from June 2012 to August 2012