UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

THE IMPACT OF NUMBERS OF PHOTONS AND COHERENT STATES ON MEASUREMENT ERROR IN Y-00 USING ML-POVM

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

MASTER OF SCIENCE

By

MITUN TALUKDER
Norman, Oklahoma
2016

THE IMPACT OF NUMBERS OF PHOTONS AND COHERENT STATES ON MEASUREMENT ERROR IN Y-00 USING ML-POVM

A THESIS APPROVED FOR THE
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

BY

Dr. Kam Wai Clifford Chan, Chair

Dr. Pramode Verma

Dr. Samuel Cheng

Acknowledgements

I would first express my profound gratitude to my thesis supervisor Dr. Kam Wai Clifford Chan who guided me through-out the entire process of my Master's degree. His consistent supervision, patience, deep knowledge on research work, and motivation helped me a lot of conducting my research work in right direction. I would like to thank him for his belief in my abilities and always there for me when I needed it. Next, I would like to express my sincere gratitude to Dr. Pramode Verma and Dr. Samuel Cheng for their valuable feedback and encouragement. Without their kind help and support, this research work could not have been executed successfully.

This work is the outcome of great collaboration of our quantum team. The fruitful discussion in weekly quantum team meeting pave the way for this research work. I would like to convey my deepest gratitude to my colleagues, Lu Zhang and Kyrus Kuplicki for their precious support, valuable comments and insightful discussion on my research work. I would like to thank our administrative assistant, Renee Wagenblatt for being such a supportive figure.

Finally, I would like to express my heartfelt gratitude to my parents for their continuous support and encouragement throughout my two years of study.

Table of Contents

List of Tables

List of Figures

Abstract

In this thesis, a lower bound between non-orthogonal coherent states and mean photon number in quantum noise randomized stream cipher (Y-00) for a given measurement error probability is proposed and compared against other measurement schemes. In this analysis, recently discovered maximum likelihood positive operator valued measure (ML-POVM) approach in a multiphoton regime is used to provide more accurate and optimum results than greedy scheme, quantum unambiguous measurement (QUM), and random guessing for which we have considered success probability of coherent state detection as a figure of merit. Moreover an analysis about the impact of erroneous output sequence of a pseudo random number generator (PRNG) in predicting the running seed key is studied.

In general, Y-00 scheme utilizes an initial shared secret key between legitimate users for which users experience superior receiver performance than does the intruder who does not know the key. An intruder suffers unavoidable quantum noise while probing the communication between legitimate users, owing to the user's ignorance of the secret key. In particular, an indefinite bound was proposed earlier between the number of non-orthogonal coherent states and the mean photon number in Y-00 scheme. In this research work, a lower bound is proposed using ML-POVM, where ML-POVM provides better probability of detection of a given number of coherent states and mean photon number than other measurement techniques can detect.

Finally, a simulation of linear feedback shift register (LFSR) is carried out as an example of PRNG for various number of bit-flip errors in the output sequence of LFSR to analyze the impact of erroneous output sequence in predicting the running seed key of LFSR, which demonstrates that a significant number of bit-flip errors is required to make the seed key indistinguishable from the observation of the output sequence of LFSR.

Chapter 1: Introduction

Today's world is experiencing ever increasing growth in data volume. Data disseminated by computing devices causes a significant amount of information-flow on the network. Hence, security in the core network, especially in the datacenter, is of prime importance nowadays to prevent cyber-attacks. The eavesdropper always poses a potential threat to information security. Moreover, security provided by classical cryptographic technologies is bounded by mathematical algorithms and complexities and is always challenged by the computational power of computing devices and new cryptanalysis techniques. In addition, there is no viable option to track information loss between legitimate users. In contrast, quantum cryptography provides security utilizing the law of quantum mechanics, therefore, this approach can provide unconditional security on the data transferred between legitimate users.

In a quantum cryptographic approach, signal degradation is directly related to information loss for eavesdropper. Quantum cryptography follows Heisenberg's "uncertainty principle" [1] and "no-cloning theorem" [2] both of which ensure data integrity, confidentiality, authenticity, and privacy between two legitimate users. So far, there are several types of quantum key distribution protocols that have been proposed and extensively investigated by implementation. The pioneering quantum cryptographic approach, BB-84 protocol [3] suffers in practical implementation, as it utilizes single photon or weak coherent states, and due to weak signal strength, this approach is not practically realizable in long distance optical fiber communication. In order to overcome the problem associated with single photon communication, multiphoton fault-tolerant approaches are proposed. In Table 1 lists different types of multiphoton communication protocols.

Approach Name	Examples
QKD with multi-photon entangled states	Fully device independent QKD, measurement device independent QKD etc.
QKD using quantum stream cipher	Keyed Communication in Quantum Noise (KCQ), α/η scheme
Continuous-variable protocols	Gaussian protocols, discrete-modulation protocols etc.
QKD using dynamic quantum session key	Braided single stage protocol
Multiple stage QKD	Random polarization based three-stage protocol

Table 1. Multiphoton Quantum Communication Protocol

In this chapter, a brief overview of cryptography is given followed by comparative analysis of mathematical and quantum cryptography. Then a generic description of quantum key distribution using a single photon approach and a multiphoton approach is discussed. Finally, the problem statement and contribution of this thesis is presented.

1.1 Cryptography

Cryptography is the study of the techniques to exchange data securely between legitimate users in the presence of third party, called an eavesdropper [4]. Information security such as data integrity, data confidentiality, data authenticity, data non-repudiation is the main focus of cryptography. Cryptography lies in the intersection of the disciplines of mathematics, physics, computer science, and electrical engineering. There are a few specific terminologies used in cryptography [5]:

Plaintext: information that a sender wants to exchange with a legitimate receiver.

Cipher text: the encrypted/obscured version of plaintext.

Key: a variable value or information that is applied to plaintext/cipher text using an encryption/decryption algorithm. The secrecy of the key provides the security of the cryptographic system.

Encryption: process of converting plaintext to cipher text.

Decryption: process of converting cipher text back to plaintext.

Cryptographic Scheme: a particular process of encryption and decryption.

Cryptanalysis: techniques used to decrypt cipher text without prior knowledge of encryption.

Cryptology: the study of cryptography and cryptanalysis.

In Fig. 1 depicts a typical diagram of cryptographic approach. Generally, plaintext is converted into intermediate state or cipher text by the application of the encryption algorithm and key. This cipher text is then transmitted to the intended receiver. After receiving this cipher text, the legitimate receiver gets the original plaintext using the decryption algorithm and key.

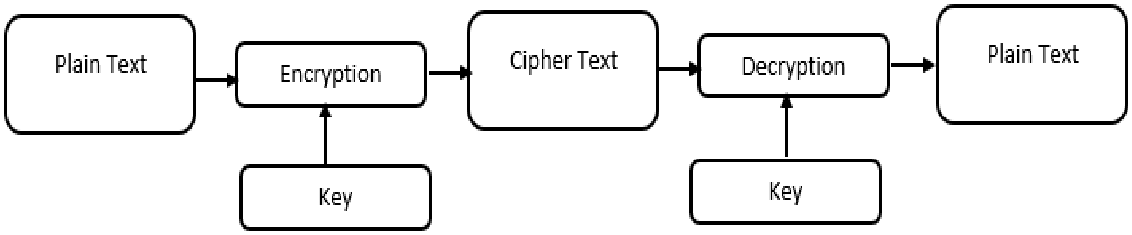


Fig. 1. A typical diagram of quantum cryptographic approach

It is worth mentioning that the strength of a cryptographic scheme depends on the strength of the key. There is the Kerckhoff' principle – "*only secrecy of the key* *provides security.*” While developing any cryptographic scheme, it is pre-assumed that the eavesdropper knows about the system - the underlying encryption and decryption algorithm. The only thing the eavesdropper does not know is the *“key.”*

1.2 Mathematical Cryptography

The cryptographic approach can be divided into many sub-divisions such as classical cryptography, modern cryptography, etc. Modern cryptography depicts the rise of the computer era. Modern cryptography can be broadly sub-divided into two major sections: mathematical and quantum cryptography. The strength or security of the mathematical cryptography solely depends on the mathematical complexity of the cryptographic algorithm. There are two strong requirements for mathematical cryptography:

1. The encryption algorithm should be “mathematically strong” to break. Here, “mathematically strong” encompasses both space and time complexity of the encryption algorithm.
2. Both legitimate users must obtain the key in a secure fashion. If this key and encryption algorithm were known by the eavesdropper, the whole communication process can be easily intercepted by the eavesdropper.

1.2.1 Classification of Mathematical Cryptography

Mathematical cryptography can be sub-divided into symmetric-key and public-key, or asymmetric key cryptography. A symmetric-key cryptographic scheme consists of plaintext, encryption and decryption algorithm, cipher text and key [5]. In Fig. 2, a simplified version of symmetric-key encryption is shown.

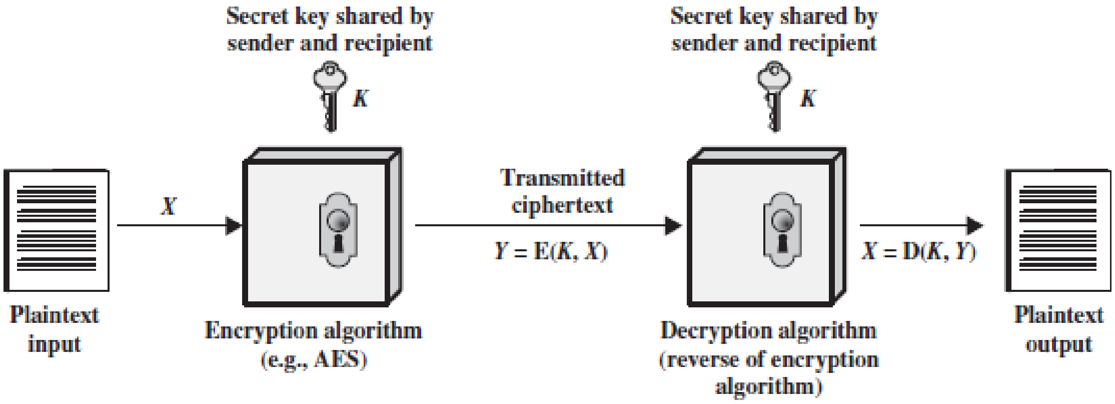

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig. 2. A simplified version of symmetric encryption [5]

The basic criteria of this type of cryptographic scheme is that the same key will be shared between sender and receiver. The key is independent of the plaintext, cipher text, and cryptographic algorithm such as encryption or decryption scheme. For the same plaintext, a different key will generate a different cipher text or a scrambled message using the same encryption algorithm. As it is seen in Fig. 2, plaintext is converted into cipher text using a shared secret key and encryption algorithm. After reception, the cipher text is converted to the original plaintext using the same key and decryption algorithm. If the plaintext input is X, encryption key is K, the encryption algorithm is E, the cipher text, Y, which can be written as,

$$Y = E(X, K), \tag{1.1}$$

The legitimate receiver with the same shared key can retrieve the original plaintext from the cipher text using decryption algorithm, D as follows:

$$X = D(Y, K). \tag{1.2}$$

The symmetric cipher can be further sub-divided by stream cipher and block cipher based on the plaintext processing- *stream cipher* is one that encrypts plaintext of one bit or one byte at a time, and *block cipher* is one that treats each block of plaintext as a whole and generates cipher text of the same length as plaintext. Fig. 3 and Fig. 4 show the diagram of a stream cipher and a block cipher respectively.

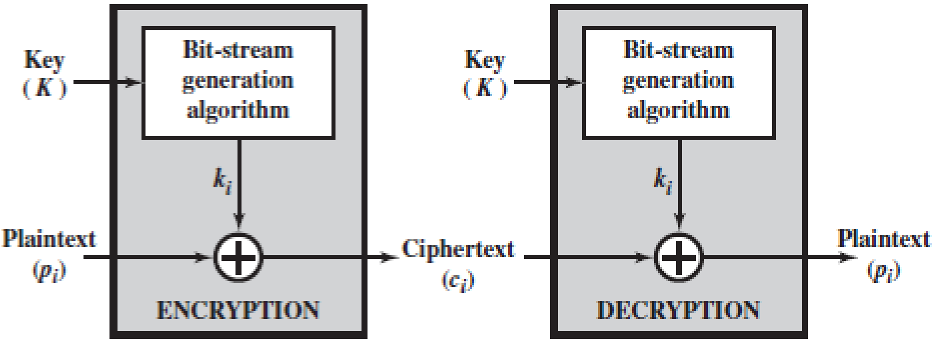


Fig. 3. Stream cipher

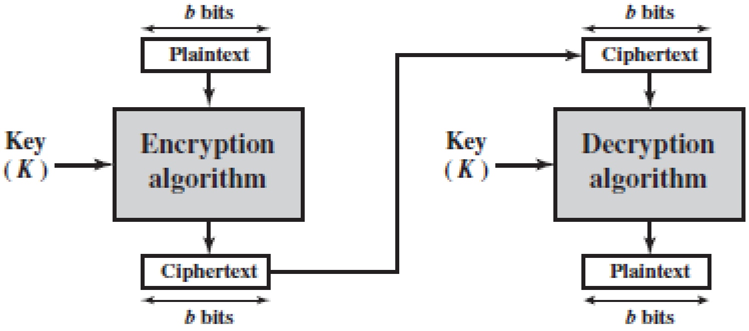


Fig. 4. Block cipher

On the other hand, public-key or asymmetric cryptography uses two separate but related keys for encryption and decryption. The public-key cryptography consists of: plaintext, an encryption and decryption algorithm, cipher text, and public and private keys. These private and public keys differentiate symmetric and asymmetric key cryptography. Actually, there is a pair of keys that have been used in such a way that if one key is selected for encryption then the other key will be used for decryption. This scheme works as follows:

1. Both sender and receiver generates a pair of keys for encryption and decryption.
2. Both sender and receiver places their public key in the public-key repository, which can be easily accessible to others while the private key will be kept secret.
3. Now, if the sender wants to send some data to the receiver, the sender will encrypt this data with the receiver's public key.
4. After reception, the receiver will decrypt this data using its private key.

A schematic diagram of public-key cryptography is shown in Fig. 5.

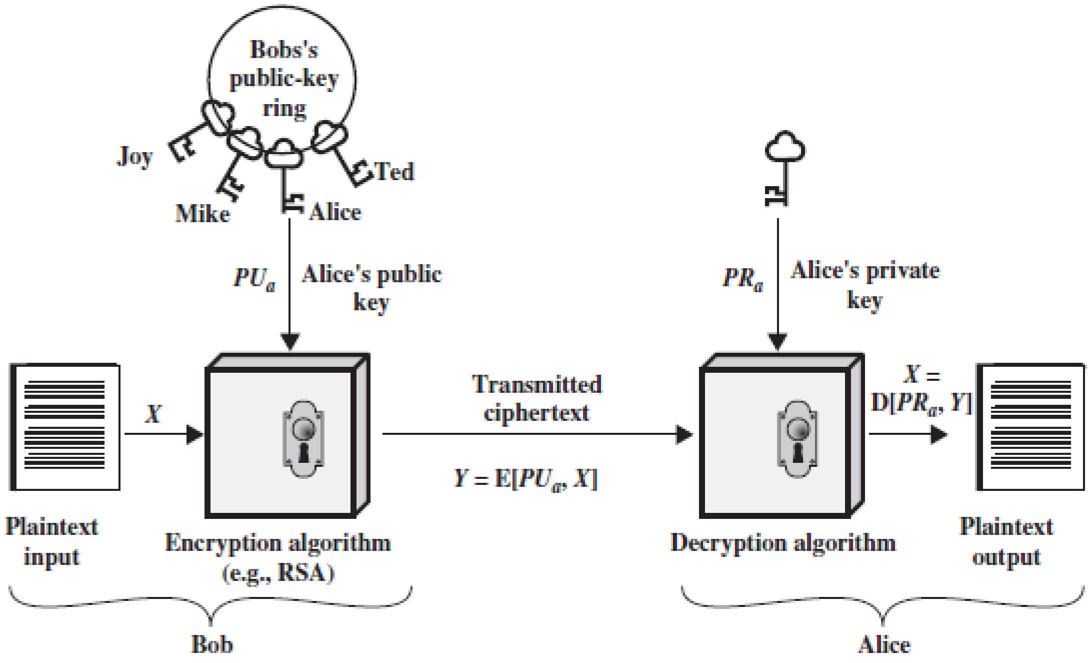


Fig. 5. Schematic diagram of public-key cryptography [5]

For example, sender (Alice) wants to send a message, X, to receiver (Bob). Bob has a related pair of keys: public key, PU_b, and private key, PR_b. PU_b is publicly available and, hence, accessible by Alice also, but PR_b is available only to Bob. So, the form of cipher text, Y, generated by Alice will be

$$Y = E(PU_b , X), \tag{1.3}$$

The legitimate receiver (Bob) then use the private key, $PR_{b,}$ to get back the original plaintext as follows:

$$X = D (PU_b, X). \tag{1.4}$$

1.3 Quantum Cryptography

Quantum cryptography exploits the law of quantum mechanics to provide secure communication between legitimate users. The first quantum cryptographic protocol was proposed by Charles Bennett and Gilles Brassard (BB-84) [6]. The main ingredients to provide security by quantum cryptography are the following: single photon with a particular polarization to represent bit-value; the Heisenberg uncertainty principle, which is the impossibility of knowing the state of a single photon along two different polarization axes [7]; and the no-cloning theorem, the impossibility of cloning a single unknown quantum state [8].

One of the most well-known and advanced applications of quantum cryptography is the quantum key distribution (QKD), which provides information-theoretically-secured exchange of keys between legitimate users. A detailed analysis of QKD will be discussed in next section. In a single photon-based QKD approach, it is not possible to clone data encoded in an unknown quantum state and any attempt to measure unknown quantum state will result in a changes in quantum state which can be detected. This is the advantage of quantum cryptography over mathematical cryptography.

1.3.1 Quantum Bits

There is a significant difference between classical and quantum bits. A classical bit can take values only between 0 and 1, whereas quantum bits can take any value from arbitrary superposition of 0 and 1. In its simplest form, a physical quantum bit or qubit can be considered as a two-state system. In Dirac notation, the mapping from a classical bit to a quantum bit can be written as follows [9]:

$$0 \rightarrow |0\rangle, \qquad 1 \rightarrow |1\rangle. \tag{1.5}$$

According to linearity of quantum theory, the arbitrary superposition of the above two states can be written as,

$$\alpha|0\rangle + \beta|1\rangle, \tag{1.6}$$

where the coefficients α and β are called probability amplitudes and satisfies,

$$|\alpha|^2 + |\beta|^2 = 1. \tag{1.7}$$

The vector representation of the states $|0\rangle$ and $|1\rangle$:

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \tag{1.8}$$

$$|1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{1.9}$$

The super-position state of quantum bit in Equation 1.6 can be written as a two-dimensional vector:

$$|\psi\rangle \equiv \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \tag{1.10}$$

1.3.2 Heisenberg's Uncertainty Principle

Heisenberg's uncertainty principle is one of the main ingredients for quantum key distribution protocol. According to the interference feature of quantum theory, a single particle, for example an electron, can exhibit wave-like characteristics, which constitutes wave-particle duality. Each particle has two complementary variables – position and momentum. This uncertainty principle states that it is not possible to know both its momentum and position simultaneously. Once we measure the position of a particle, we will lose all information about its momentum. In quantum key distribution protocol, for example in BB84, this uncertainty principle and statistical analysis is used to detect the presence of an eavesdropper in a quantum communication channel [10].

1.3.3 No-Cloning Theorem

The no-cloning theorem is another main ingredient of quantum cryptography. Wootters and Zurek proved this theorem [2]. According to this theorem, it is not possible to build a device that can clone an arbitrary unknown quantum state. This principle demonstrates the significant difference between classical and quantum information processing because classical information can be copied easily. Due to this principle of quantum communication, it is not possible for any eavesdropper to build any universal copier to clone an unknown quantum state [11]. For example, if there is a two-qubit unitary operator, which will act as a quantum copier, U and an arbitrary quantum state, $|\psi\rangle$ and an ancillary qubit, $|0\rangle$, according to no-cloning theorem, the following relationship never holds:

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle, \tag{1.11}$$

1.3.4 The Photon Polarization

As quantum cryptography utilizes laws of quantum mechanics, photon polarization is one of the basic concepts in the field of quantum mechanics. In classical physics, light is characterized by an electromagnetic wave with an oscillating electric field perpendicular to the direction of propagation of the wave, and polarization of light is described by the plane of oscillation of electric field. There are various classification of polarization as is shown in Fig. 6. For instance, a linearly polarized light is described by a definite plane of oscillation (Fig. 6(a) and Fig. 6(b) show vertically and horizontally polarized light). Because of the superposition principle, the sum of a horizontal and vertical wave of equal amplitude results in a polarized wave at +45 degree, if they are in phase or -45 degree if their phase difference is 180 degrees (Fig. 6(c) and Fig. 6(d)). Similarly, circularly polarized light is obtained when two orthogonal linearly polarized lights of equal amplitude are superimposed with a phase difference of 90 degree or -90 degree (Fig. 6(e) and Fig. 6(f) show right and left circularly polarized light).

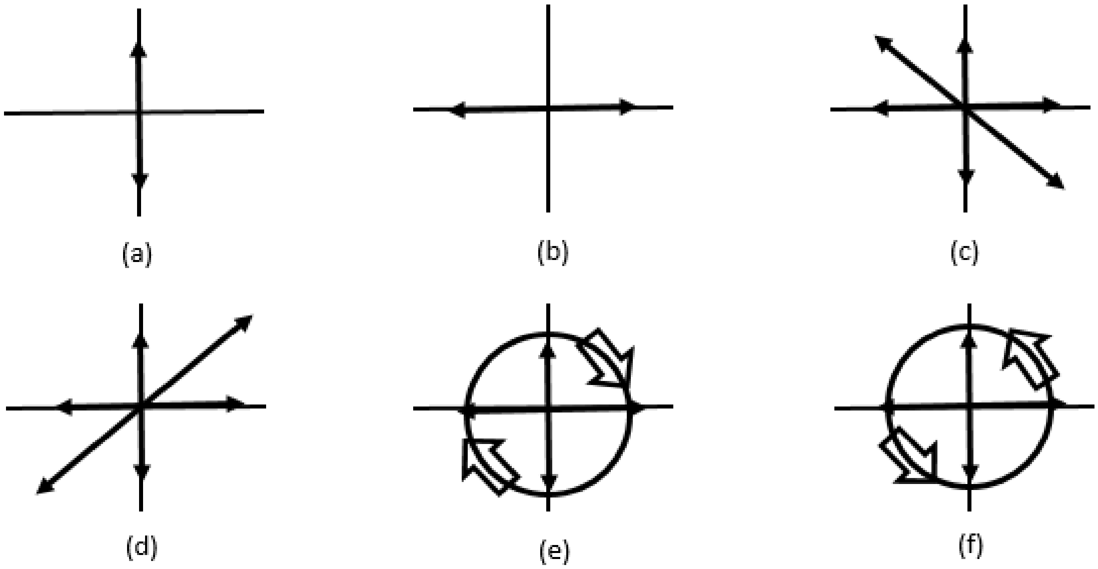


Fig. 6. Classification of Polarization

A polarized light can be generated from unpolarized light through transmission, reflection, diffraction and scattering [12]. There are different types of optical devices are available used to generate polarized light, for example, a polarizer which have anisotropic absorbing properties, a beam splitter which splits a light beam into a transmitted and reflected beam. According to Malus's law – the intensity of the transmitted light, I_T, by an optical device is:

$$I_T = I_0 \cos^2 \theta, \qquad (1.12)$$

where, I_0 = incident light and θ = angle between polarization of the incident light and the polarization axis of the optical device.

In quantum mechanics, this light beam is described by a quantum of energy called photon. A polarized light beam is described as a state of photons in which all photons have the same polarization, and an unpolarized light beam is one in which the polarization of each photon is randomly distributed. In quantum terms, intensity of light is described by the number of photons. Now, for example, consider a polarizer with a polarization axis, a, and a beam of N_0 photons polarized along the axis, b. Then according to Malus's law, a portion of photons ($N_T = N_0 \cos^2 \theta_{ab}$) is transmitted and others are absorbed. As each photon is an indivisible quanta, the probability that a photon is transmitted is $\cos^2 \theta_{ab}$. Here, it is worth mentioning that the transmitted photon is no longer polarized in b-direction; it is polarized along a-direction, which means its initial polarization is changed. This property of photon polarization is used in quantum cryptography to detect eavesdropping in the public quantum channel.

1.4 Quantum Key Distribution

The most prominent application of quantum cryptography is the quantum key distribution (QKD). A QKD approach exploits the law of quantum mechanics to provide secure communication of information between legitimate users. The underlying principle of quantum mechanics helps the legitimate users to detect the presence of eavesdropper. Using this QKD approach, both legitimate parties are able to the share same random secret key, which will be used for symmetric encryption and decryption of the message. In Fig. 6, classification of quantum methods for information security is shown [13]:

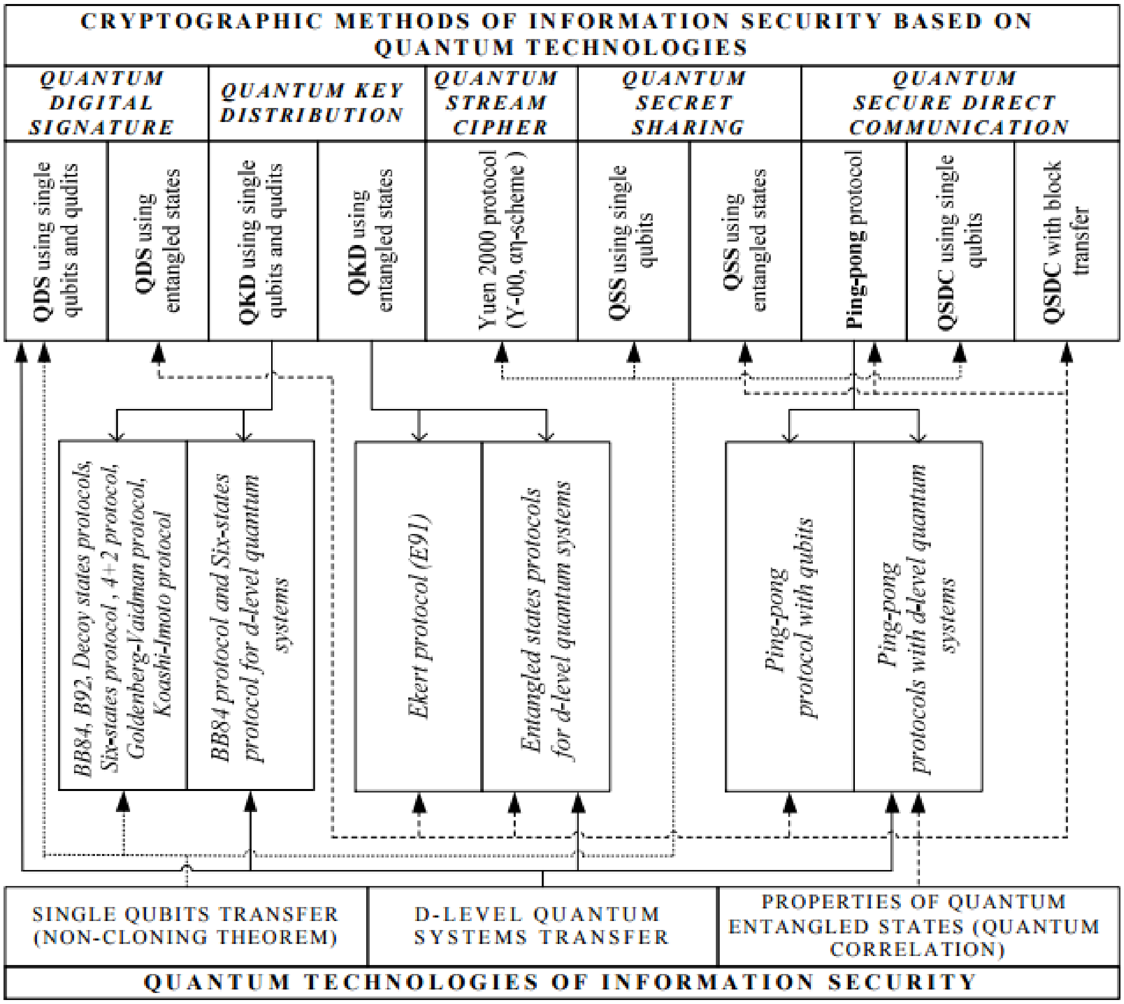

CRYPTOGRAPHIC METHODS OF INFORMATION SECURITY BASED ON QUANTUM TECHNOLOGIES
QUANTUM DIGITAL SIGNATURE
QUANTUM KEY DISTRIBUTION
QUANTUM STREAM CIPHER
QUANTUM SECRET SHARING
QUANTUM SECURE DIRECT COMMUNICATION
QDS using single qubits and qudits
QDS using entangled states
QKD using single qubits and qudits
QKD using entangled states
Yuen 2000 protocol (Y-00, αη-scheme)
QSS using single qubits
QSS using entangled states
Ping-pong protocol
QSDC using single qubits
QSDC with block transfer
BB84, B92, Decoy states protocols, Six-states protocol , 4+2 protocol, Goldenberg-Vaidman protocol, Koashi-Imoto protocol
BB84 protocol and Six-states protocol for d-level quantum systems
Ekert protocol (E91)
Entangled states protocols for d-level quantum systems
Ping-pong protocol with qubits
Ping-pong protocols with d-level quantum systems
SINGLE QUBITS TRANSFER (NON-CLONING THEOREM)
D-LEVEL QUANTUM SYSTEMS TRANSFER
PROPERTIES OF QUANTUM ENTANGLED STATES (QUANTUM CORRELATION)
QUANTUM TECHNOLOGIES OF INFORMATION SECURITY

Fig. 7. Classification of quantum methods for information security [13]

1.4.1 Single Photon Approach

The basic building block of quantum key distribution protocol is based on single photon approach which was proposed by Bennett and Brassard in 1984 and hence this protocol is named as BB84 protocol [6]. The typical scenario of this QKD protocol is as follows: two legitimate parties – Bob and Alice, have access on two channels -private quantum channel and public classical channel. The private quantum channel is used to exchange a sequence of single quanta, whereas the public classical channel is used for exchanging information. It is worth mentioning that the public classical channel needs to be authenticated to avoid man-in-the-middle attack by the eavesdropper. A schematic diagram of BB84 protocol is given in Fig. 8.

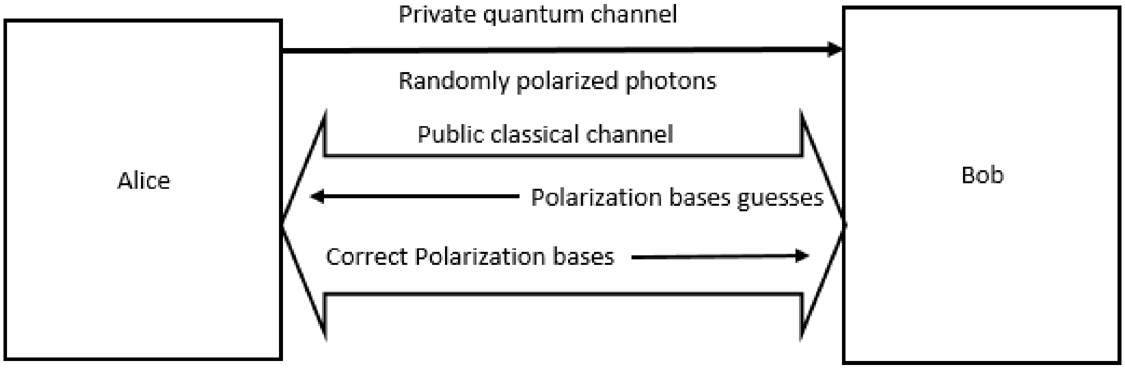

Private quantum channel
Randomly polarized photons
Public classical channel
Alice
Bob
Polarization bases guesses
Correct Polarization bases

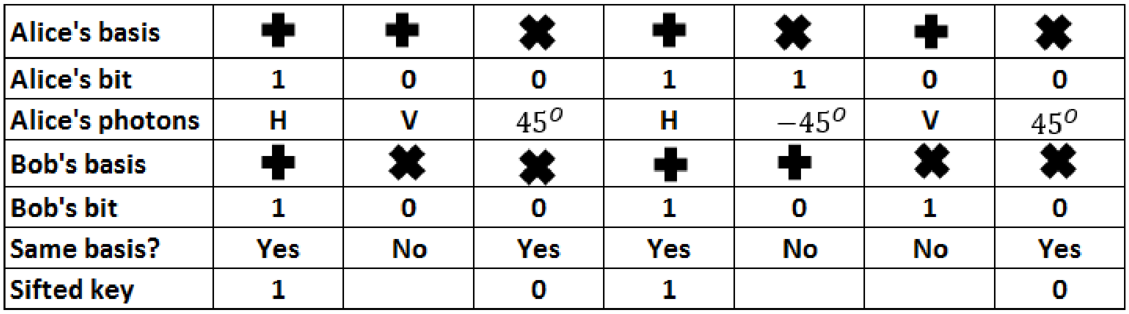
Fig. 8. A schematic diagram of BB-84 protocol

In a typical scenario of BB84 protocol, legitimate users, Alice and Bob, establish a secret random binary string, which will be used later as a secret cryptographic key. For example, Alice wants to send a sequence of secret strings by encoding her bits in a sequence of polarized photons. The coding scheme could be as follows:

$0 \rightarrow |V\rangle$	$1 \rightarrow |H\rangle$
$0 \rightarrow |45^o\rangle$	$0 \rightarrow |-45^o\rangle$

Table 2. A typical coding scheme in BB84 protocol

Alice uses two polarization bases randomly – rectilinear basis (+) for (|H⟩, |V⟩) and diagonal basis (X) for ($|45^o\rangle$, $|-45^o\rangle$), to encode her bits in a random manner. These polarized photons are then sent through a private quantum channel to Bob. After receiving, Bob will measure these photons. As Bob does not know which basis was chosen by Alice, half of the time Bob's basis choice will be the same as Alice's basis choice. After Bob's measurement, both Bob and Alice share two random bit strings in which there is a 50% probability that bits will be the same in both bit strings. To discard mismatched bits, Alice then uses public classical channel to announce her basis choice and later on, Bob will announce the instances, where his measurement bases are the same as Alice's measurement bases. Finally, in the absence of Eve, Alice and Bob share a secret random bit string, known as a sifted key. A typical scenario in BB84 protocol is given in Fig. 9.



Alice's basis	✚	✚	✖	✚	✖	✚	✖
Alice's bit	1	0	0	1	1	0	0
Alice's photons	H	V	45^{O}	H	-45^{O}	V	45^{O}
Bob's basis	✚	✖	✖	✚	✚	✖	✖
Bob's bit	1	0	0	1	0	1	0
Same basis?	Yes	No	Yes	Yes	No	No	Yes
Sifted key	1		0	1			0

Fig. 9. A typical scenario in BB84 protocol

1.4.2 Multi-Photon Approach

The pioneering quantum cryptographic approach, BB84 protocol lacks behind in the practical implementation aspect, as it utilizes single photon. Due to weak signal strength, this approach is difficult to be realized in long distance optical fiber communication. In order to overcome the problem associated with single photon communication, multiphoton fault-tolerant approaches are proposed. In Table 1, different types of multi-photon quantum communication protocol are given. In chapter-3, a detailed analysis of KCQ (Keyed Communication in Quantum Noise) approach is given. This KCQ approach is also known as Y-00 (Yuen-2000) protocols. The Y-00 protocol [14] belongs to the family of multiphoton quantum communication protocol. It provides physical layer security on data by ensuring quantum uncertainty. Y-00 protocol enhances the security of classical stream cipher by introducing quantum noise effect of uncertainty during the measurement process by any eavesdropper [15].

1.5 Problem Statement

In order to ensure physical-layer security during data communication between legitimate users, Y-00 protocol plays an important role as it is a multi-photon approach and can be easily integrated into the existing optical fiber technology. As Y-00 uses non-orthogonal mesoscopic coherent states, a definite relationship is required between coherent states and a mean photon number to restrict the probability of success of coherent-state detection of eavesdropper. In this research work, a new multi-photon coherent-state measurement technique, ML-POVM, is introduced to provide better success probability of coherent-state detection than other measurement techniques such as unambiguous measurement, random guessing, greedy scheme, etc.

Y-00 utilizes Pseudo-Random Number Generator (PRNG) to generate a long-running key from the initial shared secret key between legitimate users for coherent basis selection. Due to unavoidable quantum noise, any eavesdropper, who does not know the secret key, experiences measurement error on the output of PRNG, even in the case of a known-plaintext attack scenario. As security of this protocol relies on the secrecy of the secret key, an impact analysis of the erroneous output (in the form of bit-flip error) of PRNG is introduced to predict the running seed key of the PRNG by brute force attack.

1.6 Contribution of the Thesis

The contributions of the thesis are given below:

1 Maximum-likelihood-POVM (ML-POVM) technique for multiphoton coherent-state detection is introduced in Y-00 protocol, which provides better success probability of detection for a given number of non-orthogonal coherent states and mean photon number than do other measurement techniques such as greedy scheme, unambiguous measurement, random guessing etc.

2 A lower bound between non-orthogonal coherent states and mean photon number for a given measurement error probability using ML-POVM is given, whereas in previous Y-00 papers, an indefinite bound was proposed.

3 An impact analysis for erroneous output (in the form of bit flip error) of PRNG (Linear Feedback Shift Register (LFSR) is considered as a PRNG) due to quantum noise being carried out to quantify the required minimum number of bit-flip errors to hide running seed key from eavesdropper's exhaustive search under a known-plaintext attack scenario.

1.7 Organization of the Thesis

The thesis is organized as follows:

In Chapter 1, an introduction of cryptography is given. It begins with the procedure and need for a cryptographic approach for data communication between legitimate users. Then classification of a cryptographic approach is introduced, namely - mathematical and quantum cryptography. After the discussion on generic classification of mathematical cryptography, the working principles of quantum cryptography -

quantum bits, no-cloning theorem, and Heisenberg's uncertainty principles, are introduced. After that, an introduction of the application of quantum cryptography quantum key distribution (QKD), is given. Next, both single-photon and multi-photon-based cryptographic approaches are discussed. Finally, the problem statement and contributions of this research are given.

Chapter 2 focuses on the basic concepts of information-theoretic security analysis. The definitions of entropy, conditional entropy, and mutual information are discussed to evaluate the secrecy of any cryptosystem. Several important information-theoretic quantities are introduced, and, finally, the conditions for perfectly secured cryptosystem are given to analyze, compare, and evaluate the performance of any practically realizable cryptosystem against an ideal one.

Chapter 3 begins with the discussion on keyed communication in quantum noise (KCQ) approach. Then, basic working principle of Y-00 protocol and two pioneer implementation schemes of Y-00 protocol – phase modulation and intensity or amplitude modulation are given. After that, a measurement error analysis of the legitimate users and the attacker is given. Finally, a detailed analysis of the overall security provided my Y-00 protocol is given.

Chapter 4 begins with the poincarè sphere representation of the photon polarization. Next, a detailed overview of positive operator valued measure (POVM) is given. Then, the polarization-based maximum-likelihood-POVM technique in Y-00 scheme is addressed. After that, a comparative analysis begins by considering the success probability of coherent-state detection as a figure of merit between different measurement techniques such as ML-PVOM, unambiguous measurement, random guessing, and greedy scheme. Finally, a lower bound is proposed between the number of non-orthogonal coherent state and the mean photon number in Y-00 scheme using ML-POVM.

Chapter 5 focuses on the impact analysis of erroneous output sequences of the LFSR on predicting the operating seed key by exhaustive search under known-plaintext attack scenario. It begins a discussion of two important attacks – cipher text only attack and known plaintext attack. Considering practical implementation perspective, Y-00 utilizes Linear Feedback Shift Register (LFSR) as a PRNG. The basic working principle of the LFSR is discussed next. Then, the bit-flip error analysis for 4-bit, 8-bit and 16-bit LFSR is given to measure the required number of bit-flip errors to hide the running seed key from the eavesdropper by exhaustive search under known-plaintext attack scenario. After that, the same bit-flip error analysis for Non-Linear Feedback Shift Register (NLFSR) is given. Finally, success probability of running seed key detection in LFSR under a known-plaintext attack scenario is calculated for a given number of non-orthogonal coherent states and a mean photon number.

Chapter 6 provides a conclusion of this thesis work along with future research direction.

Chapter 2: Information-theoretic Security Analysis

The fundamental analysis of cryptographic systems was accomplished by Shannon. He published a paper named as “Communication Theory of Secrecy Systems” [16] in which he used information theory [17] to characterize cryptosystem by introducing entropy, conditional entropy, and mutual information. In his paper, he proved the existence of a perfect secrecy system—a system that provides unconditional security even though an attacker with unlimited computational power, intercepts the system. This type of secrecy is hard to achieve practically in the classical world. For example, now a days, the secrecy of most cryptographic systems depend on the computational hardness of breaking the algorithm. The main drawbacks of this perfect secrecy system to be practically realizable are 1) the length of the key should be equal to the length of the plaintext and 2) the key should be used randomly and only once, which is a one-time pad. But, in order to carry out a comparative analysis between real and perfect cryptosystems, the concept of perfect secrecy is required.

This chapter begins with the definition of entropy, conditional entropy and other related information-theoretic quantities that are required to define the secrecy of the cryptosystem. Next, a mathematical analysis for calculating entropy of deterministic algorithm is given, which provides proof that a deterministic algorithm never provides additional entropy, rather than initial entropy of the secret random variable. Then, an analysis of conditional entropy and mutual information is given to measure average information loss on the communication channel. Finally, a detailed discussion of perfectly secured systems is given to compare the performance of a practical cryptosystem with an ideal one.

2.1 Entropy

According Shannon's definition, entropy in information theory [17], measures the average uncertainty of a statistical random variable. The information content of a random variable (x):

$$I(x) = -\log_2(p(x)). \tag{2.1}$$

Hence, expected information content of the source:

$$\sum_{x \in X} P(x)I(x) = -\sum_{x \in X} p_x(x) \log_2(p(x)) = H(X). \tag{2.2}$$

In (2.2), H(X) denotes the entropy of the information source.

This entropy, H(X), is the minimum rate at which a random variable, X, can be compressed and recovered without loss of generality.

2.1.1 Entropy of a Deterministic Algorithm

Any deterministic algorithm used, for example, in Pseudo Random Number Generator (PRNG), does not increase entropy, as input space is limited by the PRNG, and there is no additional boost to increase entropy of the PRNG. Suppose, random variable X is n-bit long and each realization (there are m realizations) of random variable is equally probable with a probability of $p_i = \frac{1}{2^n} = 2^{-n}$, the entropy of this random variable becomes:

$$\begin{aligned} H(X) &= -\sum_{i=1}^{m} p_i \log_2(p_i), \\ &= -\sum_{i=1}^{2^n} 2^{-n} \log_2 2^{-n} = n. \end{aligned} \tag{2.3}$$

Now, a PRNG, which used a fixed, deterministic algorithm takes a fixed length input and produces random output that is longer as compared to the input. Here, we consider the input to the PRNG as a random variable, X, which is n-bit long and output, which is also a random variable, Y, which is 2^n bit long, other than that there is no additional bias to the PRNG. If input has $m = 2^n$ realizations, output of that PRNG also had $2^m = 2^{2^n}$ realizations, as there is no additional bias to the input of the PRNG, we can write, the probability of the rest of the realization $(2^{2^n} - 2^n)$ is equal to zero. Hence,

$$\begin{aligned} H(Y) &= -\sum_{i=1}^{m} p_i \log_2(p_i), \\ &= -\sum_{i=1}^{2^n} 2^{-n} \log_2(2^{-n}) - \sum_{i=1}^{2^{2^n}-2^n} 0 \log_2(0) = n, \end{aligned} \tag{2.4}$$

So, the upper bound regarding entropy of the output of a PRNG is as follows:

$$H(X) \geq H(Y). \tag{2.5}$$

where, H(X) and H(Y) are the entropies of the input and output random variables of the PRNG. The criteria for this (2.5) further demonstrates that for the entropy of a random variable X, which can take values ranging from 1 to n, the overall entropy is bounded by:

$$H(X) \leq \log_2 n. \tag{2.6}$$

2.2 Conditional Entropy

Now, consider another random variable, which can take values like 1, 2, 3, m. In such a situation, the conditional entropy H (X|Y) is defined as:

$$H(X|Y) = \sum_{j=1}^{m} p(Y = j) H(X \mid Y = j). \tag{2.7}$$

Equation (2.7) shows that conditional entropy measures the average uncertainty about any random variable X, given observations of random variable Y.

2.2.1 Fano's Inequality

Fano's inequality in the field of information theory relates conditional entropy of a random variable X, given a correlated variable Y, to the probability of incorrectly estimating the random variable X given Y [18]. In general, this inequality is used to find a lower bound to show how the probability of incorrectly predicting the value of X given Y is bounded by the uncertainty H (X|Y) of X given Y [19].

$$H_2(P_e) + P_e \log(|X| - 1) \geq H(X|Y). \tag{2.8}$$

where,

$$H_2(P_e) = binary\ entropy\ of\ probability\ of\ error$$

$$= P_e \log\left(\frac{1}{p_e}\right) + (1 - p_e)\log(\frac{1}{1 - p_e})$$

|X| = set of allowed realization of the input random variable

P_e = Probability of error of incorrectly estimating of random variable $\widehat{X} \neq X$

2.3 Mutual Information

The mutual information between two random variables X and Y is defined as

$$I(X;Y) = \sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)}. \tag{2.9}$$

The mutual information between two random variables can be written as

$$I(X;Y) = H(X) - H(X|Y). \tag{2.10}$$

Now, if these two random variables are completely independent of each other, there is no uncertainty in X given Y, i.e., H (X|Y) = 0. From (2.10) we get,

$$I(X;Y) = H(X). \tag{2.11}$$

Table 2 provides some important information theoretic quantities. Here, plaintext = X, cryptographic key = K, observation of legitimate receiver (Bob) = Y_B, observation of eavesdropper (Eve) = Y_E, length of plaintext = |X|

$\boldsymbol{H(X) = \sum_{x\epsilon X} P_x log\left(\frac{1}{P_x}\right)}$	Shannon Entropy, average unpredictability of random variable
$\boldsymbol{H_{min}(Y) = \min_{y\epsilon Y}\{-logP_y\}}$	Min Entropy, indicates most probable outcome from observation and most favorable condition to Eve
$\boldsymbol{H_{max}(Y) = log\|Y\|}$	Max Entropy, highest achievable uncertainty from observation of the output
$\mathbf{H(K\|Y_E)}$	Secrecy of secret key under cipher-text only attack
$\mathbf{H(X\|Y_E)}$	Secrecy of message under cipher-text only attack
$\mathbf{H\ (X\|Y_B, K)>0}$	Error rate of legitimate users, ideally $H\ (X\|Y_B, K) = 0$
$\mathbf{H(X\|Y_E) \leq H(K)}$	Shannon limit in cryptography - perfect secrecy of secret key.
$\mathbf{H\ (Y\|X, K) = 0}$	Non-random cipher
$\mathbf{H\ (Y\|X, K) \neq 0}$	Random cipher
$\mathbf{I\ (X, Y) = 0}$	Mutual information indicates, statistical independence of plaintext and cipher-text, in real scenario, $I\ (X, Y) \leq \mathcal{E}$
$\mathbf{H\ (X, X) = H(X)}$	Entropy of random variable does not change with repetition
$\mathbf{H(X\|Y) = H\ (X, Y) - H(Y)}$	Conditional entropy of random variable X, conditioned on another random variable Y
$\mathbf{H\ (X, Y) \leq H(X) + H(Y)}$	Joint entropy between two random variables
$\mathbf{H\ (X, Y) \geq H(X)}$	Additional information increases entropy
$\mathbf{H(X\|Y) \leq H(X)}$	Conditioning reduces entropy

$D(P_X \| P_U) \geq 0$	Relative entropy between two probability measures

Table 3. Important information-theoretic quantities

2.4 Perfect Secrecy System

A cryptosystem with message X, cipher-text Y, and secret key K is called perfectly secure [17], if and only if,

$$P(X|Y) = P(X). \tag{2.12}$$

which, in turn, is based on the fact that

1. One-time pad, Length of the message, |X| = Length of Cipher-text, |Y| = Length of key, |K |.
2. Each key should be equally probable, $\frac{1}{|K|}$, and should be used only once.

According to (2.12), the posteriori probability of a perfectly secured cryptosystem is equal to the priori probability. For a secrecy system, the uncertainty on key, K, given cipher text, Y, or the conditional entropy H(K|Y) can be written as [42],

$$H(K|Y) = H(X) + H(K) - H(Y). \tag{2.13}$$

In the case of a known-plaintext attack (this topic is discussed further in chapter 5), H(X) = H(Y) = 0, so (2.13) further reduces to,

$$H(K|Y) = \ H(K). \tag{2.14}$$

The implication of (2.14) is that, for a perfectly secured system, even having the knowledge of cipher text, does not reduce the uncertainty of the key. Though cryptosystem like one-time pad provides perfect secrecy, this type of approach is hard to be practically realizable.

2.5 Summary

This chapter has introduced various important information-theoretic quantities required to analyze and evaluate any cryptosystem. The uncertainty about plaintext, cipher text, and key plays an important role in deciding whether a particular cryptosystem provides the desired security level. The conditional entropy relates to the average information loss from a cryptosystem, whereas mutual information is used to identify the channel capacity of a typical communication system between legitimate users. In Table 2, some important information theoretic quantities were given. In section 2.4 a characterization of a perfectly secured system was given based on the concept of information theory. This type of characterization helps to evaluate other practically realizable cryptosystems against the ideal one. The main disadvantage of a one-time pad-based cryptosystem is that the amount of information required to represent a key is the same as amount of plaintext to be transmitted over a secure channel. It is worth mentioning that, information theory is one of the powerful tools used to evaluate and analyze any cryptosystem.

Chapter 3: Keyed Communication in Quantum Noise (KCQ)

Yuen-2000 (Y-00) is a multiphoton-based quantum cryptographic protocol that exploits the advantages of keyed communication in quantum noise (KCQ) [15]. Y-00 enhances the security of classical information transmittal between legitimate users by using quantum detection, estimation, and communication theory. In the BB-84 protocol, advantage creation is achieved by using intrusion-level detection, considering the fact that it is not possible for the eavesdropper (Eve) to clone or replicate an unknown quantum state. But in real-life scenarios, Eve can duplicate a copy similar to the user's observation due to measurement device imperfections of the legitimate users.

In Y-00, using a pre-shared secret key, the observation of Bob $\mathrm{Y_B}$, who knows the key, will never be the same as the observation of Eve Y_E who does not know the key, i.e., $Y_B \neq Y_E$. Hence security and advantage creation are ensured considering optimal quantum receiver performance of the legitimate users. Quantum stream cipher - based technique like Y-00 can be readily implemented with existing optical fiber communications technology. Unlike the single photon state used in BB-84 protocol, coherent states used by the Y-00 protocol [20] can be easily generated and measured and are also fault-tolerant.

In this chapter, the basic working principle of Y-00 protocol is given. Then different types of implementation schemes of Y-00 protocol are discussed. Next, a detailed analysis of optimum quantum receiver performance is presented. After that, the effective key generation rate by Y-00 protocol is shown, and, finally, a security analysis of Y-00 protocol is given.

3.1 Basic Working Principle: Y-00 Protocol

In 2000, a new quantum cryptographic approach, named the Y-00 protocol was proposed by Yuen. It belongs to the class of quantum stream cipher randomized by quantum noise from the measurement of coherent states. Fig. 10 depicts a generic description of the Y-00 protocol.

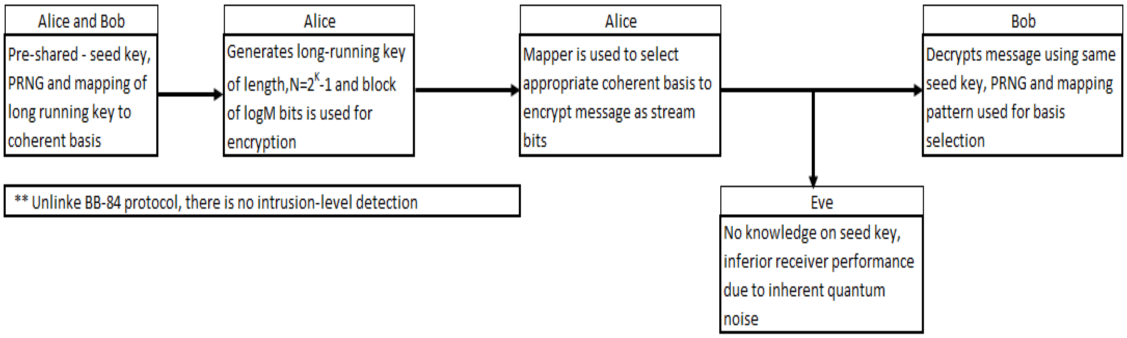

Alice and Bob
Pre-shared - seed key, PRNG and mapping of long running key to coherent basis
Alice
Generates long-running key of length,N=2^{K}-1 and block of logM bits is used for encryption
Alice
Mapper is used to select appropriate coherent basis to encrypt message as stream bits
Bob
Decrypts message using same seed key, PRNG and mapping pattern used for basis selection
** Unlinke BB-84 protocol, there is no intrusion-level detection
Eve
No knowledge on seed key, inferior receiver performance due to inherent quantum noise

Fig. 10. Working principle of Y-00 protocol

Y-00 protocol supersedes the performance of classical cryptography by exploiting the quantum effects in optical fiber communication [21]. Moreover, only symmetric key encryption supported by quantum key distribution cannot improve the security. In classical cryptography, which provides only complexity-based security, the observations of Eve and Bob are always the same, i.e., $Y_B = Y_E$.

According to information theory, the following inequality of Shannon limit for perfect secrecy holds:

$$H(X|Y_E) \leq H(K). \tag{3.1}$$

Equation 3.1 indicates the condition of the one-time pad, which should be random, used only once and should be as long as the plaintext. It is not possible for classical or conventional cipher to exceed the Shannon limit. However, in Y-00, utilizing the pre-shared key, it is possible to exceed the Shannon limit, thereby exploiting the effect of quantum noise, where the necessary condition is

$$Y_B \neq Y_E, \tag{3.2}$$

and one of the sufficient conditions is [22]:

$$H\ (X|Y_E, K_s) > H(X|Y_B, K_s) \cong 0. \tag{3.3}$$

Hence, the Y-00 protocol enhances information-theoretic security of classical random cipher, using the randomized quantum noise effect of uncertainty.

3.2 Implementation Scheme

So far, two methods from other available methods have been exercised to implement Y-00 protocol. The first method is phase modulation scheme [23], which uses mesoscopic coherent states of significant energy and the other method is amplitude modulation scheme [24-28], which uses maximum (α_{max}) and minimum (α_{min}) amplitude of the laser power. In the phase modulation scheme, there are M pairs of coherent states with amplitude:

$$\alpha_l = \alpha_0(\cos\theta_\mathrm{l} + i\sin\theta_l), \mathrm{where}\theta_l = \frac{2\pi l}{2M}; l = 1,2,3 \ldots M. \tag{3.4}$$

More precisely, M pairs of two coherent states can be written as: $|\alpha e^{i\theta_l}\rangle$ and $|\alpha e^{i(\theta_l+\pi)}\rangle$. A pre-shared seed key is used to run any kind of PRNG (Pseudorandom Number Generator) to generate a long-running key, K_R, which has a length of $N = 2^{|K_S|} - 1$. The $log_2 M$ bits of the long running key are used for the selections of a key-to-phase mapping sequence to modulate each bit of the message by following the principle of stream cipher. Thus the instances of long-running keys that are used for the mapping of coherent basis selection, follow the relation:

$$|K_R| < \frac{N}{\log_2 M}. \tag{3.5}$$

The other method is the amplitude modulation scheme, where the maximum (α_{max}) and minimum (α_{min}) amplitudes are fixed and the signal configuration is set to $\frac{|\alpha_{max} - \alpha_{min}|}{2M}$.. For eavesdropper, to get the proper knowledge of the signal set is just discrimination of 2M coherent signal-set in the absence of quantum noise.

Generally, a mapping pattern is utilized to map the running keys K_R to the parameters that the protocol deals with, such as the amplitude, intensity, or phase. A typical example of a mapping pattern is as follows:

$$\begin{pmatrix} K_R \\ \alpha \\ X \end{pmatrix} = \begin{pmatrix} 1\ \ 2\ \ 3 \dots \dots\ \ M \\ \alpha_1 \alpha_2 \alpha_3 \dots \dots \alpha_M \\ 0\ \ 1\ \ 0 \dots \dots\ \ 1 \end{pmatrix}. \tag{3.6}$$

where, K_R represents the running key obtained from the output of PRNG, α represents corresponding basis of encoding/decoding such as $|\alpha e^{i\theta_l}\rangle\ and\ |\alpha e^{i(\theta_l+\pi)}\rangle$ and X represents the corresponding message bit sequences. Fig. 11 depicts the schematic diagram of the working principle of Y-00 protocol.

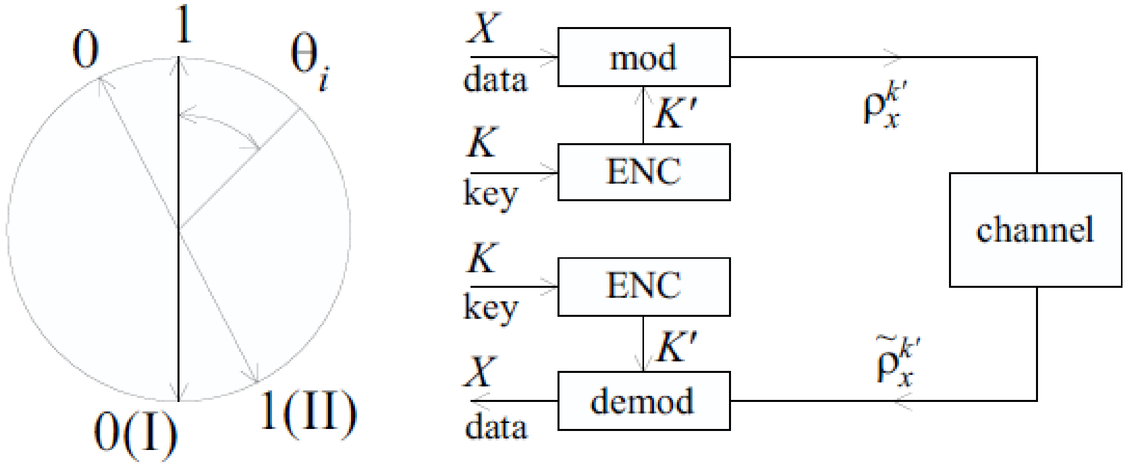


Fig. 11. Working methodology: Y-00 protocol

For example, according to the mapping above, the running key-2 is used to select the basis number-2 to modulate the message bit-2. The sequences of quantum states after the code modulator can be expressed as:

$$|\psi\rangle = |\alpha_i\rangle_1 |\alpha_j\rangle |\alpha_k\rangle_3 \ldots \text{where } i, j, k \in N = (1 - 2M). \tag{3.7}$$

where $|\alpha_i\rangle$ is one of the 2M coherent states. The single mode coherent state can be expressed in terms of the superposition of the photon number states |n⟩ [29]

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{(n!)^{\frac{1}{2}}} |n\rangle, \tag{3.8}$$

where $|\alpha|^2$ is the mean photon number of the coherent state. Hence, the probability of getting n photon is:

$$|\langle\alpha|n\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}, \tag{3.9}$$

which is the Poisson distribution. Coherent states are not orthogonal: for any arbitrary two coherent states:

$$|\langle\alpha_1|\alpha_0\rangle|^2 = e^{-|\alpha_1 - \alpha_0|^2}. \tag{3.10}$$

In order to provide an advantage over the adversary, the legitimate users need to choose the neighboring basis state with the selection strategy:

$$|\langle\alpha_i|\alpha_{i+1}\rangle|^2 \sim 1. \tag{3.11}$$

Now, if Eve utilizes heterodyne measurement on her intercepted sequences, Eve's probability of error becomes [30]:

$$P_e(i+1|i) = \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \int_0^{t_0} \exp\left(-\frac{t^2}{2}\right) dt = 0.2 \sim 0.5. \tag{3.12}$$

where, for phase modulation scheme, $t_0 = \frac{\pi|\alpha|}{2M}$ and for amplitude or intensity scheme, , $t_0 = \frac{|\alpha_{max} - \alpha_{min}|}{4M}$. Equation (3.12) represents probability of error between two neighboring states and provides the degree of quantum nose effect due to the number of coherent states, M, and quadrature amplitude, α.

3.2.1 ISK-Y-00- An Intensity-based Modulation Implementation Scheme

In Fig. 12, multi-level intensity-based modulation scheme for Y-00 protocol is shown which has been implemented in [31]. In transmitting side, a long running-key sequence is used for actual message sequence encryption generated by PRNG. The seed key of PRNG has been shared between transmitter and receiver prior to the communication. The appropriate value for coherent basis selection is controlled by the value of the long-running key. After that, based on basis value, value of intensity level of the signal is determined. Finally, input data is modulated by the code modulator to a multi-level intensity-based signal. Then, after converting it into a coherent quantum signal, the sender's message is transmitted to the optical line as a Y-00-encrypted signal.

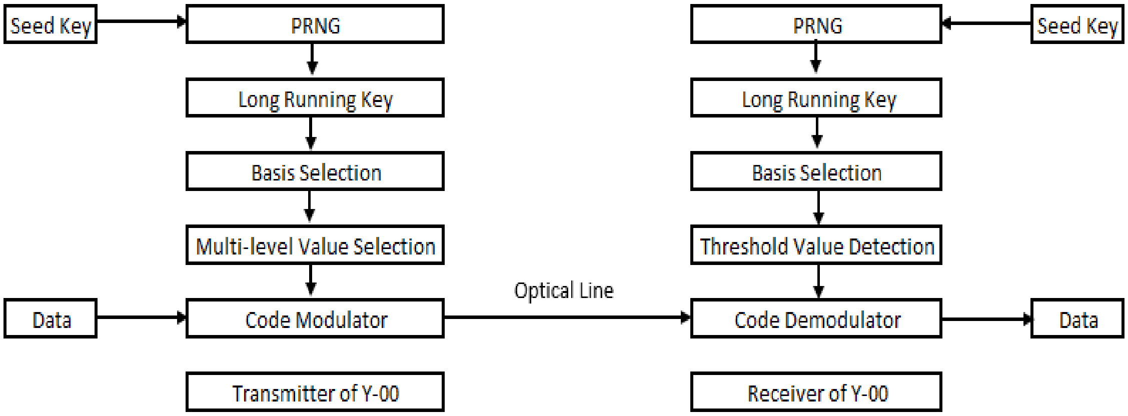


Fig. 12. A practical implementation scheme of Y-00 protocol

In the receiving side, a coherent quantum signal is converted into an electrical signal. Because the same seed key is used in both the transmitting and the receiving side, information about a coherent basis selection would be the same and properly synchronized with the transmitter. A threshold value detection is used to appropriately recover the received signal. And finally, the code demodulator is used to subsequently retrieve the original message bit sequence based on the information of the threshold value detection.

3.3 An Optical Quantum Receiver Performance

The legitimate receiver (Bob) uses a binary optimum quantum receiver together with the pre-shared secret key. At the beginning of the protocol, both sender and receiver should know the necessary system's working parameters [32, 33] in order to prepare and measure the coherent quantum state. Ideally, the output of the measurement for the legitimate users is:

$$H(X|Y_B, K_s) = 0. \tag{3.13}$$

A binary communication system transmits information during every T seconds by one of the two coherent states: $|\alpha_0\rangle$ and $|\alpha_1\rangle$ that occurs with relative probabilities P_0 and P_1, respectively. The minimum average probability of errors experiencing by any binary receiver to identify the appropriate coherent state between the two coherent signals is given by the Helstrom bound [34]:

$$P_e = \frac{1}{2}\Big[1 - [1 - 4P_0P_1 \exp(-|\alpha_1 - \alpha_0|^2)]^{\frac{1}{2}}\Big], \tag{3.14}$$

where $|\alpha_1 - \alpha_0|^2 = S$ is the square of the amplitude difference of the two coherent signals.

An adversary who does not know the key, must use a universal heterodyne receiver; and according to quantum detection and estimation theory, there is a benefit in the measurement process which implies

$$P_e(heterodynereceiver) \geq P_e(binaryreceiver). \tag{3.15}$$

For M measurement basis states and for equally probable signal, the minimum average symbol error rate attainable by optimum quantum receiver is

$$P_e = \frac{M-1}{M^2}\left[\sqrt{1+(M-1)e^{-K_s}} - \sqrt{1-e^{-K_s}}\right]^2. \tag{3.16}$$

where K_s is the length of the seed key. Fig. 13 shows an optimum quantum receiver performance for different coherent signal sets using (3.16).

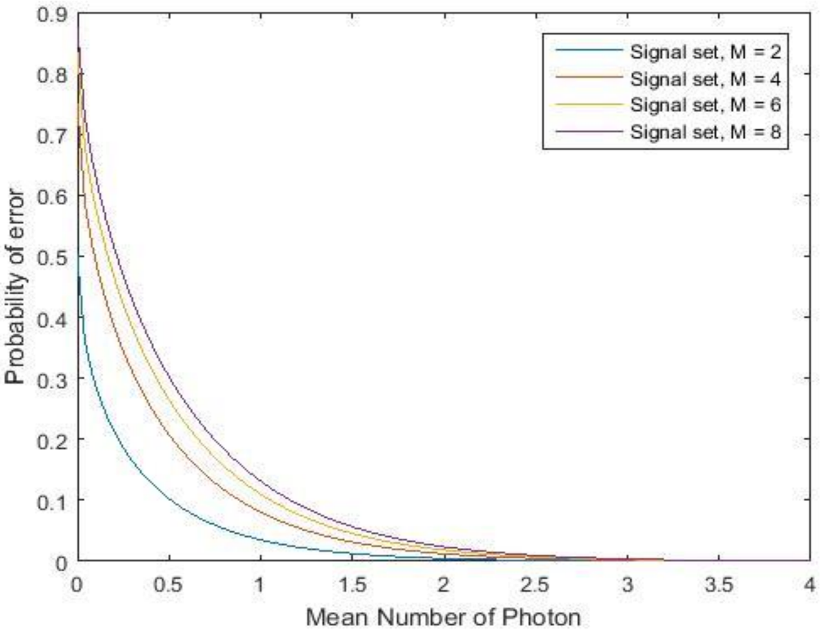


Fig. 13. Quantum optimum receiver performance for basis state number M

Overall, for heterodyne measurement and optimum quantum receiver performance, the probability of error for Eve and for legitimate users can be written as,

$$P_{e,Eve} \sim \frac{1}{2} e^{-S} \; and \; P_{e,Bob} \sim \frac{1}{4} e^{-4S}. \tag{3.17}$$

3.4 Effective Key Generation Rate

The condition for net key generation rate in Y-00 protocol can be written as,

$$|K|_{final} < \Delta I \equiv I(X, Y_B) - I(X, Y_E),. \tag{3.18}$$

where I(X,Y) is the mutual information between the two random variables X and Y. A detailed analysis of mutual information is given in chapter 2. The effective key generation for the Y-00 protocol is [14]:

$$K_{eff} = |K|_{final} - I_E - |K_v| - |K_m|,. \tag{3.19}$$

where I_E is the side information of Eve on the final key which needs to be controlled to ensure secrecy on the generated key K_{eff}, K_v is the verification key, and $|K_m|$ is the modulation key.

3.5 Security Analysis: Y-00

According to [35], "*A QKD protocol is defined as secure if, for any security parameters s >0 and l > 0 chosen by Alice and Bob, and for any eavesdropping strategy, either the scheme aborts, or it succeeds with probability at least* $O(1 - 2^{-s})$, *and guarantees that Eve's mutual information with the final key is less than* 2^{-l}. *The key string must also be essentially random.*"

Though security is an abstract concept, we can identify that a given communication system is secure, but it is not possible to measure the level of security with perfection. Several security criteria have been defined so far [36 - 40]:

Correctness: The observation of output for Alice and Bob should be identical, i.e., $Y_A = Y_B$.

Forward and Backward Secrecy: Forward secrecy means an attacker should not be able to predict the past output of the protocol based on the side information of the protocol. Backward secrecy indicates that it is not possible for the adversary to predict the future output of the protocol even if some observation of the output is compromised.

Resilience: The protocol should be resilient in the sense that even if the initial input (entropy source) of the protocol is compromised or influenced by the attackers, it is not possible for the attacker to predict the future output of the protocol.

Robustness: If a protocol exhibits the afore-stated characteristics such as correctness, forward and backward secrecy, and, resilience, then it remains *robust* under adverse conditions. In a robust condition, observation of Alice and Bob would be the same assuming no-loss in measurement device.

In a real-world scenario, there are imperfections in measurement devices, and for that reason ideal and real devices exhibit different characteristics under the same working conditions. Typically, a relaxation criterion is deployed so that real protocol does not show correctness, robustness, and secrecy like an ideal protocol. According to [36], "*A QKD protocol $\mathcal{P}^{real}$ is ϵ-secure if it is ϵ-indistinguishable from a (hypothetical) protocol $\mathcal{P}^{ideal}$ which is perfectly secure, i.e. $\mathcal{P}^{ideal}$ satisfies the correctness, the secrecy and the robustness criteria.*"

The security of the seed key for Y-00 protocol is defined as [22]:

$$Q = M^{\frac{|K_S|}{\log_2 M}} = 2^{|K_S|}.. \tag{3.20}$$

where $|K_S|$ is the length of secret key, M is the number of coherent basis used for modulating the message bit. The secrecy of Y-00 protocol is entirely depends on the seed key of the PRNG. It is assumed that the entropy of the input to the PRNG is:

$$H(K_s) = |K_s|.. \tag{3.21}$$

According to the basic principle of Y-00, even if Eve uses most powerful receiver, she will eventually suffer error while measuring her intercepted data. The masking effect due to quantum noise can be written as [41]:

$$\Gamma_{PSK} \sim \frac{\sqrt{2}M}{\pi|\alpha|},$$

$$\Gamma_{ISK} = \frac{2\sigma}{\Delta\alpha} \sim \frac{4\sqrt{\alpha}M}{\alpha_{max} - \alpha_{min}}. \tag{3.22}$$

Now, considering this masking effect, (3.20) can be written as,

$$Q = \Gamma^{\frac{|K_S|}{\log_2 M}}.. \tag{3.23}$$

When number of coherent states, M $\gg$ quadrature amplitude, $|\alpha|$, then Γ = M and equation (3.23) converges to (3.20).

Generally, the computational complexity/security of a typical PRNG can be written as:

$$Q = 2^{\eta|K_S|}.. \tag{3.24}$$

where η is a constant and is equal to 1 when there is no quantum noise. But due to masking effect of quantum noise this constant $\eta > 1$ and hence increase the burden of the attacker to get the correct operational secret key. That’s why Y-00 protocol is called quantum noise randomized stream cipher which provides additional layer of complexity in the underlying PRNG.

3.6 Summary

This chapter has introduced the basic working principle of the multi-photon quantum noise randomized stream cipher - Y-00 protocol. Of other implementation schemes, two prominent implementation schemes - phase modulation and intensity or amplitude modulation are discussed. Next, the masking effect due to quantum noise in

Y-00 protocol is discussed. The legitimate users have certain advantages over attackers due to the knowledge of the secret key. To achieve this advantage, the number of coherent states should be much higher than the mean photon number. Then, the probability of error of coherent state detection is calculated for both Alice and Bob, who knows the secret key, and for Eve, who does not know the secret key. After that, an effective key generation rate by Y-00 protocol is given using the concept of mutual information. Finally, a practical security analysis of Y-00 protocol is given to show how quantum uncertainty plays an important role in increasing the overall complexity of PRNG.

Chapter 4: Success Probability of Coherent State Detection Analysis in Y- 00 using Maximum Likelihood-POVM

This chapter introduces a new measurement technique based on maximum likelihood estimation for correct detection of a coherent state in a Y-00 scheme. In general, there are many measurement techniques that are applicable in Y-00 scheme. Out of which phase modulation is used for measuring the performance of Y-00 protocol theoretically and intensity modulation is used for practical implementation purpose. This chapter introduced a new measurement technique using polarization on the surface of 2D-Poincarè sphere. This maximum likelihood-POVM that belongs to the family of ambiguous measurement gives better success probability of coherent state detection than other measurement techniques such as unambiguous measurement, random guessing, greedy scheme, etc. for a given number of non-orthogonal coherent states and mean photon number. Moreover, a lower bound is proposed using the ML-POVM measurement technique between mean number of photons and number of non-orthogonal coherent states for a given success probability, whereas in earlier papers on Y-00 protocol, an indefinite bound was proposed.

This chapter begins with the Poincarè representation of photon polarization. Then POVM measurement technique for polarization-based coherent state detection is discussed. Next, the theory and concept behind the maximum-likelihood POVM measurement technique for photon polarization detection is discussed. After that, a comparative analysis on success probability of coherent state detection using ML-POVM, greedy scheme, random guessing, and unambiguous measurement is presented.

Finally, a lower bound between mean photon number and the number of non-orthogonal coherent states using ML-POVM is calculated.

4.1 Poincarè Sphere Representation of Photon Polarization

As discussed in chapter 1, polarization is one of the properties of light that describes the orientation of oscillation of electromagnetic waves. In quantum mechanics, this light is described as a massless quanta or number of photons instead of electromagnetic wave. The Poincarè sphere is an excellent tool to represent all different types of polarization – horizontal, vertical, elliptical, diagonal, anti-diagonal, etc. on 3D-speherical co-ordinates. A typical representation of Poincarè sphere for polarization of light [43 - 44] is given in Fig. 14.

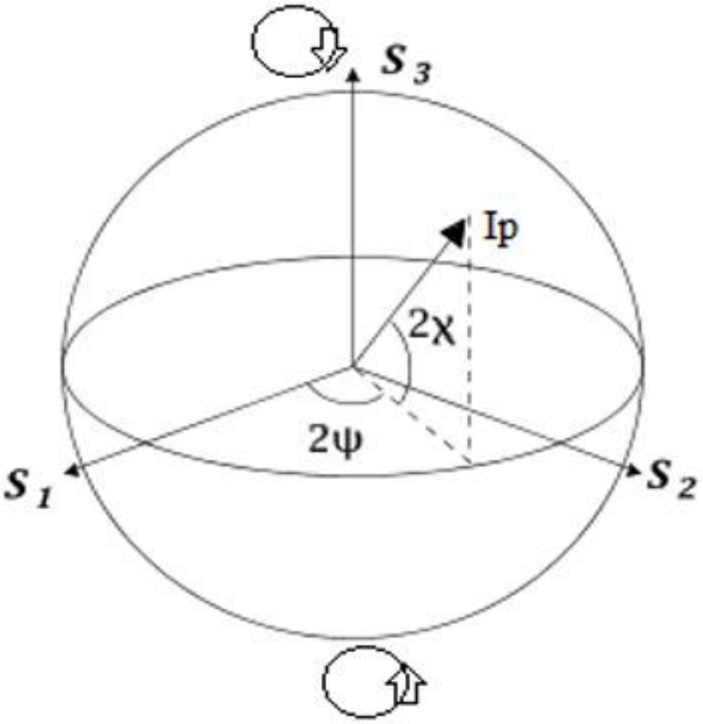


Fig. 14. Poincarè sphere representation of polarization

A Poincarè sphere is represented in the form of spherical co-ordinates $(I, p, 2\psi, 2\chi)$ with each point on the sphere representing a pure state of polarization, whereas the north-pole and south-pole represent right-circular (R) and left-circular (L), polarization respectively. Points along the equator on the sphere represents linear polarization-horizontal (H), vertical (V), diagonal (D), anti-diagonal (A). Points in the southern hemisphere represent left-handed and points in the northern hemisphere represent right-handed ellipses. The parameters 2ψ and 2χ represent polar and azimuth angles, respectively. The parameter, I, represents the identity of the photon, or the electromagnetic wave, whereas p denotes the degree of polarization. Values of p vary between 0 and 1. If p = 1, then polarization is represented on the surface of the sphere with radius I if p = 0, then there is no polarization, and if 0 < p < 1, polarization is represented as being inside the sphere. So, any polarization on the Poincarѐ sphere can be uniquely identified by these four parameters $I, p, 2\psi\ and\ 2\chi$

4.2 Positive Operator Valued Measure (POVM)

In quantum information and measurement theory [9, 45-46], a Positive-Operator Valued Measure (POVM) is a measure that gives non-negative operators $\{M_j\}_j$ on infinite-dimensional Hilbert space, and integrals of all operators give the identity operator, $\sum_j M_j = I$. Generally, a density operator is used to describe a quantum state. In case of finite-dimensional state-space, the general form of density operator is:

$$\rho = \sum_j p_j \, |\psi\rangle \langle\psi|.. \tag{4.1}$$

According to the definition of POVM, which works on a quantum state can be describes by density operator ρ and the trace becomes:

$$Tr(M_j \rho) \geq 0.. \tag{4.2}$$

Moreover, a set of measurement operators, $\{M_j\}_j$ satisfies a completeness condition:

$$\sum_j M_j^\dagger M_j = I.. \tag{4.3}$$

In case of pure state, $\rho = |\psi\rangle\langle\psi|$ the probability becomes,

$$p_j(j) = \langle\psi|M_j^\dagger M_j|\,\psi\rangle = ||M_j|\psi\rangle||^2 \quad .. \tag{4.4}$$

and for ensemble of states,

$$p_j(j) = Tr\{M_j^\dagger M_j\rho\} = Tr\{M_j^\dagger \rho M_j\} \ .. \tag{4.5}$$

The post-measurement state can be written as:

$$\rho_j = \frac{M_j\rho M_j^\dagger}{Tr\{M_j^\dagger M_j\rho\}}.. \tag{4.6}$$

In general, POVM measurement on a particular quantum system is performed, when there is no need to care about the post-measurement state. The only important thing to care about, is the probability of obtaining a particular outcome, for instance, the transmission of classical data over a quantum channel where the intended receiver does not care about the post-measurement state.

4.3 Maximum-Likelihood Positive Operator Valued Measure (ML-POVM)

The idea behind maximum-likelihood positive operator-valued measure in a multiphoton regime was proposed in paper [47]. In this paper, both success probability and mean fidelity are considered when evaluating the performance of this measurement technique with respect to other measurement technique such as the greedy scheme. Before discussing on measuring criteria of maximum-likelihood POVM, it is helpful to understand a few basic concepts of quantum measurement and information theory.

4.3.1 Trace Distance

According to the definition of trace distance, the trace distance between two operators A and B is given by,

$$\left|\left|A\ -B\right|\right|_1 = Tr\{\sqrt{(A-B)^{\dagger}(A-B)}\}.. \qquad (4.7)$$

In quantum mechanics, trace distance is a measure of indistinguishability between two quantum states. For two density operators ρ and σ, the bound for trace distance is represented as

$$0 \le \left|\left|\rho - \sigma\right|\right|_1 \le 2.. \qquad (4.8)$$

From (4.8), it is clear that two quantum states are equal if and only if the trace distance between the two states is zero. According to quantum hypothesis testing, trace distance leads to the probability of error of distinguishing two quantum states ρ and σ:

$$p_e = \tfrac{1}{2}\ [1 - \tfrac{1}{2}\ \| \rho - \sigma\|_1].. \qquad (4.9)$$

4.3.2 Fidelity

In quantum information theory, fidelity is a measure of closeness of two quantum states. The fidelity of two density matrices ρ and σ is

$$F(\rho,\sigma) = Tr\left\{\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right\}^2\ .. \qquad (4.10)$$

The fidelity for two pure states $|\psi\rangle$ and $|\phi\rangle$ is defined as:

$$F(|\psi\rangle,|\phi\rangle) =\ |\langle\psi|\phi\rangle|^2\ .. \qquad (4.11)$$

and fidelity satisfies the following bound:

$$0 \le F(|\psi\rangle,|\phi\rangle) \le\ 1\ .. \qquad (4.12)$$

The relationship between trace distance and fidelity for two quantum states ρ and σ is given by

$$1 - \sqrt{F(\rho,\sigma)} \le \frac{1}{2}\ \|\rho - \sigma\|_1 \le \sqrt{1 - F(\rho,\sigma)}\ . \qquad (4.13)$$

4.3.3 Maximum-Likelihood Estimation

In statistical analysis, maximum-likelihood estimation (MLE) is a method of estimating a statistical model’s parameter, given observed data that maximizes the likelihood of generating the observed data.

The likelihood function is calculated using the joint density function for an independent and identically distributed sample:

$$f(x_1, x_2, \dots, x_n|\ \theta) = f(x_1|\theta) \times f(x_2|\theta) \dots \times f(x_n|\theta). \tag{4.14}$$

In case of likelihood estimation, the observed values $x_1, x_2, \dots, x_n$ have to be fixed parameters, and θ will be the function’s variable which can vary:

$$L(\theta; x_1, x_2, \dots., x_n) = f(x_1, x_2, \dots, x_n|\theta) = \prod_{i=1}^{n} f(x_i|\theta). \tag{4.15}$$

The maximum likelihood method estimates θ_0 by finding the value of θ that maximizes above function:

$$\theta_{0(MLE)} = argmax_{\theta \in \Theta} f(x_1, x_2, \dots, x_n|\theta). \tag{4.16}$$

4.3.4 Maximum-Likelihood POVM in Multiphoton Regime

There are various implementation schemes for Y-00 protocol such as PSK-Y-00 (phase modulation), ISK-Y-00 (intensity/amplitude modulation) etc. In this analysis, we are considering phase randomized polarization based implementation for calculating success probability and mean fidelity in a case of given mean number of photon and number of non-orthogonal coherent states. As discussed in section 4.1, a Bloch sphere is used to represent polarization of qubit, which can be determined uniquely by θ and ϕ. In Fock or number basis, a polarized single photon is defined by creation operator

$$a_r^+ = \cos\frac{\theta}{2} a_H^+ + e^{i\phi} \sin\frac{\theta}{2} a_V^+, \tag{4.17}$$

The Fock state with n photon statistics can be created as

$$|n\rangle_r = \frac{a_r^{+n}}{\sqrt{n!}}|0\rangle. \tag{4.18}$$

In general, a coherent state can be represented as a superposition of Fock state with definite photon statistics. Instead, in this analysis, photon statistics are specified by the photon number distribution, P_n, and quantum state, which can be represented as,

$$\rho(\boldsymbol{r}) = \sum_{n=0}^{\infty} P_n |n\rangle_{\boldsymbol{r}}\langle n|. \tag{4.19}$$

where **r** is uniquely identified by θ and ϕ. Now, according to the maximum-likelihood estimation, for a given polarization **r**, the maximum likelihood estimation of initial unknown polarization, $\boldsymbol{r_o}$, is

$$\boldsymbol{r}_{0(MLE)} = argmax_{\boldsymbol{r}\in S}\, P(\boldsymbol{r}|\boldsymbol{r_0}) = \boldsymbol{r}. \tag{4.20}$$

where $P(\boldsymbol{r}|\boldsymbol{r_0})$ is the maximum likelihood estimation function using ML-POVM,

$$P(\boldsymbol{r}|\boldsymbol{r_0}) = Tr[\Pi(\boldsymbol{r})\rho(\boldsymbol{r}_0)]. \tag{4.21}$$

Here, $\rho(\boldsymbol{r}_0)$ is calculated using (4.19), and $\Pi(\boldsymbol{r})$ is calculated using quantum estimation and detection theory [34]. The maximum-likelihood POVM $\Pi(\boldsymbol{r})$ satisfies the following conditions:

$$[\Upsilon - W(\boldsymbol{r})]\Pi(\boldsymbol{r}) = \Pi(\boldsymbol{r})[\Upsilon - W(\boldsymbol{r})] = 0, \tag{4.22}$$

and

$$\Upsilon - W(\boldsymbol{r}) \geq 0. \tag{4.23}$$

where $W(\boldsymbol{r})$ is the Hermitian risk operator, and Υ is a Hermitian Lagrange operator. After calculating the integration over the Bloch surface, S, the ML-POVM, $\Pi(\boldsymbol{r})$, which satisfies (4.22) and (4.23):

$$\Pi(\boldsymbol{r}) = \sum_{n=0}^{\infty} \frac{n+1}{4\pi}\, |n\rangle_{\boldsymbol{r}}\langle n|. \tag{4.24}$$

Now, putting the value of (4.19) and (4.24) into (4.21), we get

$$P(\boldsymbol{r}|\boldsymbol{r_0}) = \sum_{n=0}^{\infty} \frac{n+1}{4\pi} P_n \left|f_{\boldsymbol{r}\boldsymbol{r_0}}\right|^{2n} . \quad (4.25)$$

where, $\left|f_{\boldsymbol{r}\boldsymbol{r_0}}\right|^2 = \frac{1}{2}\,(1 + \boldsymbol{r}.\boldsymbol{r_0})$ is the mean fidelity between polarizations **r** and $\boldsymbol{r_0}$.

Consider a finite region $S_\epsilon(r_0)$ on the Bloch sphere as a circle around polarization r_0 where 2ϵ is an angular diameter, and the value of ϵ ranges from 0 to π as shown in Fig. 15. The success probability can be calculated as

$$Q(\epsilon) = \int_{S_\epsilon(r_0)} P(\boldsymbol{r}|\boldsymbol{r_0}) d\boldsymbol{r}. \quad (4.26)$$

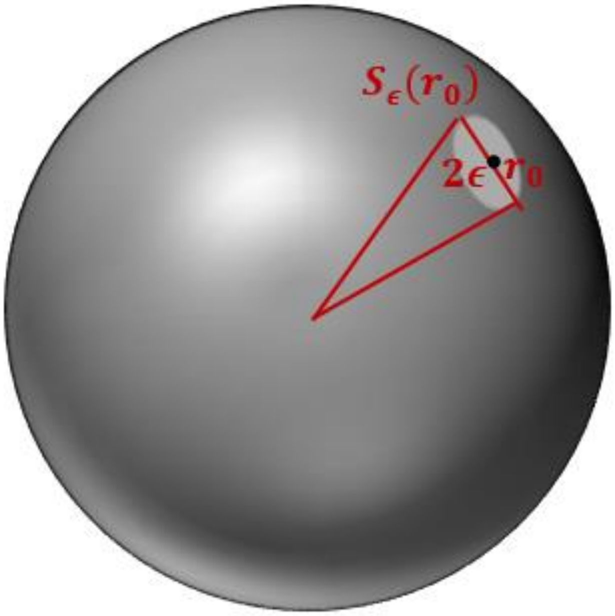


Fig. 15. Finite region of circle around polarization on Bloch sphere

Now from (4.25) and (4.26) we get,

$$Q(\epsilon) = 1 - \sum_{n=0}^{\infty} P_n \left(\frac{1+cos\epsilon}{2}\right)^{n+1}. \quad (4.27)$$

In case of Poisson distribution,

$$P_n = \frac{e^{-|\alpha|^2}(|\alpha|^2)^n}{n!}. \quad (4.28)$$

So, the success probability using Poisson distribution becomes,

$$Q_{poi}(\epsilon) \approx 1 - e^{-\frac{\epsilon^2}{4}(|\alpha|^2+1)} . \tag{4.29}$$

Equation 4.29 represents the success probability of coherent state detection of mean photon number $|\alpha|^2$ considering Poisson distribution and two neighboring qubits are ϵ-angular distance away from each other on the Bloch sphere.

4.4 Success Probability of Coherent State Detection using ML-POVM in Y-00 Protocol

In this section, success probability of non-orthogonal coherent state detection is calculated for a given number of coherent states and mean photon using ML-POVM. Now, if we consider a two-dimensional realization of Bloch sphere for representing M non-orthogonal coherent states, then we can write,

$$\pi\epsilon^2 = \frac{4\pi}{M} , \tag{4.30}$$

So using (4.29), success probability for non-orthogonal coherent state, M and mean photon number, $|\alpha|^2$ becomes,

$$Q_{poi}(\epsilon) \approx 1 - e^{-\frac{|\alpha|^2+1}{M}} . \tag{4.31}$$

Now using (4.31), success probability of correctly identifying non-orthogonal coherent state for a different number of coherent states (M = 1000, 2000, 3000) and mean photon number ($|\alpha|^2$ = 0-10000) has been calculated and shown in Fig. 16. From Fig. 16, it is worth mentioning that using the ML-POVM measurement technique to limit the eavesdropper performance in Y-00 scheme who does not know the secret key, the number of coherent state M needs to be greater than mean photon number $|\alpha|^2$.

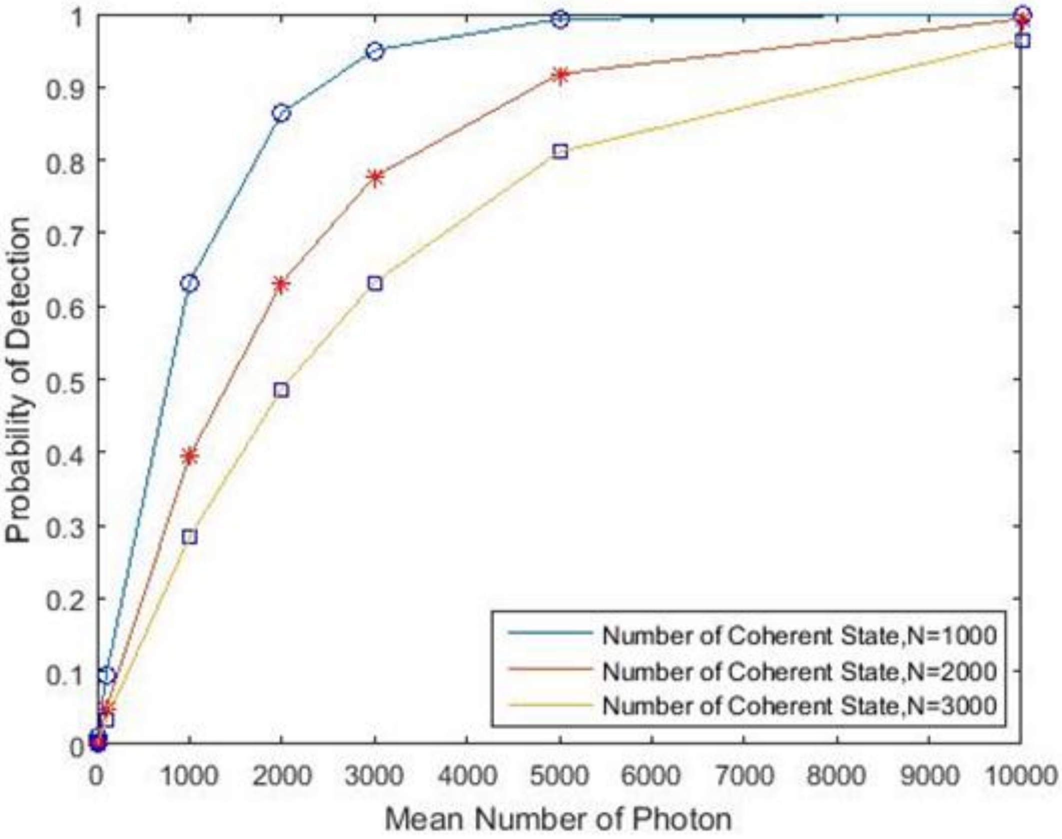


Fig. 16. Probability of detection vs mean photon number using ML-POVM

4.4.1 Comparative Analysis of Success Probability of Coherent State Detection between Ambiguous and Unambiguous Measurement

In principle, there are two ways to discriminate between non-orthogonal coherent states: ambiguous measurement, which gives erroneous result, and unambiguous measurement, which gives inconclusive result. For example, the Helstrom measurement strategy [34] belongs to the class of ambiguous measurement, which is optimum measurement strategy and provides minimum probability of error while discriminating between two non-orthogonal states.

The unambiguous measurement strategy has zero measurement error at the expenses of providing inconclusive result. The success probability using quantum unambiguous measurement (QUM) for M symmetric coherent states is given by Chefles and Barnett [49]:

$$P_D(QUM) = M \min_{k=1,2,3,..,M} |c_k|^2. \tag{4.32}$$

where

$$|c_k|^2 = \frac{1}{M}\sum_{j=1}^{M} e^{-\frac{2\pi ijk}{M}} e^{|\alpha|^2(e^{\frac{2\pi ij}{M}}-1)}$$

If the non-orthogonal coherent states are of equal prior probabilities, the probability of providing inconclusive resultd is provided by Ivanovic-Peres limit [50, 51]

$$P_{IP} = |\langle\psi_0|\psi_1\rangle|. \tag{4.33}$$

According to [49], the optimal inconclusive probability, $P_{e(unambiguous)}$ of unambiguous measurement is always greater than or equal to minimum-error probability of ambiguous measurement $P_{e(ambiguous)}$ and hence

$$P_{e(unambiguous)} \geq P_{e(ambiguous)}. \tag{4.34}$$

This is due to the fact that unambiguous measurement strategy is less likely to succeed because it eliminates any accidental probability of failure as well as it compromises any accidental probability of success. Whereas random guessing, which signifies "no-measurement" at all, belongs to the family of ambiguous measurement. It can provide wrong measurement outcome without notifying that it failed. In case of equal-probable independent events, random guessing, therefore, provides free boost of 1/n probability, which is simply a guess and very likely to be a wrong. Hence, in case of a large number of measurement bases, success probability of random guess (unambiguous measurement) for discriminating non-orthogonal coherent states is much higher than the success probability of unambiguous quantum state discrimination. In Table 4 a comparative analysis of success probability calculation using unambiguous measurement, random guessing, and ML-PVOM is given for various number of coherent states and mean photon number. From Table 4, it is clear that ML-POVM measurement provides better probability of success for non-orthogonal coherent state detection than do the other two measurement techniques for a given number of non-orthogonal coherent states and mean photon number.

Mean photon number	Number of coherent state	Success probability of coherent state detection strategies		
		Unambiguous measurement	Random guessing	Maximum-likelihood POVM
10000	2000	$3\ \times 10^{-12}$	$5\ \times 10^{-4}$	**0.6**
1000	2000	2.1565×10^{-13}	$5\ \times 10^{-4}$	**0.39**
4000	1500	$1.6510\ \times 10^{-13}$	$6.67\ \times 10^{-4}$	**0.31**

Table 4. Success probability of coherent state detection using different measurement strategies

4.4.2 Comparative Analysis of Success Probability of Coherent State Detection between Greedy Scheme and ML-POVM

A greedy scheme [52] is an adaptive local measurement with classical communication to maximize average fidelity at each measurement step. It provides better results in comparison to other measurement techniques such as stokes parameters measurement. It uses classical communication because this measurement scheme takes into consideration - the result of the previous measurement step. The likelihood function for 2D-greedy scheme after n-measurement step:

$$\mathrm{P}(\chi_{\mathrm{n}}|\mathbf{r}_0) = \prod_{k=1}^{n} \frac{1+\boldsymbol{m}_k.\boldsymbol{r}_0}{2} = \prod_{k=1}^{n} \left|\boldsymbol{f}_{\boldsymbol{m}_k \boldsymbol{r}_0}\right|^2. \tag{4.35}$$

Here, $\boldsymbol{m}_k$ is the k^{th} measurement basis where $k \geq 2$, which is calculated by maximizing the average fidelity of the k^{th} measurement step using the result of $(k-1)^{th}$ measurement step and χ_{n} is the measurement outcome at n steps.

The estimate of polarization $\boldsymbol{r_0}$ using measurement result of the greedy scheme becomes,

$$\mathbf{r}_0 = \frac{\boldsymbol{V}(\chi_{\mathrm{n}})}{|\boldsymbol{V}(\chi_{\mathrm{n}})|}. \tag{4.36}$$

where,

$$\boldsymbol{V}(\chi_{\mathrm{n}}) = \int \mathrm{P}(\chi_{\mathrm{n}}|\mathbf{r}_0) p(\boldsymbol{r}_0) \boldsymbol{r}_0 d\boldsymbol{r}_0$$

In Fig. 17 shows the success probability of coherent state detection for given number of coherent states (M = 1000) and mean photon number ($|\alpha|^2 = 45$) using greedy scheme (dotted line) and ML-POVM (solid line) is shown. From Fig. 17, it is clear that ML-POVM measurement strategy gives better results in terms of success probability of coherent detection due to collective measurement of all photons in one step.

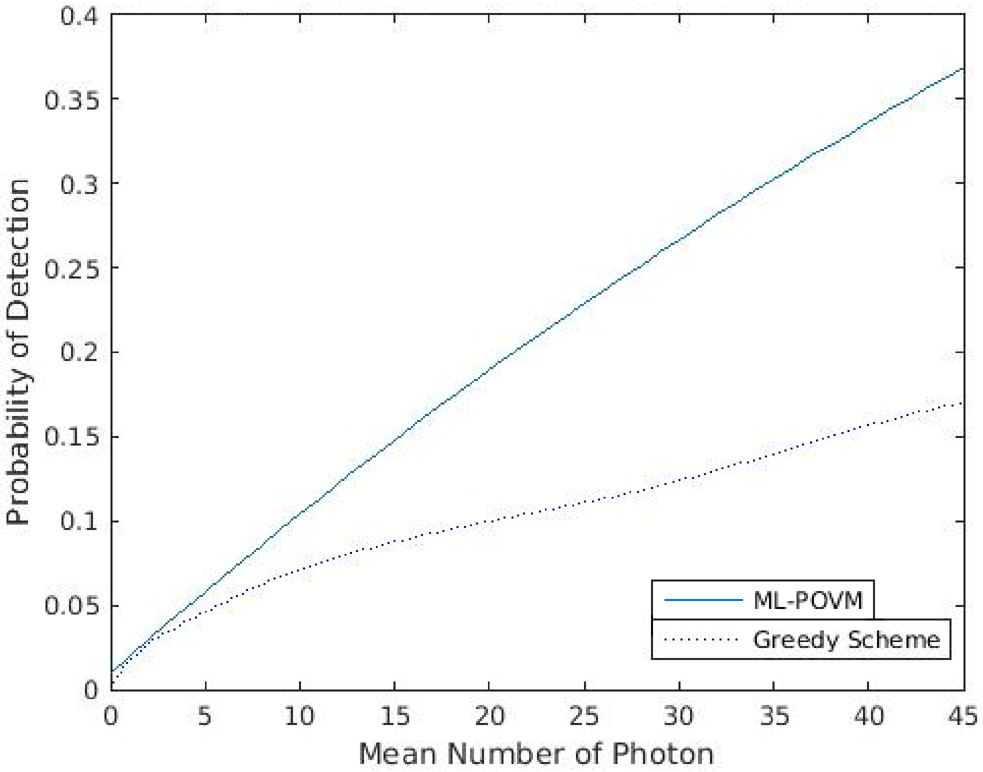


Fig. 17. Probability of detection for given number of coherent states and mean photon number using greedy scheme (dotted line) and ML-POVM (solid line)

4.5 A Lower Bound between Mean Photon Number and Number of Coherent State Using ML-POVM

In [14], an indefinite bound between numbers of non-orthogonal coherent states and mean photon number is given as:

Number of non-orthogonal coherent state (M) $\gg$ *Mean photon number* ($|\alpha|^2$)

But using the ML-POVM measurement technique, a lower bound between the number of non-orthogonal coherent states and mean photon number is calculated for a given probability of measurement error. Using (4.31) we get,

$$M \geq -\frac{|\alpha|^2+1}{\ln(P_e)} .. \tag{4.37}$$

where, probability of error, P_e = 1 – success probability (Q_{poi})

Table 5 shows the lower bound between number of coherent state and mean photon number using (4.37) for a given measurement error probability.

Probability of measurement error	Lower bound between number of coherent state and mean photon number
0.4	$M \geq 1.092|\alpha|^2$
0.5	$M \geq 1.44|\alpha|^2$
0.6	$M \geq 1.96|\alpha|^2$

Table 5. Lower bound between number of coherent states and mean photon number for given probability of error using ML-POVM

4.6 Conditional Entropy Calculation of Running Key of PRNG in Y-00

In Y-00 protocol, an eavesdropper measures the output of the PRNG without having any prior knowledge on seed key. Due to lack of knowledge on seed key, Eve always introduces error while measuring the output of the PRNG. Fano's inequality as described in section 2.2.1 plays an important role to measure the average uncertainty on running key sequence given the Eve's observation (Y_E), which can be written as,

$$H_2(P_e) + P_e \log\left(2^{|K_s|} - 1\right) \; = \; H(K_R|Y_E).. \tag{4.38}$$

In Table 6, conditional entropy of running key sequence given Eve's observation is shown.

Number of non-orthogonal coherent state, M	Mean photon number ($|\alpha|^2$)	Probability of error using ML-POVM	Conditional entropy ($H(K_R|Y_E)$)
1000	50	0.95	95.07
1000	100	0.9	90.15

1000	1000	0.37	38.43
1000	2000	0.14	16.84
2000	2000	0.37	38.43
3000	2000	0.51	51.97
**In this calculation, seed key length is considered as 100 bit, which is independently and identically distributed random variable and period of PRNG is $2^{100} - 1$			

Table 6. Conditional entropy calculation of running key of PRNG using Fano's inequality and ML-POVM

4.7 Summary

In this chapter, a Poincarè representation of photon polarization is introduced. Next, a pioneer photon polarization measurement technique is discussed, namely Positive Operator Valued Measure (POVM). Then, we introduced recently formulated maximum-likelihood POVM (ML-POVM) in multiphoton regime. We have compared the success probability of coherent state detection for a given number of coherent states and mean photon numbers, using different polarization measurement techniques such as greedy scheme, unambiguous measurement, ML-POVM, etc. in the Y-00 scheme. From the comparative analysis of measurement techniques where success probability is considered as a figure of merit, we have proved that ML-POVM shows better success probability of coherent state detection for a given number of coherent states and mean photon numbers. After that a lower bound is proposed between the number of non-orthogonal coherent states and mean photon numbers, using ML-POVM. Finally, using Fano's inequality, conditional entropy of the long-running key (K_R) of PRNG is calculated based on the arbitrary intercepted observation (Y_E) of eavesdropper.

Chapter 5: Impact Analysis of Measurement Error in Pseudo-Random Number Generator (PRNG)

In Y-00 protocol, the use of Pseudo-Random Number Generator (PRNG), is to generate a long-running key sequence from the short secret key. The key-bit sequences from a long-running key are used for appropriate coherent basis selection to modulate plaint-text sequence according to a mapping table. Eve always introduces error in Y-00 protocol while measuring the output of PRNG due to her lack of knowledge of the seed key. This measurement error is due to the quantum uncertainty. The overall security of Y-00 protocol lies in the secrecy of the seed key. Eve's main task is to predict the seed key based on her observation of the long-running key. From an implementation perspective, Linear Feedback Shift Register (LFSR) is generally used as a PRNG in Y-00 protocol. The measurement error in the output of PRNG plays an important role in predicting the seed key.

This chapter begins with a brief introduction on the different types of cryptographic attacks. In particular, the importance of considering known-plaintext attack on multiphoton-based approach is discussed. The next section begins with the working principle of the LFSR, the impact of feedback polynomial, and the number of tapings required to generate maximum length ($2^n - 1$, n = number of bits in the input sequence) output sequence of the LFSR. For analyzing the impact of error in the output sequence of LFSR, we have considered a typical scenario of bit-flip error. We have simulated different implementation of LFSR such as 4-bit, 8-bit, and 16-bit LFSR. Then we have introduced random bit flip-error into the output sequence of the PRNG to analyze the impact of error for predicting the seed key. It has been shown that a significant number of bit-flip error is required to make the seed key unpredictable from the erroneous observation of the output sequence of the PRNG by brute-force attack. Moreover, the configuration or set-up of the LFSR is also important for analyzing the impact of bit-flip error in the output sequence on the prediction of the seed key. Finally, a similar bit-flip error analysis was conducted on non-LFSR to evaluate the correlation between the input and output sequence.

5.1 Attacks on Cryptosystem

An eavesdropper always poses a potential threat to the cryptosystem. Typically, the main objective of a cryptographic attack is to retrieve the key, rather than the plaintext, from the cipher text. Cryptanalytic attacks exploit the characteristics of the algorithm with some knowledge of the plaintext or sample plaintext-cipher text pair. Based on the nature of attacks on the cryptosystem, the cryptographic attacks can be categorized as cipher text only attack, known plaintext attack, chosen plaintext attack, man-in-the-middle attack, birthday attack, timing attack, side channel attack, correlation attack, power analysis attack, etc. Table 7 shows characteristics of different types of attacks on the encrypted message [5].

Type of attack	Known to attacker
Cipher text only	➢ Cipher text ➢ Encryption algorithm
Known Plaintext	➢ Encryption algorithm ➢ One or more plaintext-cipher text pairs
Chosen Plaintext	➢ Encryption algorithm

	➢ Plaintext chosen by attacker together with corresponding cipher text generated by secret key
Chosen Cipher text	➢ Encryption algorithm ➢ Cipher text chosen by attacker together with corresponding plaintext generated by secret key
Chosen Text	➢ Encryption algorithm ➢ Plaintext chosen by attacker together with corresponding cipher text generated by secret key ➢ Cipher text chosen by attacker together with corresponding plaintext generated by secret key

Table 7. Different types of attack on the encrypted message

In case of a cipher text only attack, one possible approach Eve can use is to check all possible combinations (brute force attack) of the seed key. In this approach if the key space is very large, then this type of approach becomes impractical. In general, in cipher text only attacks, the attacker has the least information available as compared to other types of attacks listed in Table 7. Known and chosen plaintext attacks are crucial in the sense that the attacker has much more information about the plaintext-cipher text pair to analyze. In cryptography, an encryption scheme is called *unconditionally secure* if the generated cipher text does not contain enough information to uniquely identify the plaintext. An encryption scheme is called *computationally secure* if the cost of breaking the encryption scheme exceeds the value of the information or time required to break the encryption scheme exceeds the valuable lifetime of the information.

5.1.1 Cipher text only and Known Plaintext Attack on Single Photon based QKD

Single-photon-based Quantum Key Distribution (QKD) protocol like Bennett-Brassard protocol [54], which is based on microscopic quantum signal that contains one copy of polarized photon, secures against known plaintext and cipher text only attack. Actually, a cipher text only attack on the key, for both single-photon and multi-photon-based approach, does not reveal much information about the key [14]. BB-84 protocol is also secured against known-plaintext attack, as discussed in section 1.4.1, because with one copy of a polarization state and two measurement bases (rectilinear and diagonal), it is not possible for Eve to come to a conclusive result.

5.1.2 Known and Chosen Plaintext Attack on Multiphoton based QKD

In multi-photon based quantum cryptographic approach like Y-00 protocol, is susceptible to known and chosen plaintext attack because this type of approach uses mesoscopic coherent states of significant energy. In this scenario, photon number splitting attack is a very common approach to analyzing multiple photons having the same characteristics (phase, polarization, etc.). One of the main purposes of the Y-00 protocol is to enhance the complexity of the underlying PRNG by randomizing the output sequence due to quantum noise. It is worthy enough to consider the known-plaintext attack scenario in Y-00 protocol to analyze the effect of quantum noise. In section 5.3, bit-flip error due to quantum noise is considered under known plaintext attack scenario to evaluate the effect of quantum noise in LFSR.

5.2 Linear Feedback Shift Register (LFSR)

A Linear Feedback Shift Register (LFSR) belongs to the class of sequential shift register consisting of combinational logic that enables it to pseudo-randomly iterate through a binary sequence [53]. In Fig. 18, a typical 4-bit LFSR is shown. In Fig. 18, 1, 2, 3, 4 denotes the chain of registers, and $\oplus$ represents exclusive-or operation. The "Feedback" term comes from the fact that output of exclusive-or operation between register 3 and register 4 are fed back to register 1. Due to this feedback, LFSR generates a certain length of output sequences of pseudo-random value before it repeats. The "Linear" term arises as the exclusive-or operation is a linear operation. Linear Feedback Shift Register is also known as Pseudo-Random Number Generator (PRNG), and the term "Pseudo" derives from the fact that after each N elements the output sequence repeats itself, unlike True Random Number Generator (TRNG).

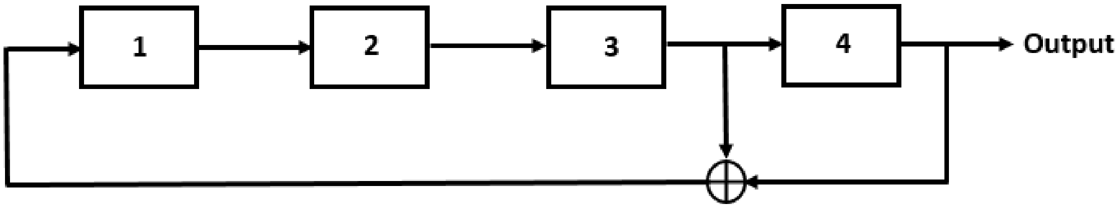


Fig. 18. A 4-bit Linear Feedback Shift Register (LFSR)

In LFSR, the selection of points (taps) between the registers plays an important role in generating maximum length output sequence. For example, the taping between register 3 and 4 as shown in Fig. 18 generates maximum length ($2^4 - 1 = 15$ bits) output sequences before it repeats while taping between register 2 and 4, generates output sequence of only 6 bits long. So, for generating maximum length output sequence by LFSR, the choice of taps is very important.

In general, a typical maximum-length LFSR will generate a pseudo-random sequence of length $2^n - 1$, where n is the number of stages. There can be different combinations of selection of points (taps) to generate a maximum-length output sequence. The output sequence of the LFSR depends on the feedback polynomial, seed value, and the tap positions. A *primitive polynomial mod 2* [5] is generally used as a feedback polynomial in LFSR, and the tap sequences usually describe the exponent in the polynomial. For example, a 4-bit LFSR with tap positions at 3rd and 4th bits (Fig. 18), the primitive polynomial mod 2 becomes,

$$\mathrm{x}^4 + x^3 + 1. \tag{5.1}$$

An output sequence of 4-bit LFSR with tap position at 3-th and 4-th bits positions (Fig. 18) is shown in Table 8.

	Register States				
Sequence Number	Bit 1	Bit 2	Bit 3 (tap)	Bit 4 (tap)	Output Sequence
1	1	1	1	1	1
2	0	1	1	1	1
3	0	0	1	1	1
4	0	0	0	1	1
5	1	0	0	0	0
6	0	1	0	0	0
7	0	0	1	0	0

8	1	0	0	0	1
9	1	1	0	0	0
10	0	1	1	0	0
11	1	0	1	1	1
12	0	1	0	1	1
13	1	0	1	0	0
14	1	1	0	1	1
15	1	1	1	0	0
16	1	1	1	1	1

Table 8. A typical output sequence of 4-bit LFSR

5.3 Bit-flip Error Analysis in LFSR

In this section, we are going to analyze the impact of bit-flip error in the output sequence of LFSR for the prediction of the correct seed key under the condition of known-plaintext attack. In Y-00 protocol, Eve always introduces error while measuring the output sequence of the LFSR due to the quantum noise. This section focuses on the optimal number of required bit-flip error to make the seed key unpredictable from the erroneous observation of the output sequence. As discussed in chapter 4, using ML-POVM technique, we are going to estimate the number of non-orthogonal coherent states and mean photon number to set the probability of measurement error for Eve in a particular range so that from the erroneous observation of the long-running key, it is not possible for Eve to predict the seed key by brute-force attack. For bit-flip error analysis in LFSR, we are going to use a TRUE-KEY selection procedure as described in Table 9.

TRUE-KEY selection in LFSR	
Step 1	Select n-bit LFSR
Step 2	Generate all possible sequences (2^n) of length $2^n - 1$
Step 3	Select a particular seed key with output sequence
Step 4	Get the erroneous sequence with random bit-flip error of length $2^n - 1$
Step 5	Compare all possible output sequences $2^n - 1$ with erroneous sequence to get the least number of bit-flip and estimated seed key
Step 6	If the estimated seed key in step 5 = seed key in step 3: Then, set TRUE-KEY = 1 Else, Set TRUE-KEY = 0

Table 9. TRUE-KEY selection procedure in LFSR

Using TRUE-KEY selection procedure in LFSR, we have analyzed effective bit-flip error required in the output sequence of the 4-bit, 8-bit, and 16-bit LFSR respectively, as described in Figs. 19, 20 and 21, to make the seed-key unpredictable by brute-force attack.

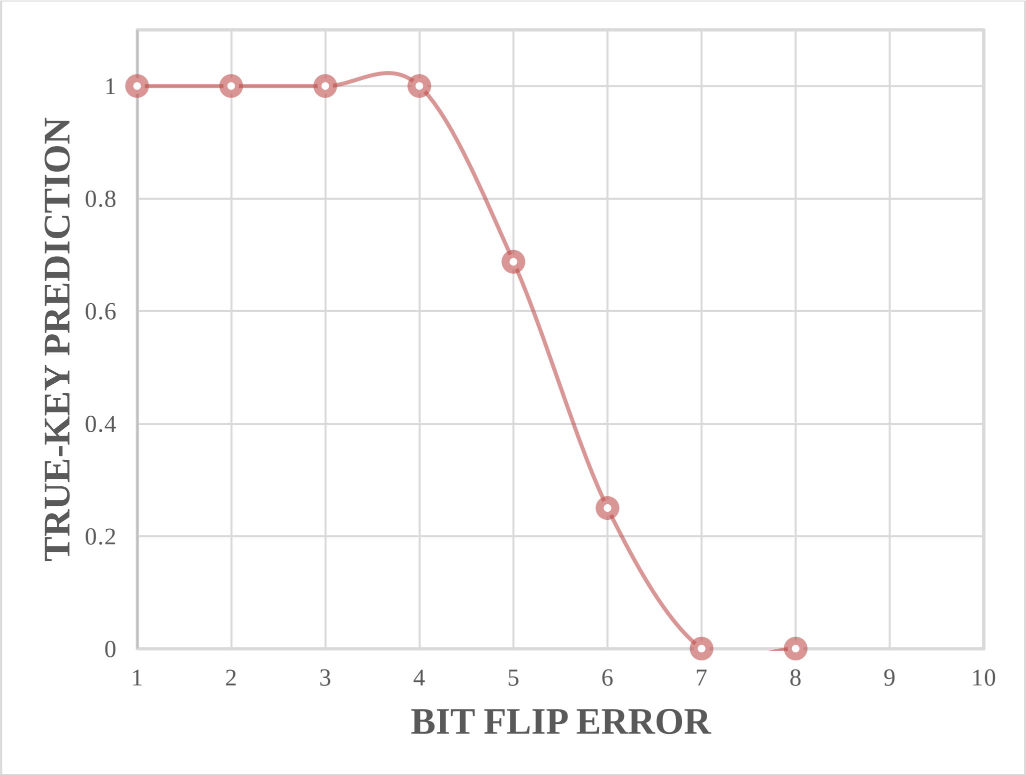


Fig. 19. TURE-KEY selection in 4-bit LFSR

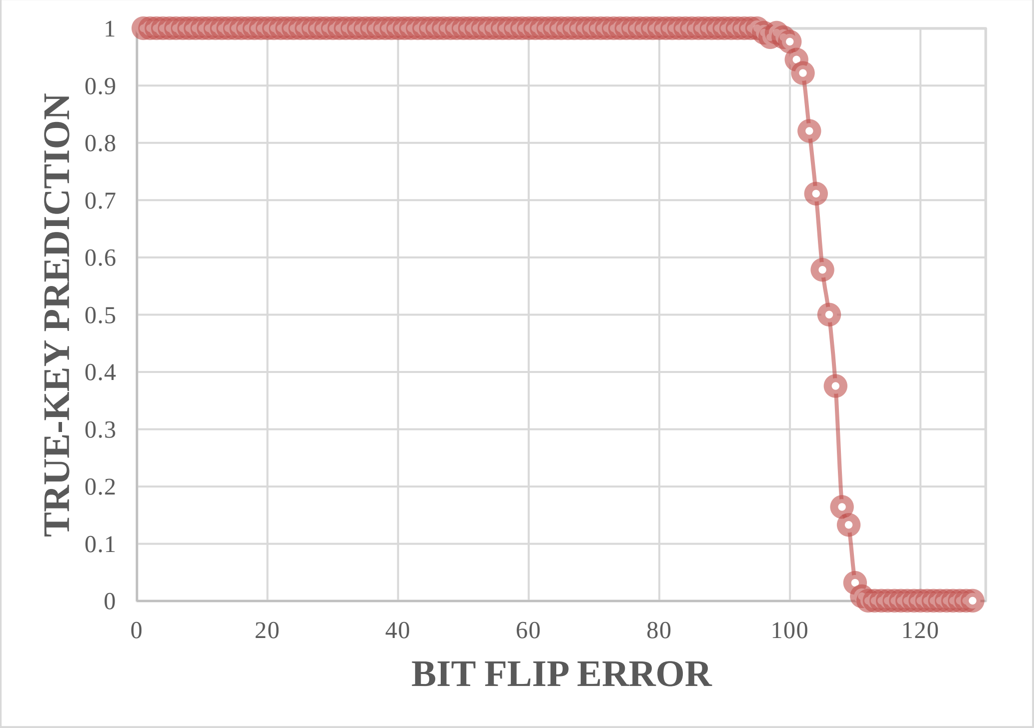


Fig. 20. TRUE-KEY selection in 8-bit LFSR

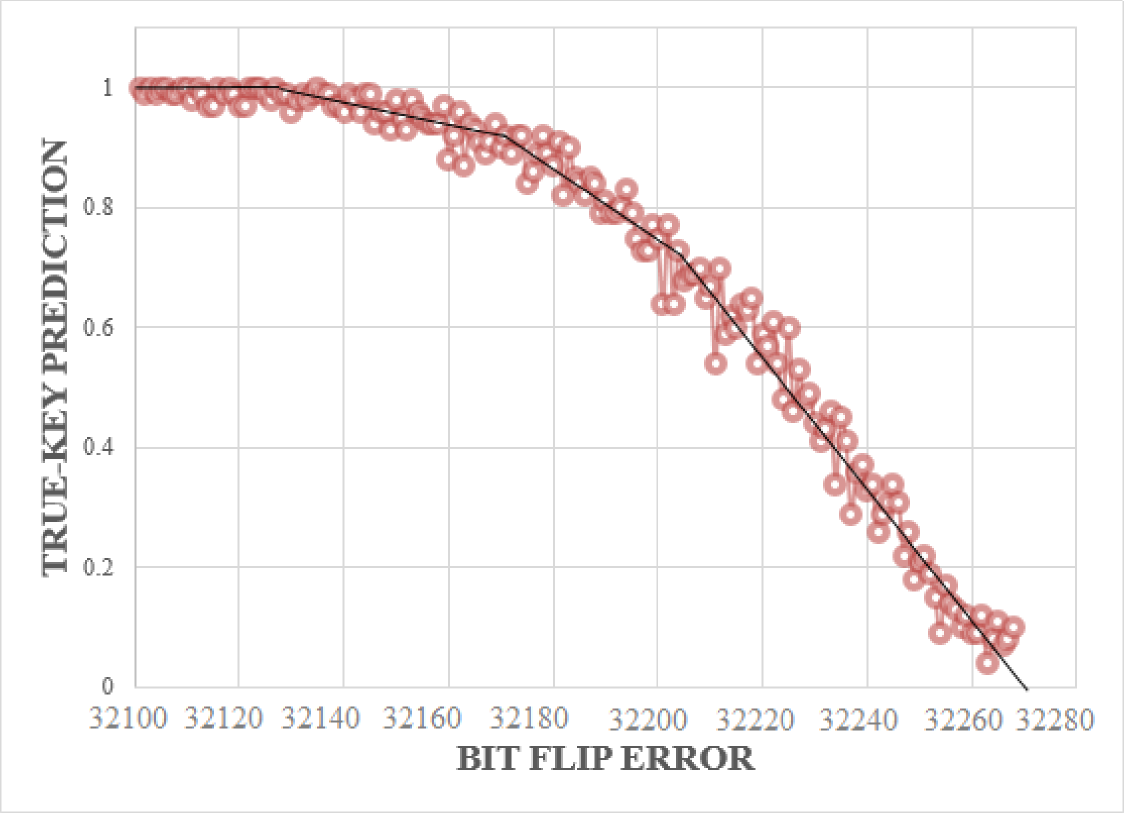


Fig. 21. TRUE-KEY selection in 16-bit LFSR

The feedback polynomials used to implement these three different types of maximum-length LFSR are as follows:

$$\begin{gathered} \mathrm{x}^4 + x^3 + 1 \\ x^8 + x^6 + x^5 + x^4 + 1 \\ x^{16} + x^{15} + x^{13} + x^4 + 1 \end{gathered} \tag{5.2}$$

From the Figs. 19, 20 and 21, one can see that a significant portion of bit-flip error is required to make the seed key unpredictable in LFSR by brute-force attack. If the length of the input-space of LFSR increases, the number of required bit-flip error also increases. For example, in case of 8-bit LFSR (period is 255), more than 100 bit flip errors are required to make the seed key unpredictable by brute-force attack whereas for 16-bit LFSR (period is 65535), more than 30100 bit-flip errors are required to make the seed key unpredictable. This is due to the co-relation between the output and input sequences of the LFSR and the choice of the internal configuration of the LFSR. This type of attack is called *correlation attack* and belongs to the class of known plaintext attacks. Stream cipher like LFSR is very susceptible to correlation attack [55, 56]. If the length of the input space is very large in LFSR, then significantly large numbers of bit-flip error are required in the output sequence to make the seed key unpredictable by any attacker.

5.3.1 Success Probability Calculation for Seed Key Estimation in LFSR

In cryptography, it is assumed that an attacker has unlimited computational power. If an attacker gets hold on the full copy of the output sequence of the LFSR, even though it is erroneous output due to measurement error, there has to be significant number of errors to prevent the attacker from accurate prediction on the seed key. In order to estimate the success probability for estimating the correct seed key for a given number of bit-flip error in the output sequence due to measurement error, we have proposed success probability as follows:

$$\mathrm{p}\ [\mathrm{K_s}|\mathrm{E_{bit-flip}}(\mathrm{M},|\alpha|^2)] = \frac{\mathrm{C}^{n}_{\mathrm{E}_{bit-flip}}}{\sum_{i=1}^{\mathrm{C}^{n}_{\mathrm{E}_{bit-flip}}} Rank_{effective}(of\ all\ probable\ seed\ key)} \tag{5.3}$$

In (5.3), K_s is the running seed key of the LFSR, $\mathrm{E_{bit-flip}}$ is the number of bit-flip errors that Eve encountered in the output sequence of the LFSR for a given number of non-orthogonal coherent states (M) and mean photon number ($|\alpha|^2$), $\mathrm{C}^{n}_{\mathrm{E}_{bit-flip}}$ represents different possible combination of the bit-flip error in the output sequence of the LFSR.

For example if the output sequence, n, is 255 and bit-flip error due to quantum noise, $\mathrm{E}_{\mathrm{bit-flip}}$ is 4, then $\mathrm{C}_{\mathrm{E}_{bit-flip}}^{n}$ becomes C_{4}^{255}. In (5.3), $Rank_{effective}$ has special meaning. Rank for a given number of bit-flip error is calculated by considering the fact that there is a minimum number of bit-flip required in the correct output sequence to get the same erroneous output sequence. For example, the output sequence is 255 bit long and there is 4-bit flip error in the output sequence, and if the output sequence for seed key-2 (seed key number) needs minimum number of bit-flip to get the same erroneous output, then the rank for the seed key-2 will be 1. Similarly for other seed keys, the corresponding ranking 1, 2, 3 etc. are calculated to get the same erroneous output sequence. Due to the correlation between the input and output sequence in the LFSR, it is very much obvious that there is always a high possibility to get more than one seed key which belong to same rank. Now, $Rank_{effective}$ is calculated in slightly different way. For example in 8-bit LFSR, effective operating seed key is key-2 and Eve retrieves the output sequence with 105-bit-flip errors. The calculated rank for seed key-2 is 2, then all other seed keys having rank up to 2 belong to $Rank_{effective}$. In this scenario, if seed key-4, 5, and 6 have rank 1, 1 and 2 respectively and actual seed key-2 is of rank 2 then value of $Rank_{effective}$. becomes 4. Using these considerations, the success probability $\mathrm{p}[\mathrm{K_s}|\mathrm{E}_{\mathrm{bit-flip}}(\mathrm{M}, |\alpha|^2)]$for correctly estimating operating seed key is calculated for 4-bit, 8-bit LFSR respectively and is shown in Figs. 22 and 23. From Figs. 22 and 23, it is worth mentioning that, if the length of the input space is in increasing order, it needs higher number of bit-flip errors in the output sequence to reduce the success probability of correctly estimating the seed key by any eavesdropper.

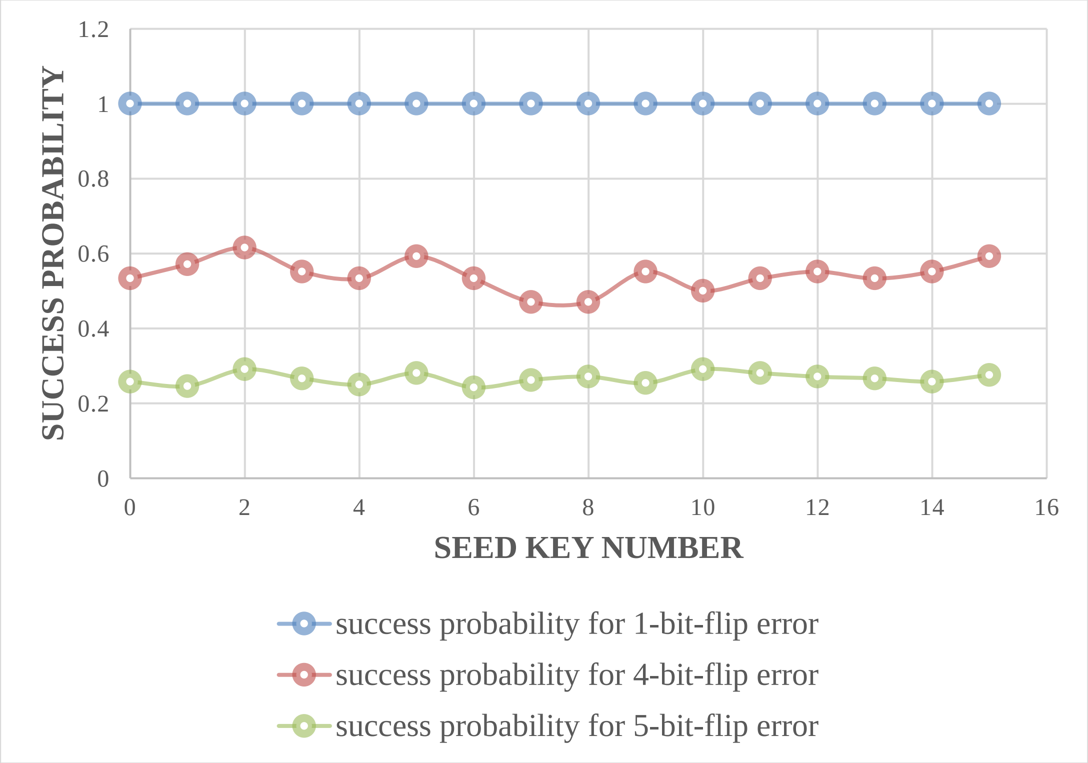


Fig. 22. Success probability for estimating seed key in 4-bit LFSR

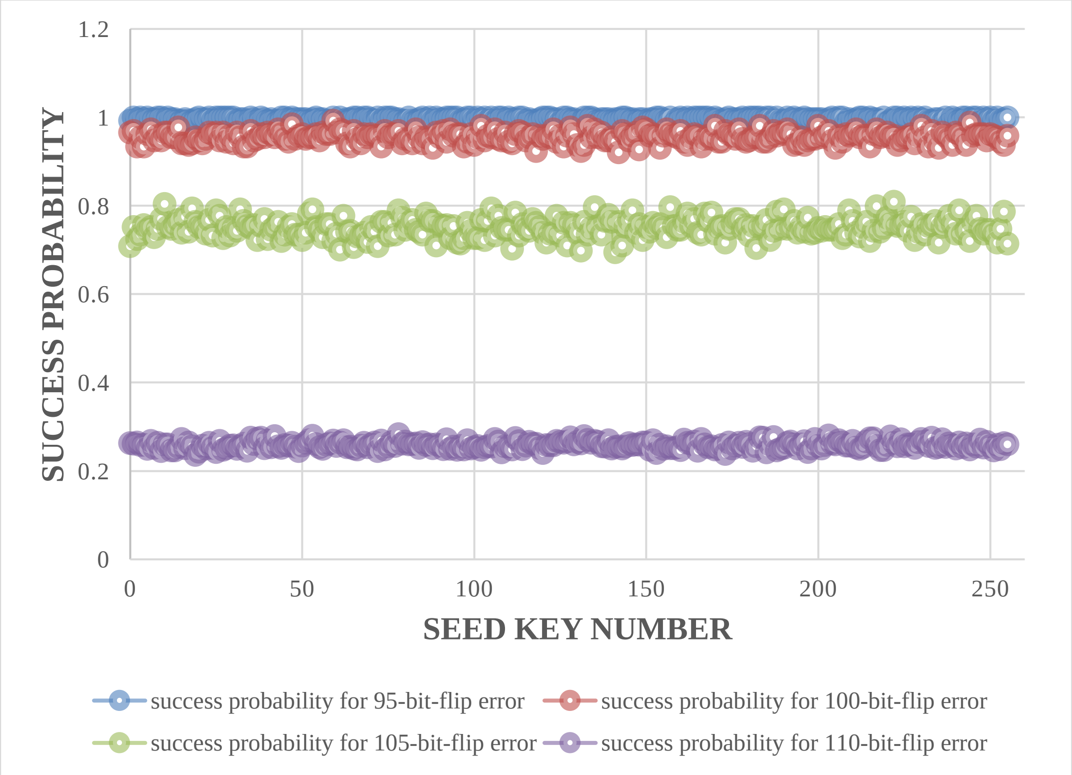


Fig. 23. Success probability for estimating seed key in 8-bit LFSR

5.4 Bit-flip Error Analysis in NLFSR

In this section, we will consider Non-Linear Feedback Shift Register (NLFSR) as a PRNG. In paper [57], Y-00 protocol is realized by implementation of NLFSR. Generally, Non-LFSR is a generalization of LFSR, where present state of the register is an output of the non-linear combination of the previous state [58]. In Fig. 24 a typical set-up for maximal-length 4-bit NLFSR is shown. In this figure, both "AND" and "EXCLUSIVE-OR" operations are utilized to generate nonlinearity in the output sequence [59].

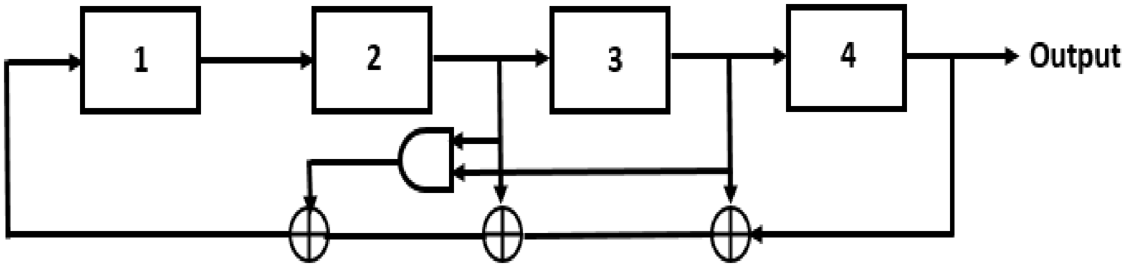


Fig. 24. A typical maximal-length 4-bit NLFSR

Now, using the same procedure as discussed in section 5.3.1, we have calculated success probability of predicting seed key for a given number of bit-flip error in the output sequence of the NLFSR. The calculated success probabilities for 4-bit and 8-bit NLFSR are shown in Figs. 25 and 26, respectively. The feedback polynomial used in NLFSR is:

$$\mathrm{x}^4 + x^3 + x^2 + x^3.x^2 + 1$$
$$x^8 + x^5 + x^4 + x^7.x^4.x^3 + 1 \tag{5.4}$$

From Figs. 25 and 26, it is clear that if Eve gets hold on the full copy of output sequence, whether it is from LFSR or NLFSR, there should be significant number of bit-flip error to prevent correlation attack. So far, in terms of maximal-length NLFSR implementation, number of bit length in input sequence is limited to only $n \leq 25$ [60].

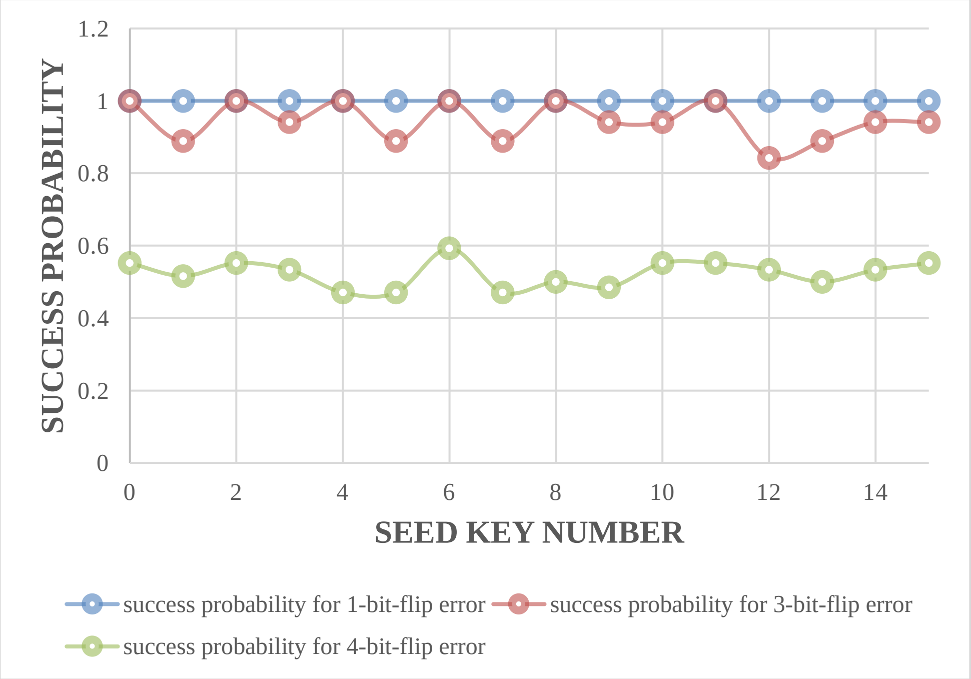


Fig. 25. Success probability for estimating seed key in 4-bit-NLFSR

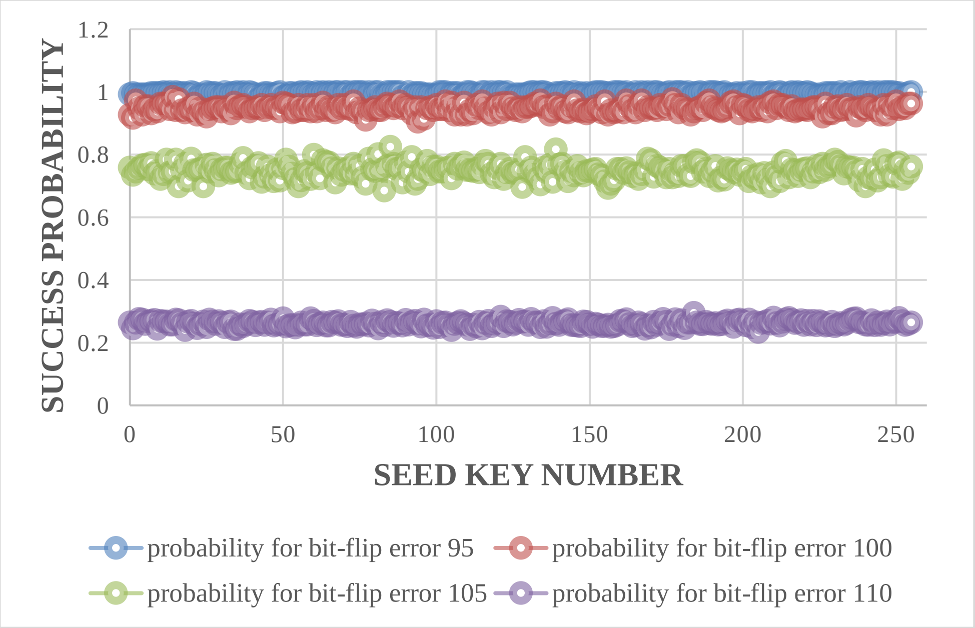


Fig. 26. Success probability for estimating seed key in 8-bit-NLFSR

5.5 Summary

In this chapter, we have started our discussion on two prominent cryptographic attacks, namely as known plaintext and cipher text attack. Known plaintext attack is particularly important for multiphoton-based cryptographic approach because there is always a probability for Eve to get additional copy of the quantum state to measure it. Then, we discuss on the working principle of the LFSR as a PRNG. Next, bit-flip error analysis is carried out on 4-bit, 8-bit and 16-bit LFSR to evaluate the effect of the erroneous output on predicting the correct seed key of the LFSR. It has been proven that, the tap positions, feedback polynomial, Boolean operations, choice of underlying structure in the LFSR play important role to minimize the correlation between input and output sequences. After that, an equation of success probability of estimating the seed key for a given number of bit-flip error due to number of non-orthogonal coherent states and mean photon number is given. It has been shown that, if the input space of the LFSR is large enough then subsequently large number of bit-flip error is required to prevent known plaintext attack by Eve. Finally, a similar bit-flip error analysis is conducted on 4-bit and 8-bit NLFSR respectively, which also shows strong correlation between the input and output sequence.

Chapter 6: Conclusion and Future Work

This chapter begins with the conclusion of this research work. As Y-00 protocol is a multiphoton-based quantum cryptographic approach, it has practical implications to be implemented with the existing optical fiber technology. Currently, several initiatives for the implementation of Y-00 protocol are ongoing [31]. Finally, this chapter presents few specific working scopes, which can be carried out in future.

6.1 Conclusion

Y-00 utilizes a shared secret key to determine quantum signal set for individual information sequence. Also quantum noise plays a major role in enhancing the complexity and security of classical cipher according to quantum measurement, estimation and detection theory. In Y-00, there is theoretical constraint to exceeding the Shannon limit in cryptography, and there is a certain bound on device limitation to provide security against known plaintext attacks. From the presented results, it has been proven that for non-orthogonal coherent state detection, ML-POVM provides better success probability for coherent-state discrimination than do other measurement techniques such as greedy scheme, quantum unambiguous measurement, random guessing, etc. In Y-00 implementation schemes, Linear Feedback Shift Register (LFSR) is used as a PRNG to generate long-running keys. Due to the correlation between input and output sequence of LFSR, the choice of feedback function, underlying algorithm, and length of the input seed key play important role in preventing correlation attack by an eavesdropper. As in quantum cryptography, it is a universal concept that an eavesdropper always poses unbounded computational power. If Eve by any means, gets a hold on the whole output sequence of the LFSR by known-plaintext attack, then a significant proportion of bit-flip error is required in the output sequence to prevent Eve from correctly estimating seed key. Moreover, Non-LFSR, which is a generalization of LFSR, shows almost the same degree of correlation between input and output sequences like LFSR.

6.2 Future Work

This research work is the first time that recently formulated maximum-likelihood POVM technique to measure the phase randomized polarization of the non-orthogonal coherent states have been introduced. Besides, there are still a few more particular working scopes available regarding the performance evaluation of Y-00 protocol.

6.2.1 Practical Implementation of ML-POVM technique in Y-00 scheme

The immediate working scope could be practical implementation of ML-POVM measurement technique into Y-00 scheme. To restrict Eve's performance, the number of coherent states and mean photon number are two important factors in the ML-POVM measurement technique. Moreover, the speed and memory required to map the running key sequence to a coherent basis selection are also necessary to evaluate synchronization between two legitimate users.

6.2.2 Detailed Proof of Working Methodology of Y-00 Scheme

To date, Y-00 protocol suffers from rigorous proof of showing how it exceeds the Shannon limit in cryptography. Though, the necessary condition (Equation 3.2) to exceed the Shannon limit is well established [22], the sufficient condition (Equation 3.3) is suffering from rigorous proof. The working principle of Y-00 protocol is based on the fact that the inherent quantum uncertainty will increase the overall complexity of the LFSR by exceeding Shannon limit, the theoretical and practical proof of this sufficient condition could be an important future working scope in Y-00 protocol.

6.2.3 Implementation of Machine Learning Approach in Y-00 Scheme

Machine learning is all about creating an effective algorithms and methods so that a system can learn from the intercepted data, analyze the data, and be able to predict the future based on perceived knowledge. Though, implementation of machine learning concepts in the quantum world is new, this approach can be implemented in Y-00 protocol, especially to analyze Eve's performance on the intercepted data. For example, using the ML-POVM measurement technique, for a given number of non-orthogonal coherent states and mean photon numbers, the failure probability of coherent state detection for Eve can be calculated. Now, if Eve introduces bit-flip error in the output sequence of the LFSR during the failure events of correctly identifying the coherent states, she can calculate a particular rank for different seed keys as described in section 5.3.1.

In Fig. 27 shows histograms of different ranks of randomly chosen running seed key-2 (seed key number): 110 bit-flip error (Fig. 27(a)) and 120 bit-flip error (Fig. 27(b)) in the output sequence of 8-bit LFSR. Similarly, Fig. 28 shows histograms of different ranks of another randomly chosen running seed key-30 in 8-bit LFSR. In order to calculate rankings for both randomly chosen seed keys, 255 different random combinations of 110 and 120 bit-flip errors in the output sequence (255-bit sequence) are considered out of C_{110}^{255} and C_{120}^{255} different possible combinations, respectively. From Figs. 27 and 28, it is clear that if the number of bit-flip errors are increased in the output sequence of the LFSR, corresponding rankings of the running seed key are also increased.

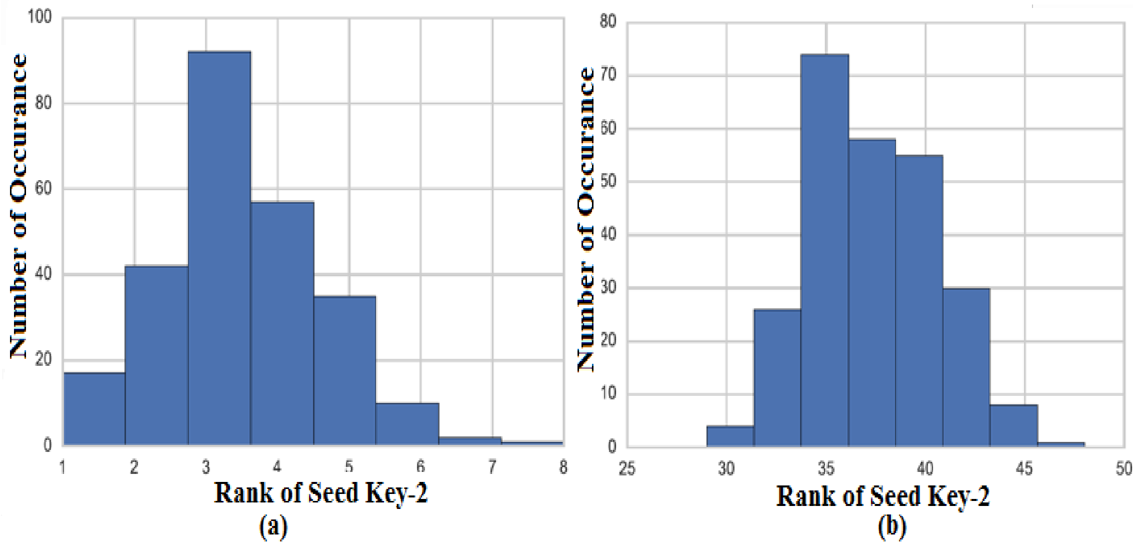


Fig. 27. Histogram of different rank of seed key-2 for 110 bit-flip error (a) and 120 bit-flip error (b) in the output sequence of 8-bit LFSR

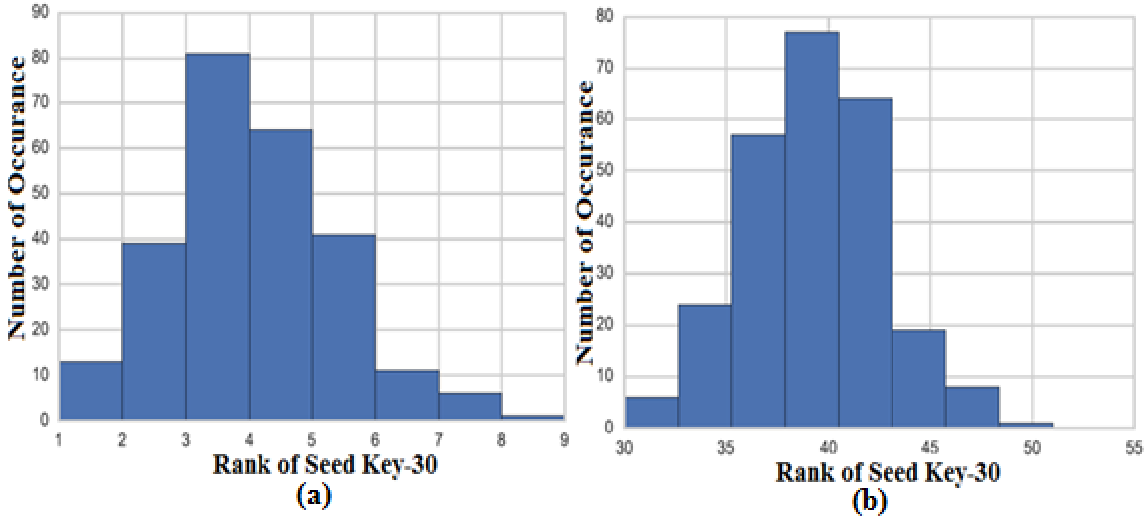


Fig. 28. Histogram of different rank of seed key-30 for 110 bit-flip error (a) and 120 bit-flip error (b) in the output sequence of 8-bit LFSR

From these observations, Eve can train any suitable classifier of machine learning algorithm to predict the input of the LFSR and in this scenario, *Naïve Bayes* classifier [61] could be one of the best candidates to predict the running seed key. Fig. 29 shows a typical workflow of machine learning.

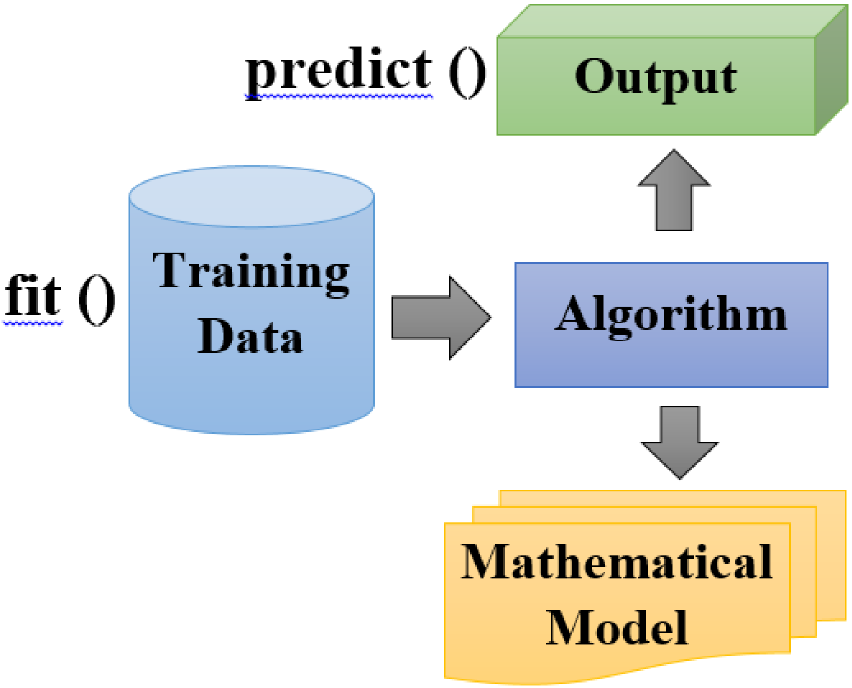


Fig. 29. A typical workflow of machine learning

Moreover, one of the main advantages of using a machine learning algorithm in predicting seed key of the LFSR from the observation of the output sequence is that there is no definite need to measure the whole output sequence of the LFSR because Eve can train her classifier based on her measured observation of any length, even though more data on the measured observation of the output sequence will help the classifier to predict the seed key more accurately.

References

[1] Heisenberg, W. (1927), "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik", Zeitschrift für Physik (in German), 43 (3–4): 172–198, Bibcode: 1927 ZPhy.43.172H, doi:10.1007/BF01397280.. Annotated pre-publication proof sheet of Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik, March 21, 1927.

[2] W. Wootters and W. Zurek, "The no-cloning theorem", Phys. Today, vol. 62, no. 2, pp. 76-77, 2009.

[3] Bennett, C. H. "G. Brassard in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India,(New York)." (1984): 175.

[4] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography. p. 10.

[5] Stallings, William. Cryptography and network security: principles and practices. Pearson Education India, 2006.

[6] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.

[7] Busch, Paul, Teiko Heinonen, and Pekka Lahti. "Heisenberg's uncertainty principle." Physics Reports 452.6 (2007): 155-176.

[8] Wootters, William K., and Wojciech H. Zurek. "A single quantum cannot be cloned." Nature 299.5886 (1982): 802-803.

[9] Wilde, Mark M. "From classical to quantum Shannon theory."arXiv preprint arXiv:1106.1445 (2011).

[10] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers Systems and Signal Processing, pages 175{179, Bangalore, India, December 1984.

[11] I. Chakrabarty, A. Pati, and S. Adhikari, "Stronger no-cloning, no-signalling and conservation of quantum information," arXiv preprint quant-ph/0605173, 2006.

[12] Polarization. Available:
http://www.physicsclassroom.com/class/light/Lesson-1/Polarization

[13] Korchenko, Oleksandr, Yevhen Vasiliu, and Sergiy Gnatyuk. "Modern quantum technologies of information security against cyber-terrorist attacks."Aviation 14.2 (2010): 58-69.

[14] Yuen, Horace P. "KCQ: A new approach to quantum cryptography I. general principles and key generation." arXiv preprint quant-ph/0311061 (2003).

[15] Yuen, Horace P. "Key generation: foundations and a new quantum approach." IEEE Journal of Selected Topics in Quantum Electronics 15.6 (2009): 1630-1645.

[16] C.E. Shannon. Communication theory of secrecy systems. Bell System Technical Journal, 28:656{715, October 1949

[17] C.E. Shannon. A mathematical theory of communication. Bell Systems Technical Journal, 27(3):379{423, July 1948

[18] Cover, Thomas M., and Joy A. Thomas. "Elements of information theory 2nd edition." (2006).

[19] Prelov, Vyacheslav Valer'evich, and Edward C. van der Meulen. "Mutual information, variation, and Fano’s inequality." Problems of Information Transmission 44.3 (2008): 185-197.

[20] Vilnrotter, Victor, and Chi-Wung Lau. "Quantum detection and channel capacity for communications applications." High-Power Lasers and Applications. International Society for Optics and Photonics, 2002.

[21] Hirota, Osamu, et al. "Quantum key distribution with unconditional security for all-optical fiber network." Optical Science and Technology, SPIE's 48th Annual Meeting. International Society for Optics and Photonics, 2004.

[22] Hirota, Osamu, and Masaki Sohma. "Towards a New Way of Quantum Communication: Getting around the Shannon Limit of Cryptography." 玉川大学量子情報科学研究所紀要= Tamagawa University Quantum ICT Research Institute bulletin 1.1 (2011): 1-13

[23] G.A.Borbosa, E.Corndorf, G.S.Kanter, P.Kumar, and H.P.Yuen, Secure communication using mesoscopic coherent state, Physical Review Letters, vol-90, 227901, 2003

[24] Hirota, Osamu, et al. "Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme." Physical Review A. 72.2 (2005): 022335

[25] Kato, Kentaro. "Error performance of intensity modulation-based quantum stream cipher by Yuen 2000 protocol with nonlinear pseudorandom number generator."SPIE Optical Engineering Applications. International Society for Optics and Photonics, 2009.

[26] Hirota, Osamu, et al. "Quantum stream cipher beyond the Shannon limit of symmetric key cipher and the possibility of experimental demonstration." SPIE Optical Engineering Applications. International Society for Optics and Photonics, 2010.

[27] Kato, Kentaro, and Osamu Hirota. "Randomization techniques for the intensity modulation-based quantum stream cipher and progress of experiment." SPIE Optical Engineering Applications. International Society for Optics and Photonics, 2011.

[28] Hirota, Osamu, and Fumio Futami. "Progress in Y-00 physical cipher for Giga bit/sec optical data communications (intensity modulation method)."SPIE Optical Engineering Applications. International Society for Optics and Photonics, 2014.

[29] Walls, Daniel F., and Gerard J. Milburn. Quantum optics. Springer Science & Business Media, 2007

[30] Hirota, Osamu, and Kaoru Kurosawa. "Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol." Quantum Information Processing 6.2 (2007): 81-91.

[31] Harasawa, K. New Quantum Cipher Optical Communication: Y-00. INTECH Open Access Publisher, 2012.

[32] Hirota, Osamu, et al. "Quantum stream cipher based on optical communications." Optical Science and Technology, the SPIE 49th Annual Meeting. International Society for Optics and Photonics, 2004.

[33] Hirota, Osamu, et al. "A quantum symmetric key cipher (Y-00) and key generation (Quantum stream cipher-Part II)." Moscow, Russia. International Society for Optics and Photonics, 2005.

[34] Helstrom, Carl W. Quantum detection and estimation theory. Academic press, 1976.

[35] Nielsen, Michael A., and Isaac L. Chuang. Quantum computation and quantum information. Cambridge university press, 2010.

[36] Müller-Quade, Jörn, and Renato Renner. "Composability in quantum cryptography." New Journal of Physics 11.8 (2009): 085006.

[37] Biham, Eli, et al. "A proof of the security of quantum key distribution." Journal of cryptology 19.4 (2006): 381-439.

[38] Niemiec, Marcin, and Andrzej R. Pach. "The measure of security in quantum cryptography." Global Communications Conference (GLOBECOM), 2012 IEEE. IEEE, 2012.

[39] Hirota, Osamu. "Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol." Physical Review A. 76.3 (2007): 032307.

[40] Tomamichel, Marco, and Anthony Leverrier. "A rigorous and complete proof of finite key security of quantum key distribution."arXiv preprint arXiv:1506.08458(2015).

[41] Iwakoshi, Takehisa, Fumio Futami, and Osamu Hirota. "Quantitative analysis of quantum noise masking in quantum stream cipher by intensity modulation operating at G-bit/sec data rate." SPIE Security Defense. International Society for Optics and Photonics, 2011.

[42] Stinson, Douglas R. Cryptography: theory and practice. CRC press, 2005.

[43] Jones, Joshua A., Anthony J. D'Addario, and Enrique J. Galvez. "The Poincaré-sphere approach to polarization: Formalism and new labs with Poincaré beams."

[44] Stokes parameters. Available: http://en.wikipedia.org/wiki/Stokes_parameters

[45] E. B. Davies, "Quantum theory of open systems," 1976.

[46] POVM. Available: https://en.wikipedia.org/wiki/POVM

[47] Zhang, Lu, Kam Wai Clifford Chan, and Pramode K. Verma. "Universal optimal estimation of the polarization of light with arbitrary photon statistics."Physical Review A. 93.3 (2016): 032137.

[48] Maximum likelihood estimation. Available: https://en.wikipedia.org/wiki/Maximum_likelihood_estimation

[49] Chefles, Anthony, and Stephen M. Barnett. "Optimum unambiguous discrimination between linearly independent symmetric states." arXiv preprint quant-ph/9807023 (1998).

[50] Ivanovic, Igor D. "How to differentiate between non-orthogonal states." Physics Letters A. 123.6 (1987): 257-259.

[51] Peres, Asher. "How to differentiate between non-orthogonal states." Physics Letters A. 128.1 (1988): 19.

[52] Bagan, E., A. Monras, and R. Munoz-Tapia. "Comprehensive analysis of quantum pure-state estimation for two-level systems. "Physical Review A71.6 (2005): 062318.

[53] Linear-feedback shift register. Available: https://en.wikipedia.org/wiki/Linear-feedback_shift_register

[54] Bennett, C., "Quantum cryptography using any two nonorthoganol states." Phys. Rev. Lett. 68, 1992, pp. 3121-3124.http://prola.aps.org/pdf/PRL/v68/i21/p3121_1

[55] Donnet, Stéphane, et al. "Security of Y-00 under heterodyne measurement and fast correlation attack." Physics letters A 356.6 (2006): 406-410.

[56] Yuen, Horace P., and Ranjith Nair. "On the security of Y-00 under fast correlation and other attacks on the key." Physics Letters A. 364.2 (2007): 112-116.

[57] Kato, Kentaro. "Error performance of intensity modulation-based quantum stream cipher by Yuen 2000 protocol with nonlinear pseudorandom number generator."SPIE Optical Engineering Applications. International Society for Optics and Photonics, 2009.

[58] Nonlinear Feedback Shift Register. Available: http://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_361

[59] Maximum Period NLFSR. Available: https://people.kth.se/~dubrova/nlfsr.html

[60] Dubrova, Elena. "A List of Maximum Period NLFSRs." *IACR Cryptology ePrint Archive* 2012 (2012): 166.

[61] Nilsson, Nils J. "Introduction to machine learning. An early draft of a proposed textbook." (1996).