ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -02 February, 2016 Page No. 15685-15699

On the Underlying Mathematical and Quantum Structures of Quantum Cryptography

Ajey Dilip Gotkhindikar
Department of Mathematics,
Tampere University of Technology,
Korkeakoulunkatu 10, FI-33720 Tampere
ajey.gotkhindikar@student.tut.fi

Abstract

Quantum cryptography is a novel approach to provide secure communication, based on the laws of physics. It offers perfect security for the communication between two authorized parties, while assuming very high computational capacity for the eavesdropper, who may be attempting to intrude into this communication. It provides a very high rate of intrusion detection as against the classical systems. Classical cryptography is built on a fundamental assumption that it is difficult to invert some of mathematical functions, in a limited time, with the use of efficient computing resources. While, quantum cryptography is based on formidable laws of nature, making it less prone to attack.

With the advent of quantum computing, boundaries between various subjects like quantum physics, computer science and mathematics are getting reduced. In the early seventies, Steven Wiesner made pioneering efforts in the field Quantum Cryptography. In its present form, Quantum Cryptography depends on two essential principles of Quantum Mechanics. One is that no information is available without causing disturbance in the system and other is Principle of No-Cloning. In this paper we present some of fundamental aspects of Quantum Cryptography and the underlying structures that makes it a credible option for providing perfect security of information.

Keywords: Hilber Space Formalism, No-cloning Theorem, Quantum Entanglement, Quantum Cryptography, Quantum Key Distribution

1 Introduction

Security provided by *quantum cryptography* does not rely on vulnerabilities like, mathematical sophistication to invert certain mathematical functions, algorithmic swiftness used for decryption, or higher computational resources available at the hand of an adversary. Development in the field of quantum cryptography stems from the quest of having a perfectly secure cryptographic technique. Classical cryptosystems which mainly rely on complexities of mathematical operations and on the assumption of limited computational resources with the intruder, have shortcomings in detecting eavesdropping.

In section 1.1 and section 1.2 of this text we discuss in brief about classical and quantum cryptography. In section 2 we proceed to understand the underlying mathematical and quantum mechanical structures which provide strong foundation for developing quantum cryptography. Section 3 focuses on what is quantum cryptography and the notion of quantum key distribution as a perfectly secure method to establish secret key among authorized parties in the communication. Throughout this text we address sender as A (for Alice), receiver B (for Bob) and eavesdropper E (for Eve).

DOI: 10.18535/ijecs/v5i2.6

1.1 A Note on Classical Cryptography

A critical part in the process of secure communication is the exchange of key or a secret between authenticated parties involved in the communication. A key is a vital secret, compromise of which could be detrimental to the very basis of cryptosystems. Depending on the nature of secure exchange of keying material, classical cryptosystems are divided into following major categories.

Private Key Cryptosystems

Public Key Cryptosystems

One of the example of perfectly secure ciphers in classical cryptosystems is Vernam cipher or One-time pad. There are two important features of this cipher to be noted: First, that the message and the key have the same length and second, each key must be used only once [1]. This cipher has been proven most secure because it does not reveal any information about the plaintext. But it faces two potential problems, one is, if the size of the message grows, the size of the key increases accordingly and second is, since each message requires new key, a large amount of secret keys have to be distributed among the parties involved in the communication.

While execution of private key cryptosystems is very fast yet they suffer from a major drawback of secure key distribution. The problem of secure key distribution is solved by the public key cryptosystems [2]. Public key cryptography deploy mathematical process that is responsible for generating what is known as public key and private key pair, which are computationally related to each other. Private keys are safe in the custody of individual parties involved in communication, while public key is available at large. This cryptosystem is based on unproven mathematical assumption that it is difficult to derive private key from the public key in a limited time [3]. Certainly, this assumption is made on the efficiency of current computational resources. This possible security threat to the ciphers that are based on complexity of solving mathematical function, has led researchers to seek for novel approach to provide secure communication.

1.2 A Note on Quantum Cryptography

Quantum Cryptography uses microscopic objects such as individual photons as information carries [4]. Main advantages of Quantum Cryptography is in its successful demonstration of perfectly secure data transfer, modalities of which are based on universal laws of quantum mechanics. Quantum Cryptographic systems take advantage of Heisenberg's uncertainty principle, according to which measuring a quantum system in general disturbs it and yields insufficient information about its state before the measurement [5, 6]. This prompts that any attempt of eavesdropping would then cause unavoidable disturbance in the system, alerting about this attempt to the legitimate users [7]. What makes Quantum Cryptography superior is *No cloning Theorem*, which states that an unknown quantum state can not be cloned [8]. Thus, absolute security in quantum cryptography is provided based on two major forbidding in quantum physics, one claims that it is impossible to make measurement of quantum state without imposing disturbances and second claims that it is impossible to clone an unknown quantum state. Based on this, it is very clear that any eavesdropping in data transfer will cause irreversible changes in quantum state and eavesdropping could then be established.

There is another important quantum mechanical phenomenon of *quantum entanglement*, that has added to the design of cryptography based on Quantum Information theory. Entanglement is non-local quantum mechanical correlation in which two quantum systems, that have been interacting at some point, can be expressed with reference to each other, even though the individual systems may be spatially separated [9, 10].

These quantum phenomenons have led to the emergence of protocols for Quantum Communication [11]. A survey [12] presents applications of principles in quantum mechanics to the field of Cryptography. Bennett and Brassard first presented QKD protocol in 1984 which is known as BB84 [13, 14]. First experimental demonstration [15] of this protocol which sought attention of research community for possible wider exploration of this field. In 1992 Bennett [16] proposed

improvements in BB84 coding scheme by utilizing two out of four states in BB84. Six state protocol [17, 18] added another alternative to existing QKD protocols. Ekert [19] presented innovative method of distributing quantum key through entangled states based on Einstein-Podolsky-Rozen paradox. Gisen et al [20] summarized information on various cryptographic protocols.

In the next section we discuss about mathematical and quantum mechanical structures on which quantum cryptography is based.

2 Preliminaries

The observations on quantum systems are stochastic in nature and that calls for the understanding of probabilistic systems. In case of probabilistic systems, it is difficult to have exact knowledge of state of the system and it is expressed as probability distribution of the states. We say that states of the system $x_1, \ldots, x_n$ have probabilities $p_1, \ldots, p_n$ such that,

$$p_1[x_1] + p_2[x_2] + \ldots + p_n[x_n] \tag{2.1}$$

where $p_i > 0$ and $p_1 + \ldots + p_n = 1$ is probability distribution, for the system is in state x_i with probability p_i. The quantum systems are expressed in somewhat similar way.

Understanding of fundamental linear algebraic notions like linear operators, vector arithmetic notions, vector space, norm, basis, dimension of vector spaces, normalization, inner product space, eigenvalues, eigenvectors etc., is utmost essential and we refer to [21] for further details. In section 2.1 we cover some of the essential linear algebraic notions.

2.1 Mathematical Structures for Quantum Systems

Definition 1. *If n is a positive integer, then a sequence of n real (or complex) numbers $(a_1, a_2, \ldots, a_n)$ is called an* ***ordered-n-tuple****. The set of all ordered n-tuple is called* ***n-space*** *and it is denoted by $\mathbb{R}^n$ over real number and by $\mathbb{C}^n$ over complex numbers. For the current discussion we use notation F^n to denote either $\mathbb{R}^n$ or $\mathbb{C}^n$.*

Vector spaces in which scalars are real numbers, are called **real vector spaces**, and those in which scalars are complex numbers, are called **complex vector spaces**.

The space of n-tuple complex numbers is very important in complex vector spaces. It is denoted as $\mathbb{C}^n$. A vector $u \in \mathbb{C}^n$, $(u = u_1, u_2, \ldots, u_n)$, given as,

$$u_1 = a_1 + b_1 i, u_2 = a_2 + b_2 i, \ldots, u_n = a_n + b_n i$$

The *inner product* of two vectors is equivalent to a row vector of first vector multiplied column vector of the second vector. If $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ are vectors in F^n then their inner product is given as,

$$\begin{aligned}
\langle u, v \rangle &= u \cdot v = u^t v \\
&= (u_1, u_2, \ldots, u_n) \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \\
&= u_1 v_1 + u_2 v_2 + \ldots + u_n v_n \\
&= \sum_{i=1}^{n} u_i v_i
\end{aligned}$$

Definition 2. *An* ***inner product*** *on a vector space V is a function that associates a number $\langle u, v \rangle \in F$, with each pair of vectors u and v in V in such a way that the following axioms hold for all vectors u, v and w in V and all scalars k.*

DOI: 10.18535/ijecs/v5i2.6

1. $\langle v, v\rangle \geq 0$ *and* $\langle v, v\rangle = 0$ *if and only if* $v = 0$ *(positivity axiom)*
2. $\langle v, v\rangle = 0$ *if and only if* $v = 0$ *(definiteness axiom)*
3. $\langle u + v, w\rangle = \langle u, v\rangle + \langle v, w\rangle$ *(additivity axiom)*
4. $\langle ku, v\rangle = k\langle u, v\rangle$ *(homogeneity axiom)*
5. $\langle u, v\rangle = \overline{\langle v, u\rangle}$ *(conjugate symmetry axiom)*

The **inner product space** is a vector space V along with inner product on V.

Definition 3. *If* $u = (u_1, u_2, \ldots, u_n)$ *and* $v = (v_1, v_2, \ldots, v_n)$ *are vectors in* $\mathbb{C}^n$*, then their* ***complex Euclidean inner product*** $u \cdot v$ *is defined as,*

$$u \cdot v = \bar{u_1}v_1 + \bar{u_2}v_2 + \ldots + \bar{u_n}v_n$$

where, $\bar{v_1}, \bar{v_2}, \ldots, \bar{v_n}$ *are complex conjugates of* $v_1, v_2, \ldots, v_n$*.*

Definition 4. *If* V *is a inner product space, then* ***norm*** *(or* ***length****) of a vector* $v \in V$ *is denoted by* $\|v\|$ *and it is defined as,*

$$\|v\| = \langle v, v\rangle^{\frac{1}{2}}$$

Definition 5. *When* $S = \{v_1, v_2, \ldots, v_n\}$ *be a set of vectors in inner product space, then* S *is called an* ***orthogonal****, if*

$$v_i \cdot v_j = 0 \quad \forall\, i \neq j$$

An orthogonal set in which each vector has norm 1 *is called* ***orthonormal****.*

Time evolution of quantum states is given by the unitary transformations. We understand in brief about the unitary operators.

Definition 6. *Let* A *be a matrix with complex entries and matrix* $\bar{A}$ *is obtained from* A *by replacing each entry of* A *by its complex conjugate. Then the matrix*

$$A^* = \bar{A}^t$$

is called ***conjugate transpose*** *of* A*. Here* $\bar{A}^t$ *is transpose of* $\bar{A}$*.*

Definition 7. *A square matrix* A *with complex entries is called* ***unitary*** *if,*

$$A^{-1} = A^*$$

The observables (measurable quantities) in quantum systems are described by Hermitian operators, which are defined as below.

Definition 8. *A square matrix* A *with complex entries is called* ***Hermitian****, if*

$$A = A^*$$

Mathematically equivalent formalisms for quantum systems were developed further by John von Neumann [22] into *Hilbert space formalism*. The theory of linear operators on Hilbert spaces, forms a very important part of quantum systems. The Hilbert space is thus a central mathematical structure for quantum systems, respresented as H_n, which in practice can be treated as an n-tuple complex space, $\mathbb{C}^n$. The H_n is called as a *state space* of an n-level quantum system. The dimension n of H_n is the number of perfectly distinguishable states of the system.

The states of n-level quantum system are described as vectors in n-dimensional Hilbert space H_n. A general state of n-level quantum system is described by a vector

$$\alpha_1|x_1\rangle + \ldots + \alpha_1|x_1\rangle \tag{2.2}$$

where $|x_1\rangle, \ldots, |x_n\rangle$ is a basis of H_n and term $\alpha_i \in \mathbb{C}$ is called as the *amplitude* of x_i, such that $|\alpha_1|^2 + \ldots + |\alpha_n|^2 = 1$. The basis $|x_1\rangle, \ldots, |x_n\rangle$ refers to an *observable* having certain value. The probability that the system is seen bearing property x_i is $|\alpha_i|^2$. The amplitude distribution as expressed in equation (2.2) is interpreted as a unit-length vector of Hilbert space.

The fundamental unit of classical information is a *bit* (or *binary digit*) while fundamental unit of quantum information processing systems is called the *qubit* (or *quantum bit*). The classical bit has two states, namely 0 and 1, two basis states of qubits are denoted as $|0\rangle$ and $|1\rangle$. The special notation '$|\rangle$', is referred as *Dirac notation* (or *ket*) and it is a standard notation for states in quantum systems. The Hilbert space structure can be well expressed in terms of *Dirac notations*. The state of a physical system described by a state-vector v is denoted as *ket*, $|x\rangle$, such that for a vector $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$,

$$|x\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Its corresponding *conjugate transpose*, known as Hermitian adjoint is written as *bra*, $\langle x|$ and it is denoted as

$$\langle x| = (x_1^*, \ldots, x_n^*)$$

Linear algebraic notions are instrumental in developing basic framework for quantum systems. We further discuss on the quantum mechanical structures that aid in the development of quantum cryptography.

2.2 Fundamentals of Quantum Systems

The theory of *quantum information* deals with storage, transmission and processing of information based on laws of quantum systems. In the quantum information processing, information is processed in the quantum states of a physical system. In classical information theory there is an underlying assumption that the state of the system in which information is encoded can be perfectly distinguished, it can be copied and it can be measured with an arbitrary precision. Laws of classical physics upheld approximations of system behavior in the classical information theory. Quantum information theory investigates how quantum physical properties of physical systems can be extended to explore limits of efficient storage and transmission of information [23]. We gather information about notions that contribute in building quantum system.

Quantum postulates are set of hypothesis which along with mathematical framework, described in section 2.1 enables making theoretical predictions and verify the experimental results for quantum systems.

The first postulate is referred to as description of state space of the system.

Postulate 1 Every physical system is represented by a Hilbert space, known as state space of the system. States are represented by linear operators in that space. For every physical system there is associated Hilbert space and vectors in this space represent pure states of the system.

In general, any state of the system would be a vector in the Hilbert space and an arbitrary vector can be expressed in terms of the basis vectors as *superpositions* of basis vectors.

The second postulate describe about evolution of the quantum system with the time.

Postulate 2 The time evolution of the closed quantum system is described by the unitary transformations. That is the transition of the state from $|\psi\rangle$ in time instance t_1 to some other state $|\psi'\rangle$ in time instance t_2, is given by unitary operator operating on the starting state.

$$|\psi'\rangle = U|\psi\rangle$$

,where U is some unitary operator.

The consequences of unitarity is that the time evolution of the quantum system is *invertible*.

The third postulate deals with the measurement on the quantum systems.

Postulate 3 This states that every physically measurable quantity can be represented by a Hermitian operator, where the values of the observable are eigenvalues of the operator corresponding to that observable.

Fourth postulate deals with the structure of the composite systems.

Postulate 4 If a composite system is composed of the subsystem Hilbert space, say H_1 and H_2, then the associated Hilbert space of the joint system is described by the *tensor product* of the subsystem spaces $H_1 \otimes H_2$.

We understand about tensor products in section 2.2.3. We now take a closer look at fundamental unit of quantum information processing.

2.2.1 Quantum Bits

Based on the underlying mathematical structures we formally define qubits as below.

Definition 9. ***Qubits*** *are described as two-dimensional complex vector space* $\mathbb{C}^2$*, known as* Hilbert space*, denoted as* H_2*. The states* $|0\rangle$ *and* $|1\rangle$ *constitute the computational basis,* $B = \{|0\rangle$ *and* $|1\rangle\}$ *and they are orthonormal to each other. For example,* $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ *and* $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$*, which is also known as coordinate representation of qubit.*

There are certain interesting comparative facts of properties of bits and the qubits. A classical bit has a definite value whereas qubit need not have a definite value until the moment it is read. A bit can only be 0 or 1, but qubit can be in a superposition of 0 and 1, simultaneously. A bit can be copied without affecting its value on the other hand for qubits an unknown state cannot be copied at all. Reading a qubit which is initially in a superposition may change the qubit, whereas a classical bit can be read without affecting its value. Reading one classical bit can not affect any other unread bit, but reading a qubit entangled with another qubit, does affect the other one.

The major difference to the classical bit is that qubit also allows states in between $|0\rangle$ and $|1\rangle$, which is known as *superpositions*. Superposition of the states $|0\rangle$ and $|1\rangle$ is expressed in the form

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.3}$$

where $\alpha, \beta \in \mathbb{C}$. Qubit state is a unit vector, that is its length is normalized to 1, then the scalars α and β satisfy the following equation.

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.4}$$

2.2.2 Photon Polarization

In terms of physical realization of qubits, electronic spin or polarized photons are such examples depicting this. The basis states $|0\rangle$ and $|1\rangle$ of a single qubit are regarded as reliably distinguishable states of the qubit, generally referred as horizontal and vertical polarization of the photon or spin-up ($|\uparrow\rangle$) and spin-down ($|\downarrow\rangle$) of an electron along particular axis. This is sometimes referred as *rectilinear basis*. While in case of a polarized photon, superposition of the basis states correspond to other polarizations. Another commonly used basis is *diagonal basis* which is denoted as $\{|\nearrow\rangle, |\searrow\rangle\}$ for notational convenience. It is given as,

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad |\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Yet another interesting basis used especially in *quantum cryptography* is known as *circular basis*, denoted as $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$. It is given as,

$$|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \quad \text{and} \quad |\circlearrowright\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

DOI: 10.18535/ijecs/v5i2.6

A unit three-dimensional sphere, known as Bloch sphere, depicted in figure 1 is a very useful representation of state of a single qubit. In figure 1, the north pole corresponds to the pure state $|0\rangle$ and the south pole corresponds to orthogonal pure state $|1\rangle$. All other points on the surface of the Bloch sphere correspond to the superposition states of the form $\alpha|0\rangle + \beta|1\rangle$, for all possible values of α and β where $\alpha, \beta \in \mathbb{C}$, such that $|\alpha|^2 + |\beta|^2 = 1$.

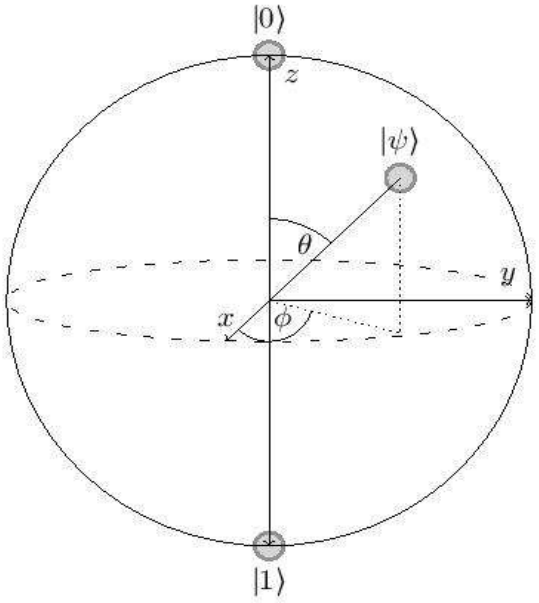

Figure 1: Bloch sphere representation of a qubit

In figure 1, the states $|0\rangle$ and $|1\rangle$ correspond to North and south pole of the Bloch sphere, respectively. Axis that passes through these points is the z-axis. By reading the value of a qubit is then measuring the alignment of its spin w.r.t. z-axis. The *spin-up* aligned particle is in $|0\rangle$ state and if particle is *spin-down* aligned then it is in $|1\rangle$ state. When a single qubit $\alpha|0\rangle + \beta|1\rangle$ is observed (read or measured), w.r.t. to some axis, its value depends on the values of α and β, commonly used axis being z-axis. Measurement of qubit w.r.t. the axis is called a measurement *in the computational basis*, since the resultant value obtained is $|0\rangle$ or $|1\rangle$. The outcome is not certain but depends upon values of α and β. Measuring the bit value of $\alpha|0\rangle + \beta|1\rangle$ in the computational basis yields $|0\rangle$ with $|\alpha|^2$ probability and $|1\rangle$ with $|\beta|^2$ probability.

The standard polarization obtained, are listed as follows.

1. Left circular polarization, $|\circlearrowleft\rangle$
2. Right circular polarization, $|\circlearrowright\rangle$
3. Horizontal polarization, $|\leftrightarrow\rangle = \frac{i}{\sqrt{2}}|\circlearrowleft\rangle - |\circlearrowright\rangle$
4. Vertical polarization, $|\updownarrow\rangle = \frac{1}{\sqrt{2}}|\circlearrowleft\rangle + |\circlearrowright\rangle$
5. Diagonal (45°) polarization, $|\nearrow\rangle = \frac{1+i}{2}|\circlearrowleft\rangle + \frac{1-i}{2}|\circlearrowright\rangle$
6. Diagonal (135°) polarization, $|\nwarrow\rangle = \frac{1-i}{2}|\circlearrowleft\rangle + \frac{1+i}{2}|\circlearrowright\rangle$

Photons are polarized based on their oscillating electric field and that becomes a base for encoding bit values for photons. In this section we described that photons are either in rectilinear

polarization or they are diagonally polarized, which in turn is derived from superposition of spin polarizations, $|\circlearrowleft\rangle$ and $|\circlearrowright\rangle$. The linear and diagonal polarizations are also sometimes denoted as ⊞ and ⊠. There are some conventions followed in encoding photons based on polarization. In ⊞ polarized light, either vertically polarized photons ($|\updownarrow\rangle$) correspond to 0 and horizontally polarized photons ($|\leftrightarrow\rangle$) correspond to 1 or in ⊠ polarized light, 45° ($|\nearrow\rangle$) polarized photons correspond to 0 and 135° ($|\nwarrow\rangle$) polarized photons correspond to 1.

2.2.3 Quantum Entanglement

The *Entanglement* is a very powerful phenomenon that distinguishes quantum information systems from that of classical information systems. Entanglement implies correlation between different parts of a quantum system. The system is in entangled state when the whole system cannot be expressed as a direct product of the states for its parts. For entangled state when action is performed on one subsystem, it may have effect on another sub-system even though other subsystem is not acted upon directly. It is also observed that this phenomenon persists even if the subsystem states are separated apart by some distance. It is essentially due to the phenomenon of entanglement, that the quantum algorithms exhibit exponential speedup over their classical counterparts.

Notion of *tensor product* (or *Kronecker product* or *direct product*) of qubit states is vital in understanding multiple qubits quantum states.

Definition 10. *Consider we have two quantum states as,* $|\psi\rangle = \sum_{i=0}^{2^m-1} a_i|i\rangle$, *be an m-qubit pure state and* $|\varphi\rangle = \sum_{j=0}^{2^n-1} b_j|j\rangle$, *be n-qubit pure state. The compound quantum state is formed by taking a* ***tensor product*** *(or* Kronecker product *or* direct product*),* $|\psi\rangle \otimes |\varphi\rangle$, *as follows.*

$$|\psi\rangle \otimes |\varphi\rangle = \sum_{i=0}^{2^m-1} a_i|i\rangle \otimes \sum_{j=0}^{2^n-1} b_j|j\rangle$$

Let there be two independent quantum systems with Hilbert spaces H_m and H_n, of dimensions m and n, respectively. The elements of H_m can then be expressed as $|\psi_m\rangle = a_0|0\rangle_m, +a_1|1\rangle_m + \ldots + a_{m-1}|m-1\rangle_m$ and H_n can be then expressed as $|\psi_n\rangle = b_0|0\rangle_n, +b_1|1\rangle_n + \ldots + b_{n-1}|n-1\rangle_n$. Where $a_0, a_1, \ldots, a_m$ and $b_0, b_1, \ldots, b_n$, are some complex numbers. Hilbert space for the composite system is then given as tensor product, $H = H_m \otimes H_n$. If a pure (mixed) state $|\psi_{mn}\rangle$, of a composite quantum system, defined on a Hilbert space $H_m \otimes H_n$ can be expressed as,

$$|\psi_{mn}\rangle = |\psi_m\rangle \otimes |\psi_n\rangle$$

then it is said to be a **separable state**. If a state $|\psi_{mn}\rangle$, of a composite quantum system, defined on a Hilbert space $H_m \otimes H_n$, is not a separable state then it is **entangled state**.

The 2-qubit entangled states, that are obtained from the computational basis are known as **Bell State** after the name of scientist Bell or **EPR pair** (or *EPR states*), after the name of researchers Einstein, Podolsky and Rosen, due to their famous paper [24]. The state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, is an example of a entangled state.

2.2.4 No-cloning Theorem

Notion of No-cloning [8] highlights limitation of quantum systems and it states that it is not possible to make a copy of unknown quantum state. But this limitation works advantageous in certain situations, like detecting event of eavesdropping in quantum cryptography. No-cloning theorem is stated as below, for its detailed proof we refer to [25].

Theorem 1. ***No-Cloning Theorem*** *For an n-level quantum system having state space denoted by* H_n, *being an n-dimensional complex vector space, then the* no-cloning theorem *states that for* $n > 1$, *there is no quantum copy machine.*

DOI: 10.18535/ijecs/v5i2.6

3 Quantum Cryptography

Pioneering effort of Wiesner presented in his paper [26] where he proposed to implant quantum serial number along with a classical serial number, on banknotes, could not receive much attention, until his concepts of using quantum mechanics in making unforgeable banknotes, were applied by Bennett and Brassard in the construction of secure quantum communication. This construction was carried according to laws of nature, in some of then new concept in public key cryptography [27, 28]. Thus born a first paper in Quantum Cryptography [29], providing an impetus to explore the field of quantum cryptography.

The quantum states assume a key role of information carriers, in quantum cryptography. In its very essential form quantum cryptography does not refer to creation of quantum cryptosystem but it offers the most secure way of establishing random secret key. As we have seen earlier that the One-time Pad is a perfectly secure cryptosystem, if the key distribution problem is effectively addressed and quantum cryptography exactly offers to address this critical requirement. A method of *quantum key distribution* claims to provide safest way of exchanging the keys between the authorized parties involved in the communication. In particular, it is about sharing random classical bit strings using quantum states. The security of the quantum cryptography lies in the fact that nonorthogonal quantum states, in terms of photon polarization, in which the bit strings are prepared, are indistinguishable from each other and that any attempt to measure these states induces irreversible perturbations in the system.

There are following few requirements to enable well encrypted and secure communication in any form of cryptography. The legitimate users are authenticated, there is a secure transfer of keying material between authentic users and further, during communication any attempt of interference is discovered successfully. Quantum cryptography is to fulfill these basic requirements. Precisely keeping these criteria in view, Quantum Key Distribution (QKD) technique is developed which facilitates agreement of shared random sequence of bits (viewed as keying material) and leaves very low probability of twisting these bits, by enabling early detection of such intrusion and alerting legitimate users of it. Once the keys are established they can be used to augment the perfectly secure classical cryptosystem like, *One Time Pad*. A practical advantage of combining it with QKD, is that the communicating parties need not meet physically to refresh their keying material, which was one of the major shortfall of One Time Pad cryptosystem.

This quantum distribution scheme is based on transmission of single microscopic particle of photon and value of a classical bit encoded by the polarization of a photon [13, 16, 15].

3.1 Quantum Key Distribution

There are various ways of implementing QKD and it depends on the behavior of the quantum systems. Although these different ways do not differ too much and they achieve similar ultimate goal. On broader terms, in one of the approach the classical bits are encoded into the set of non-orthogonal quantum states. In the user perspective, the single quantum states are prepared by Alice and measured by Bob, to exchange the random bits. This way of implementation is therefore referred as "prepare-and-measure" scheme. Another approach uses quantum phenomenon of entanglement. The entanglement ensures that the simultaneous measurement of states by Alice and Bob will lead to perfectly correlated secret bits. Any attempt of intrusion destroys perfect entanglement.

In "prepare-and-measure" approach of QKD, Alice generates a stream of perfectly random bits from which Alice and Bob distill out a matching private key. Once the stream of random bits are generated they are encoded into the quantum states in the stream of photons. Alice transmits vertically, horizontally and diagonally polarized photons to Bob. This encoding gurantees that any kind of attempt made to measure the encoding, without the knowledge of encoding used, will add up to the quantum bit error rate (QBER), thus revealing attempt of intrusion. If QBER is very low and the tests reveal there is no intrusion attempt succeeded, then communication channel is assumed to be secure while the key distribution and further, the random bits remaining after protocol has ended, used as cryptographic keys. But at any instance if the intrusion is detected

then the key exchange is discarded and exchange for fresh key distribution is initiated.

Security measures employed by quantum cryptography is much stronger than one present in classical cryptography. The security of quantum cryptography lies in the indistinguishability of nonorthogonal quantum states and the irreversible disturbance arise due to the measurement of these states by Eve, in a complete absence of knowledge of the encoding states. This is an underline security measure kept in view while developing various QKD protocols. Some of the QKD techniques are listed below.

1. BB84 protocol developed by Bennett and Brassaed, based on two non-commuting observables [13].
2. B92 protocol developed by Bennett based in two non-orthogonal states [16].
3. "Six-state" protocol (extending BB84 protocol) developed by Bruss [17, 18].
4. "Entanglement-based" protocol by Ekert [19].
5. "Orbital Angular Momentum" based protocol by Spefalieri [30].
6. Protocols based on coherent states [31, 32].

3.1.1 The BB84 QKD Protocol

The BB84 protocol uses four nonorthogonal quantum states belonging to two conjugate bases and two states in each basis are orthogonal [13]. These four states as we discussed are, $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|\nearrow\rangle$ and $|\nwarrow\rangle$. This is much similar to the selection of bases made by Wiesner in preparing quantum serial numbers for unforgeable banknotes. These basis states are pairs of orthogonal quantum states, with rectilinear or diagonal polarization of photons. Thus the quantum states of one of the pairs are *non-orthogonal* to the ones of the other pair.

Alice and Bob are assumed to be connected via quantum channel, where presence of Eavesdropper is not denied. In addition to that they have classical channel where Alice and Bob establish mutual trust with the help of shared secret. In this communication channel access is denied to any unauthorized party (like Eve) who has not established mutual trust.

BB84 protocol works as follows.

1. *Preparation Phase.* Alice prepares truly random qubits encoded in one of four states and sends them to Bob via quantum channel. Alice and Bob agree on the encoding strategy that if Alice is sending 0 to Bob then she transmits either $|\updownarrow\rangle$ or $|\nwarrow\rangle$ with equal probability and if she is sending 1 then she transmits either $|\leftrightarrow\rangle$ or $|\nearrow\rangle$ with equal probability.
2. *Measurement Phase.* For each qubit that Bob receives from Alice, he chooses at random either rectilinear or diagonal bases and measures the qubit with respect to that basis. If Basis chosen by Bob matches to one prepared by Alice to encode the qubit, then Bob is able to determine correct polarization state of the photon. This assist him in ascertaining encoding strategy used by Alice and then further, it helps him determining if Alice has sent a 0 or 1. However, if their basis do not match then Bob would have only 50% chance of determining correct value of qubit sent by Alice. But at this stage Bob do not have idea which bit values measured are correct and which one not correct.
3. *Sifting Phase.* In order to determine the correct bit values, upon completion of measurement Bob communicates Alice the basis in which he measured photons sent to him by Alice. It's only the basis are communicated here and not actual values. This communication can take place on authenticated classical communication channel. Alice conveys Bob where basis of preparation of qubits matching to the basis of measurement used by Bob. They keep those bits where the basis selection coincide. Thus now they have matching sequence of randomly generated bits. These bits form what is called, *sifted bits*.

4. *Error Estimation Phase.* Until this point Alice and Bob do not have knowledge about possible intrusion by an Eavesdropper. To ascertain the presence of Eve, Alice and Bob chooses to sacrifice a subset of sifted keys. If Eve is listening to this, she would prepare basis to measure values of those bits. Just like Bob, Eve would only succeed with $\frac{1}{2}$ probability. But in doing so she would have disturbed the state of the photons, while re-transmitting those photons to Bob. In a consequence to this Bob would measure wrong polarization with $\frac{1}{2}$ probability. Thus for each bit in sifted key there is $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$ probability that Eve is detected. Thus with a small portion of sifted key bits, Alice and Bob would be able to establish presence of Eve.

5. *Establishing Secret Key.* With the result of above steps, Alice and Bob form a joint secret key from the remaining bits by performing (classical) error correction and privacy amplification.

We list some of subprocesses involved in BB84 protocol that ensure successful distribution of shared secret key.

1. Sifting. It is a process whereby Alice and Bob winnow away all the obvious failed qubits from a series of pulses; as a result leaving only those symbols Bob received and those Bob has calculated using same basis as Alice's.

2. Error Estimation. This process allows Alice and Bob to determine all the error bits among their shared, sifted bits and correct them so that Alice and Bob share the same sequence of error corrected bit. This allows Alice and Bob to measure QBER of ongoing communication, which becomes vital input for the further step of privacy amplification.

3. Privacy Amplification. It is a process that reduces Eve's partial knowledge about Alice and Bob's key. This process uses Alice and Bob's key to produce a new, shorter key, in such a way that Eve has only negligible information about the new key.

4. Authentication. It allows Alice and Bob to guard against man-in-the-middle attacks, ensuring Alice that she is communicating with Bob (and not with Eve) and vice versa.

Figure 2 gives schematic representation of basic steps involved in QKD to share secret key. Reading it from bottom to top, these steps play a vital role in successful implementation of QKD [33, 34].

3.1.2 BB84 QKD when there is Eavesdropping

Attack that Eve carry on the communication between Alice and Bob is generally termed as *measure and resend*. We have discussed previously that due to No-cloning theorem it is not possible to copy any arbitrary quantum state and because of this reason Eve would not be able to make copy of the states being transmitted by Alice. Eve has to then measure the polarization orientation of the photons emancipating form Alice and retransmit them to Bob to cover her tracking. In order to disguise, Eve adopts same strategy as Bob do. She intercepts the photons underway from Alice and set her own measure of polarization. Eve has no idea about the basis in which Alice has prepared those photon, since Alice announces this information only after Bob has received all the photons. Eve can only guess about the polarizer orientation and make her measurement. If Eve is making measurement on say $2n$ number of photon then for half of them that is for n cases she may succeed in her guesses and for other half result would be in random and not in sync with Alice's preparation. But to hide her attempt of eavesdropping, Eve has to resend those photons to Bob and she does not know the basis in which Alice has prepared them, so Eve send those photons in a basis that she has used to measure photons coming from Alice. In this case there are only n of newly created qubits that are in sync with Alice's measurement. After Bob receives qubits, that are now sent by Eve, Bob makes his measurements on them. Alice and Bob carry out the *sifting phase* described in the execution of BB84 protocol above. At this phase only in $^{n}/_{2}$ cases

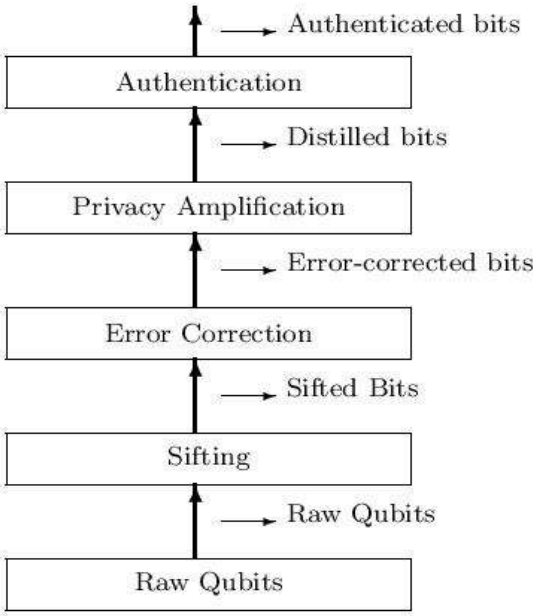

Figure 2: Stages of QKD

Bob's measurement would match to that of Alice's and Eve's basis of measurement would disagree there. Bob's measurement for sifted keys will be wrong for $^{n}/_{4}$ number of cases, that is there are chances of 25% error here. In the *error estimation phase* of the protocol if Alice and Bob identify such a high error rate they abort the protocol. The attempt of eavesdropping is established at this stage. This intrusion scenario reveals that more Eve tries to make an attempt to measure quantum states, more errors she would infuse, thus making her attempt of eavesdropping known to the authorized parties in the communication.

3.2 Various Protocols based on Quantum Systems

Advances in the study QKD prompted development of several protocols that are based on Quantum System. We take a look at some of them.

3.2.1 B92 Protocol

In 1992 Bennett [16] proposed this scheme based on observation that if two quantum states are incompatible, then two states are also sufficient and cannot be recognized unambiguously without adding irrevocable disturbance thus maintaining secrecy in quantum cryptography. Major difference with BB84 however is that B92 lets Bob learn bit he get, without further conversation with Alice. Having only two quantum states, this scheme is easier to implement yet certain experimental set up seem be difficult to comprehend.

3.2.2 Six State Protocol

This protocol [18, 17] is based on a central theme of having third basis, letting qubits to have three mutually unbiased basis, which is apparently maximum basis per qubit, offered. Compared to BB84, QBER is 33% as against 25% in BB84, if Eve attempts to measure every photon [35].

3.2.3 SARG04 Protocol

This protocol uses same quantum states as in BB84 but with a different encoding information [36]. While this does not give any information to Eve, yet it gives Bob full information about a classical bit, if he measures bit in proper basis.

3.2.4 Protocol based on Quantum Entanglement

The Ekert E91 Protocol was proposed by Ekert in his paper [19]. This protocol uses a quantum phenomena of entanglement to produce secret key. The entangled quantum states are distributed between Alice and Bob. It build upon the fact that measurement of both qubits in any basis gives correlated results. In this entangled state every photon is associated with one more synchronized photon, that are created and measured together.

4 Conclusion

With the underlying quantum structures, Quantum cryptography is perceived as a fitting solution towards the development of unconditionally secure cryptosystem. Quantum cryptographic techniques are fundamentally strong and they have very high rate of intrusion detection. Due to strong foundations of laws of quantum mechanics, attempts of eavesdropping is established and that the intruder gets no knowledge of the keying material. With inherent advantages, QKD can set its foothold in the field network security and it can well be combined with the internet technology, to provide secure communication for practical purposes.

Over the last decade there have been substantial advances in the field of quantum cryptography, yet there are some limitation for quantum cryptography becoming widely used key distribution techniques for personal, enterprise, academic and research purposes. These challenges include developing hardware resources to enhance rapid delivery of keying material and carry it to the longer distance.

The advances in computer processing and threat factor present for the classical cryptosystems that are widely used, will be a driving factor for more research and development in the field of quantum cryptography. Overcoming certain technological challenges, possibilities of improvements into quantum infrastructure and ability of these methods to combine well with the classical methods make quantum cryptography as a promising alternative to be an unconditionally secure cryptographic technique.

References

[1] Vernam G.S. (1926), J. AIEE 45, 109.

[2] Simmons G. J. (1992), *Contemporary Cryptography*, IEEE Press, Piscataway.

[3] Pfleeger C. P., Pfleeger S. L. (2003), *Security in Computing*, Upper Saddle River, NJ: Prentice Hall.

[4] Nguyen T.M.T., Sfaxi M.A., Ghernaouti-Helie S., *Integration of quantum cryptography in 802.11 networks*, Proc. 1st Int. conf. on Availability, Reliability and Security, (2006).

[5] Hrg, D., Budin, L., Golub, M. (2004), *Quantum cryptography and security of information systems*, IEEE Proceedings of the 15th Conference on Information and Intelligent System, pp. 63-70.

[6] Papanikolaou N. (2005), *An introduction to quantum cryptography*, ACM Crossroads Magazine, Vol.11 No.3, pp. 1-16.

[7] Teja V., Banerjee P., Sharma N.N., Mittal R.K. (2007), *Quantum cryptography: State-of-art, challenges and future perspectives*, 7th IEEE Conference on Nanotechnology, IEEE-NANO 2007, pp.1296-1301.

[8] Wootters W. K., Zurek W. H. (1982), *A single quantum cannot be cloned*, Nature (London) 299, pp. 802-803.

[9] Bennett C. H.; Brassard G. (1987), *Quantum public key distribution reinvented*, SIGACT News 18, pp.51-53.

[10] Bennett C. H.; DiVincenzo D.P. (2000), *Quantum information and computation*, Nature 404, pp.247-255.

[11] Nielsen M., Chuang I., *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

[12] Singh S. (1999), *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, (Fourth Estate, London).

[13] Bennett C.H., Brassard G. (1984), *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc. Of IEEE Int. Conf. On Comput. Sys. And Sign. Proces., Banglore, India, pp.175-179.

[14] Shor P.W., Preslill J. (2000), *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett 85, pp.441-444.

[15] Bennett C.H.; Bessette F.; Brassard G. Et al (1992), *Experimental Quantum Cryptography*, J. Cryptology vol. 5, pp.3-28.

[16] Bennett C.H. (1992), *Quantum Cryptography Using any Two Nonorthogonal States*, Phys. Rev. Lett. V.68, pp.3121.

[17] Bechmann-Pasquinucci H.; Gisin N. (1999), *Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography*, Physical Review A (Atomic, Molecular, and Optical Physics), Volume 59, Issue 6, pp.4238-4248.

[18] Bruss D. (1998), *Optimal eavesdropping in quantum cryptography with six state*, Phys. Rev. Lett., V.81, pp.3018-3021.

[19] Ekert A.K. (1991), *Quantum cryptography based on Bellś theorem*, Physical Review Letters, Vol. 67, No. 6. pp. 661-663.

[20] Gisin N., Ribordy G., Tittel W., Zbinden H. (2002), *Quantum cryptography*, Reviews of Modern Physics 74(1): pp.145-175.

[21] Strang G. (February 2009), Introduction to Linear Algebra (4th ed.), Wellesley-Cambridge Press, ISBN 978-0-98-02327-14.

[22] John von Neumann, *Mathematische Grundlagen der Quantenmechanik*, Springer (1932).

[23] Benatti F., Fannes M., Floreanini R., Petritis D., Quantum Information, Computation and Cryptography, Lecture notes in Physics, vol 808, An Introductory Survey of Theory, Technology and Experiments, Springer.

[24] Albert Einstein, Boris Podolsky, Nathan Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Physical Review 47, 777-780 (1935).

[25] Hirvensalo M., *Quantum Computing*, Natural Computing Series, Springer, 2nd edition (2003).

[26] Wiesner S. (1983), *Conjugate coding*, written circa 1970 and belatedly published in Sigact News 15(1), pp. 78-88.

[27] Diffie W., Hellman M.E. (1976), *New directions in cryptography*, IEEE Transactions on Information Theory 22(6), pp. 644-654.

[28] Brassard, G. (2005), *Brief history of quantum cryptography: a personal perspective*, IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, pp.19-23.

[29] Bennett C.H., Brassard G., Breidbart S., Wiesner S. (1982), *Quantum cryptography, or Unforgeable subway tokens*, Advances in Cryptology: Proceedings of Crypto 82, Santa Barbara, Plenum Press, pp. 267-275.

[30] Spedalieri F. M., *Quantum Key Distribution Without Reference Frame Alignment: Exploiting Photon Orbital Angular Momentum*, Optics Communications, Volume 260, Issue 1 (2006) pp. 340346.

[31] F. Grosshans and P. Grangier, *Continuous Variable Quantum Cryptography Using Coherent States*, Phys. Rev. Lett., Volume 88 (2002) 057902.

[32] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, *Quantum Key Distribution using Gaussian-modulated Coherent States*, Nature, Volume 421 (2003) pp. 238241.

[33] Sharbaf, M. S. (2011), *Quantum cryptography: An emerging technology in network security*, IEEE International Conference on Technologies for Homeland Security (HST), pp.13-19.

[34] Elliott C., Pearson D., Troxel G. (2003), *Quantum cryptography in practice*, In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '03). ACM, New York, NY, USA, pp. 227-238.

[35] Kurochkin V. L. (2011), *Protocols for quantum cryptography*, International Conference and Seminar of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM), pp.114-115.

[36] Scarani V., Acin A., Ribordy G., Gisin N. (2004), *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*, Phys. Rev. Lett., Vol 92, 057901.