https://doi.org/

Quantum Computing and Quantum Key Distribution: A Short Review for Beginners

Sushmita Sarkar[1] and Sourav Bera[2]

[1]Department of Mathematics, NIT Jamshedpur, Jamshedpur, India-831014
[2]Information Security Research Center, National Sun Yat-Sen University, Kaohsiung, Taiwan-80424
Corresponding author: berasourav561@gmail.com

Abstract. Quantum Key Distribution (QKD) is a secure way of communication, leveraging the fundamental properties of quantum computing. QKD enables two parties to generate and share a secret key with unconditional security. This manuscript explains how secure communication has changed over time with the use of quantum theory. In the past forty years, quantum mechanics has brought big changes to this area. Starting with the BB84 protocol, the first model for secure communication in 1984, this field has made a lot of progress.

QKD offers a new way to look at secure communication. Unlike classical cryptography, QKD ensures security through the basic principles of quantum physics rather than computational hardness.

QKD uses phenomena such as superpositions and entanglement to transmit keys securely. The no-cloning theorem ensures that quantum information cannot be copied without detection. Any interception of quantum bits alters their state, alerting the communicating parties. QKD systems have been experimentally implemented over fibre-optic cables and free-space links. However, challenges remain in scaling, error correction, and hardware reliability.

Key words: Quantum cryptography; Operator; Measurement; Coherence; Key distribution
Received: 2 January 2026 **Revised:** 25 January 2026 **Accepted:** 27 January 2026

Contents

Chapter 1

Cryptography in Classical and Quantum Domain

Cryptography is the art of science for a secure communication between legitimate parties through an insecure channel, such that only the legitimate parties can get the information. An unintended person cannot obtain any information from this process. This is the basic concept for enhancing interest in studying cryptography.

There are many useful cryptographic tools to protect our data in cloud storage, communication, and other fields in daily life, like online shopping, messaging apps (like WhatsApp), password protection, online money transactions, etc [2–4].

The encryption procedure of a cryptographic scheme is a five-tuple system $(\mathcal{P}, \mathcal{C}, \mathcal{E}, \mathcal{D}, \mathcal{K})$. The terms are significant as follows:

$\mathcal{P}$ is the space of all plaintexts of the encryption procedure, which is the information or message that is wished to transmit through a public channel.

$\mathcal{C}$ is the space of ciphertexts that is the encrypted version of plaintexts $P \in \mathcal{P}$.

$\mathcal{E}$ symbolizes the space of the encryption process, where a plaintext $P \in \mathcal{P}$ is transformed into a ciphertext $C \in \mathcal{C}$

$\mathcal{D}$ symbolizes the space of the decryption process, where a ciphertext $C \in \mathcal{C}$ is returned to that plaintext $P \in \mathcal{P}$.

$\mathcal{K}$ is the key space of the encryption procedure, where a key $K \in \mathcal{K}$ is used to obtain the ciphertext C from the plaintext P.

In this chapter, we discuss cryptographic schemes in two different domains: the Classical domain and the Quantum domain. The study of cryptographic schemes in the classical domain is called the study of classical cryptography, and the study of cryptographic schemes in the quantum domain is called the study of quantum cryptography.

1.1. Classical Cryptography (CC)

The security of cryptographic schemes in the classical domain are based on mathematically hard problems like prime factorization of large integers, subset sum problems, discrete-log problems, etc. Some cryptographic schemes, like Substitution cipher, Stream cipher, Block cipher, etc. are examples of symmetric key cryptosystems which means that the encryption and decryption procedure of these types of ciphers utilize the same key. Whereas, RSA, ElGamal, and Knapsack are some of the asymmetric key cryptosystems, where encryption and decryption procedure utilize two different keys (secret key and public key). The encryption procedure is done by a secret key by the sender, and decryption procedure is done by the corresponding public key by receiver [1].

With the immense growth of research in quantum computing, many cryptographic schemes in classical field are vulnerable due to Shor's algorithm [5]. Therefore, for secure computation and communication, the study is moving toward investigating schemes using the fundamental properties of quantum computation and quantum information.

1.2. Quantum Cryptography (QC)

QC is the study of cryptographic schemes that are designed utilizing the basic properties of quantum computing [6]. The study of quantum computation and quantum communication is a revolutionary step to secure computation and communication against quantum computers. Quantum cryptography provides cryptographic protocols that are long-term secure. In this paper, we discuss secure key distribution procedures in the quantum domain. This area of

research is known as QKD. It is a cryptographic protocol for securely sharing encryption keys with the legitimate parties using basic fundamental properties of quantum computing.

1.2.1 Quantum States and their Properties

Like as a bit (0 or 1) is the basic key of information for classical computers, the basic key of the same in quantum computers is a quantum state. A quantum state in quantum cryptography is called a *Qubit.* Mathematically, a quantum state is expressed by a column vector in Hilbert space ($\mathcal{H}$), and it is symbolized by ket ($|\rangle$) symbol. Thus, the basis of qubits in a 2-dimensional $\mathcal{H}$ space is defined by the two quantum states $|0\rangle$ and $|1\rangle$, where $|0\rangle = [1,0]^t$ and $|1\rangle = [0,1]^t$ ($[a,b]^t$ is the transpose of the row vector $[a,b]$).

A superposition state of an arbitrary quantum state $|\psi\rangle \in \mathcal{H}$ is expressed as follows:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{where } \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1. \tag{1}$$

An arbitrary qubit $|\psi\rangle$ that is in a superposition state, can exist in both of the states $|0\rangle$ and $|1\rangle$. However, after measurement in basis $\{|0\rangle, |1\rangle\}$, the qubit $|\psi\rangle$ projects in one of the states $|0\rangle$ or $|1\rangle$. In the above expression, $|\alpha|^2$ provides the probability of finding the arbitrary quantum state $|\psi\rangle$ in $|0\rangle$ state, and $|\beta|^2$ gives probability of obtaining $|\psi\rangle$ in $|1\rangle$ state.

Physically, in $\mathcal{H}$, a state vector satisfying the condition 1 is a normalized quantum state. The modulus of the coefficient of basis quantum states is calculated as follows:

$$|\alpha|^2 = \alpha\alpha^*$$
$$|\beta|^2 = \beta\beta^*$$

where α^* and β^* are complex conjugate of α and β respectively.

Chapter 2

Operators and Matrix Representations

An operator between two Hilbert spaces U and V is defined by a function $f : U \longrightarrow V$, and a linear operator is an operator that is linear in its inputs to U. It is easy to observe the properties of a linear operator through the matrix representation of the operator. Some basic linear operators are defined as follows:

Identity Operator: An identity operator is the kind of function that maps an element $u \in U$ to itself, and it is denoted by $\hat{I}$. Obviously, in this case, $U \subseteq V$. Mathematically, the identity operator is expressed by $\hat{I}(u) = (u)$.

Zero Operator: A zero operator is the kind of function that maps each $u \in U$ to zero element (0_V) of V, and it is denoted by $\hat{0}$. Mathematically, the zero operator is expressed by $\hat{0}(u) = 0_V$.

2.1. The Pauli Operator

In quantum computation, Pauli operators are four linear operators which are the fundamental components of linear operators. These operators are defined and denoted as follows:

Let $\mathbb{C}^2$ be a 2-dimensional $\mathcal{H}$ over the set of complex numbers $\mathbb{C}$. $\{|0\rangle, |1\rangle\}$ be the basis of $\mathbb{C}^2$ to execute quantum operations on a qubit. Then, the Pauli operators [7] $\sigma_I, \sigma_x, \sigma_z,$ and σ_y are defined as

$$\begin{aligned}
\sigma_I |0\rangle &= |0\rangle, & \sigma_I |1\rangle &= |1\rangle; \\
\sigma_x |0\rangle &= |1\rangle, & \sigma_x |1\rangle &= |0\rangle; \\
\sigma_z |0\rangle &= |0\rangle, & \sigma_z |1\rangle &= -|1\rangle; \\
\sigma_y |0\rangle &= i|1\rangle, & \sigma_y |1\rangle &= -i|0\rangle.
\end{aligned}$$

The matrix representation of these operators is as follows:

$$\sigma_I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

For an arbitrary quantum stat $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, satisfying the condition of the Born rule, the operators effect in the following:

$$\sigma_I |\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \sigma_x |\psi\rangle = \alpha|1\rangle + \beta|0\rangle, \quad \sigma_z |\psi\rangle = \alpha|0\rangle - \beta|1\rangle,$$
$$\text{and } \sigma_y |\psi\rangle = i\sigma_x\sigma_z = i(\alpha|1\rangle - \beta|0\rangle).$$

2.2. Adjoint Operator

The adjoint of a linear operator σ is denoted by $\sigma^\dagger$, and is defined by the following relation:

$$\langle\alpha| \sigma^\dagger |\beta\rangle = \langle\beta| \sigma |\alpha\rangle^*.$$

That is, the adjoint of an operator is obtained by taking the conjugate transpose of the coefficients in the expression of the operator, changing ket to bra, bra to ket, and finally reversing the order of the operators ket and bra.

2.3. Unitary Operator

A linear operator σ is called a unitary operator if it follows the given condition:

$$\sigma\sigma^{\dagger} = \sigma^{\dagger}\sigma = \sigma_I,$$

where $\sigma^{\dagger}$ is an adjoint operator of σ, i.e., the complex conjugate transpose of the matrix representation of the operator σ, and σ_I is the identity operator. In this case, $\sigma^{\dagger}$ is the inverse of σ by definition of an inverse operator.

2.4. Hermitian Operator

A linear operator σ is said to be a hermitian operator if it satisfies the following condition:

$$\sigma^{\dagger} = \sigma$$

That is, a hermitian operator is its own conjugate.

2.5. Normal Operator

A linear operator σ is said to be a normal operator if it satisfies the following condition:

$$\sigma\sigma^{\dagger} = \sigma^{\dagger}\sigma$$

That is, a normal operator is an operator that satisfies the commutative property with its adjoint operator.

2.6. Projection Operator

Let $|\psi\rangle$ be any arbitrary quantum state. Then, a projection operator can be formulated by the outer product of $|\psi\rangle$. This means that for a given qubit $|\psi\rangle$, the projection operator is defined by $P = |\psi\rangle \langle\psi|$.

2.7. Outer Product

The notation '$\langle|$' is called bra notation and is defined as the transpose of ket $|\rangle$. The outer product is formed by matrix multiplying of a ket state and a bra state of a qubit. Moreover, for any arbitrary qubits $|\psi\rangle, |\phi\rangle, |x\rangle$, the following holds:

$$(|\psi\rangle \langle\phi|) |x\rangle = |\psi\rangle \langle\phi|x\rangle$$

2.7.1 Metric Representation of the Outer Product

Let $|\psi\rangle$ and $|\phi\rangle$ be two qubits. Suppose

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} and \quad |\phi\rangle = \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}$$

Then outer product of these qubits is formed as follows:

$$|\psi\rangle \langle\phi| = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \begin{pmatrix} \alpha_2^* & \beta_2^* \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2^* & \alpha_1\beta_2^* \\ \beta_1\alpha_2^* & \beta_1\beta_2^* \end{pmatrix}$$

$$|\phi\rangle\langle\psi| = \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}\begin{pmatrix}\alpha_1^* & \beta_1^*\end{pmatrix} = \begin{pmatrix}\alpha_2\alpha_1^* & \alpha_2\beta_1^*\\ \beta_2\alpha_1^* & \beta_2\beta_1^*\end{pmatrix}$$

2.8. Spectral Decomposition

Spectral Decomposition Theorem: In a vector space V, if an operator A is normal and can be expressed as a diagonal matrix with respect to some basis $\{u_i\}_{i=1}^n$ of V, then it is said that the operator A satisfies the spectral decomposition theorem [8]. The operator A can also be represented as follows:

$$A = \sum_{i=1}^{n} \alpha_i |u_i\rangle\langle u_i|, \quad \text{where } \alpha_i \text{ are eigenvalues of} A.$$

It can be evaluated that the spectral decomposition of Pauli-X operator σ_x and Pauli-Z operator σ_z are given below:

$$\sigma_x = |+\rangle\langle+| - |-\rangle\langle-|, \quad \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|,$$

where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

2.9. The Heisenberg Uncertainty Principle

In 1927, the uncertainty principle [9] was introduced by Werner Heisenberg. It states that it is not possible to accurately measure or calculate both the momentum and the position of a particle at the same time. In particular, the more precisely a particle's position is known, the less accurately its momentum can be inferred from the initial conditions, and conversely.

Let Δx denote the uncertainty in the position of a particle and Δp denote the uncertainty in the momentum of the same particle, then Δx and Δp satisfy the following:

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

where $\hbar$ is the reduced Planck's constant.

Since every dynamical variable is an observable in quantum theory, and the Heisenberg uncertainty principle affects dynamical variables, this principle plays a significant role in quantum information and quantum computation. If σ_A and σ_B are any two operators of quantum computation, their uncertainties $\Delta\sigma_A, \Delta\sigma_B$ satisfy the following:

$$\Delta\sigma_B \Delta\sigma_A \geq \frac{1}{2}|\langle[\sigma_B, \sigma_A]\rangle|,$$

where $[\sigma_A, \sigma_B]$ is called commutator of the operators σ_B, σ_A, and the operator is defined by $[\sigma_B, \sigma_A] = \sigma_B\sigma_A - \sigma_A\sigma_B$. The commutator of two operators can be found by multiplying the matrices of the corresponding linear operators.

Chapter 3

Quantum Measurement Theory and Quantum Entanglement

Quantum phenomena tell the measurement theory of a physical observable. The measurement theory has no involvement with the classical computation, while in quantum system, it performs adequately on a quantum state in an irreversible way. The measurement theory says which kind of measurement is applicable to a quantum state.

Consider a qubit $|\psi\rangle$ in the quantum superposition state $(\alpha|0\rangle + \beta|1\rangle)$, where $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$. Once a measurement is made, the qubit collapses into either the basis state $|0\rangle$ or the basis state $|1\rangle$. After the measurement, α or β is not revealed, and the original state $|\psi\rangle$ no longer exists. During measurement, the quantum state is coupled with the system through a measurement device. This kind of coupled system is known as an open system. In general, the measuring apparatus is known as an ancilla.

3.1. Projective Measurements or Von Neumann Measurement

These measurements are the most basic type found in quantum mechanics and are considered ideal or perfect measurements of a quantum system. The measurement operators in projective measurements are projectors, with operator P satisfying the condition

$$P^2 = P.$$

Example:

$$P_0 = |0\rangle\langle 0|, \quad P_0^2 = (|0\rangle\langle 0|)^2 = |0\rangle\langle 0|0\rangle\langle 0| = |0\rangle(\langle 0|0\rangle)\langle 0| = |0\rangle\langle 0| = P_0$$

- For a 2-dimensional Hilbert space H with basis $\{|0\rangle, |1\rangle\}$, the projection operators are as follows:

  $$P_0 = |0\rangle\langle 0|, \quad P_1 = |1\rangle\langle 1|$$

  Note that the projection operators P_0 and P_1 are mutually exclusive. They form two projection subspaces of H.

- If a qubit is in the ground state, we denote the qubit by $|g\rangle$, and a qubit in excited state is denoted by $|e\rangle$. The corresponding projection operators can be written as

  $$P_g = |g\rangle\langle g|, \quad P_e = |e\rangle\langle e|$$

  We assume that these projection operators P_g and P_e are also mutually exclusive, and they form two projection subspaces.

- If $P_1 P_2 |\psi\rangle = 0$, then P_1 is called an orthogonal projection of P_2, and vice versa.

- Let a Hilbert space H of dimension d and $P_1, P_2, \ldots, P_m$ are m projection operators on H, then it should be $m \leq d$.

3.2. Born Rule [10]

The Born rule describes the probability of finding an output state after measuring a quantum system. A single quantum system is a system over a Hilbert space, generated by a finite-dimensional basis vector $\{u_i\}$. An ensemble is a collection of a large number of single quantum systems. Quantum systems of an ensemble can be observed in more than one different quantum

state. After the projection measurement of $|\psi\rangle$ for a single quantum system, the probability of getting the output result i can be calculated as follows: $P_r(i) = |\langle u_i|\psi\rangle|^2$.

For an ensemble quantum system, the probability of a measurement outcome acts in a classical way of calculating the probability of an event. This means that the measurement outcome is a statistical mixture, an incomplete information. The measurement of this kind of quantum system is done by observing the corresponding density operator. The density operator of a pure state $|\phi\rangle$ is defined by $\rho = |\phi\rangle\langle\phi|$. The density operator of a mixed state quantum system is defined by $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$, where p_i is the probability of a member of the system prepared in the state $|\phi_i\rangle$.

3.3. Generalized Measurement

In this section, we discuss a measurement operator and its properties in a general form. We symbolize a measurement operator by M_i, where the subscript i denotes an output measurement result. Let $|\phi\rangle$ be any arbitrary quantum state, then the probability of obtaining measurement output i is obtained by

$$Pr(i) = \langle\phi| M_i^\dagger M_i |\phi\rangle$$

After measurement, the original quantum state $|\phi\rangle$ is destroyed, and the new quantum state of the system is

$$|\phi'\rangle = \frac{M_i|\phi\rangle}{\sqrt{\langle\phi| M_i^\dagger M_i |\phi\rangle}}$$

General measurement operators must satisfy the completeness property and which is expressed by $\sum_i M_i^\dagger M_i = I$, where I is the identity operator. To obtain a measurement result i for a mixed state quantum system, the probability is computed by

$$Pr(i) = \mathrm{Tr}(M_i^\dagger M_i \rho),$$

where the system is observed with a density operator ρ.

If $\{P_i(= |u_i\rangle\langle u_i|)\}_i$ is a set of orthogonal projection operators and the corresponding measurement result is i, which is found with probability

$$Pr(i) = \mathrm{Tr}(P_i^\dagger P_i \rho) = \langle u_i|\rho|u_i\rangle = \mathrm{Tr}(|u_i\rangle\langle u_i|\rho)$$

Let a mixed state quantum system be described by a density operator ρ. After projective measurement, the measurement result is obtained i. Let ρ' be the density operator describing the new quantum state, which is computed by

$$\begin{aligned}\rho' &= \frac{P_i \rho P_i^\dagger}{\mathrm{Tr}(P_i^\dagger P_i \rho)} \\ &= \frac{|u_i\rangle\langle u_i|\rho|u_i\rangle\langle u_i|}{\langle u_i|\rho|u_i\rangle}.\end{aligned}$$

3.4. Positive Operator-Valued Measurement (POVM) [11]

Practically, all measurements are not repeatable. In particular, after detection of a photon, it is destroyed. Therefore, the concept of repeated measurements on a quantum system is not possible. In this case, a POVM measurement can be applied to the quantum system because

without regard to the postmeasurement state, it allows for describing measurements on the system.

In general, POVM measurement consists a set of positive definite operators that are denoted by E_i. Let $|\phi\rangle$ be any arbitrary quantum state, and the event is that the measurement outcome obtained is let say i, then the probability

$$Pr(i) = \langle\phi| E_i |\phi\rangle$$

A mixed quantum state system in $|\phi\rangle$ with density operator ρ, this probability is obtained by

$$Pr(i) = \mathrm{Tr}(E_i\rho).$$

The set of all positive operators $\{E_i\}$ of POVM satisfies the completeness property i.e., $\sum_i E_i$ is the identity operator. A POVM measurement operator can be formed from a projective measurement operator, which is defined by $E_i = P_i^\dagger P_i$. Note that a POVM measurement operator can describe a projective measurement operator, but it is not a projective measurement operator.

3.5. Entanglement [12]

Einstein, Podolsky, and Rosen (EPR) in 1935 claimed that the quantum theory is incomplete [13]. After that, in 1952, David Bohm did the EPR thought experiment by considering a spin-0 particle and spin-1/2 particles. In 1964, Bell's theorem came out, and it gives a clear distinction between quantum mechanics and local realism. The experiment agreed with the rules of quantum computing.

Entanglement is a bipartite system consisting of two subsystems. Two systems are called entangled when the quantum states of each composite system can only be described in terms of the other system's state. For example, Hilbert spaces of a composite system are a tensor product of two Hilbert spaces. Bell states are another example of an entangled quantum state.

3.5.1 Bell States or EPR States

Let $\mathcal{H}$ be a Hilbert space, which is a composite system and $\mathcal{H}_1, \mathcal{H}_2$ are two subspaces of $\mathcal{H}$. Then the composite system can be written as

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$$

. If $\{|\alpha_i\rangle\}$ be a basis of $\mathcal{H}_1$, and $\{|\alpha_i'\rangle\}$ be a basis of $\mathcal{H}_2$ then $\{|\alpha_i\rangle \otimes |\alpha_i'\rangle = |\alpha_i\alpha_i'\rangle\}$ be the basis of $\mathcal{H}$.

For a bipartite system, the Bell states or EPR states can be considered as a basis for the system. This states are defined and denoted as follows:

$$\begin{aligned} |\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned}$$

In general, the Bell states are expressed as

$$|\beta_{xy}\rangle = \frac{|0y\rangle + (-1)^x |1\bar{y}\rangle}{\sqrt{2}},$$

where y is called the parity bit and x is called the phase bit .

Chapter 4

Discussion of Some Existing QKD Protocols

QKD is a way to securely communicate that utilizes the fundamental properties of quantum computing. Basically, two legitimate parties, Bob and Alice share secret keys through two types of communication channels. The first type is a regular public channel i.e., classical communication channel, which is just a normal way of sending messages—like the Internet, a mobile phone, or a landline. The second kind of channel is a quantum communication channel, which is used to share quantum keys. In real life, this is done using single photons (tiny particles of light) that have different polarization states.

As we previously discussed that if a quantum state is measured, it changes its original quantum state. This is a basic rule in quantum computing. But the measurement result gives a classical outcome of a quantum state. So, to find out what the original key is, a person would have to measure the photons. But doing the measurement would disturb the system. If an eavesdropper (called Eve) tries to obtain information about the key by measuring the photons, it will change the state and thus, Alice and Bob will know that someone (an unintended person) is trying to get the key. In this section, we will discuss some basic key distribution protocols in the quantum domain.

4.1. BB84 Protocol [14]

In 1984, Charles Bennett and Gilles Brassard proposed the first QKD protocol, which is well known as the BB84 Protocol. There are three important principles used in the BB84 Quantum Key Distribution protocol:

4.1.1 No-Cloning Theorem [15]

This theorem, which was discussed by Wootters, Zurek, and Dieks, says that any arbitrary state in the quantum domain cannot be cloned or copied. This fundamental property of quantum mechanics prevents an eavesdropper from copying the quantum states used for secret key generation. Any such attempt introduces disturbances that reveal the presence of eavesdropping.

4.1.2 Measurement Leads to State Collapse

An important idea in QKD is that different bases are used to make a bit string. When we measure a quantum state using one of the given bases, the state collapses to one of the basis states. This means that it will provide completely random output when we measure the quantum state in a basis other than the basis in which the quantum state was prepared. So, if someone tries to get information, it will disturb the state of the system when measuring in a random quantum basis.

4.1.3 Measurements are Irreversible

Let $|\phi\rangle$ be an arbitrary quantum state in a Hilbert space H. Also assume that $\{|\beta_i\rangle\}$ be a bases space of H, and $|\phi\rangle$ is a superposition of the basis states $\{|\beta_i\rangle\}$. Measuring the state $|\phi\rangle$, the original superposition state is destroyed. It is not possible to obtain the superposition coefficients of the state $|\phi\rangle$. That is, we can not reverse the result after measurement.

For example, let a system be in the quantum state $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$, and the measure is made in the Hadamard basis $\{|+\rangle, |-\rangle\}$, then the measurement outcome is in the state $|+\rangle$

with probability $\frac{1}{2}$, while the measurement outcome is in the state $|-\rangle$ with probability $\frac{1}{2}$. Note that the system was originally encoded in the quantum state $|0\rangle$, and after measurement it is lost. Suppose that we obtain the quantum state $|+\rangle$ as a measurement outcome. Therefore, in the basis $\{|0\rangle, |1\rangle\}$, the state $|+\rangle$ is now different from what it was originally. In $\{|0\rangle, |1\rangle\}$ basis, the state $|+\rangle$ is:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Thus, using the Born rule, we can say that from the measurement output state $|+\rangle$, the probability of obtaining the original state $|0\rangle$ is $\frac{1}{2}$.

The protocol:

In the BB84 protocol, two types of basis states are utilized: one is the computational basis $\{|0\rangle, |1\rangle\}$ and the other is $\{|+\rangle, |-\rangle\}$ basis. The basis state $\{|+\rangle, |-\rangle\}$ is also called the Hadamard basis, and is also denoted by $\{|\pm\rangle\}$.

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Alice randomly chooses qubits from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and creates a string of $2n$ qubits. If a qubit is equal to $\{|0\rangle \text{ or } |+\rangle\}$, then it is symbolized by logical 0 (0_L). If the qubit is equal to $\{|1\rangle \text{ or } |-\rangle\}$, then it is symbolized by logical 1 (1_L). Then Alice transmits the sequence of $2n$ qubits to Bob over a quantum channel.

Bob measures each qubit of this sequence by randomly selecting the basis, either $B_1 = \{|0\rangle, |1\rangle\}$ or $B_2 = \{|\pm\rangle\}$ at each position. Therefore, according to the basic probability arguments, it can be said that among the $2n$ qubits, about n qubits will be measured in the B_1 basis and n of the qubits will be measured in the B_2 basis. Alice and Bob announce the basis at each position, which they have used to measure the qubit at that position. They check their basis states at each position and discard the states where they have considered different quantum states for measurement. After discarding all the qubits where Alice and Bob used two distinct basis states for measurement, the resulting key is called the *sifted key*.

The BB84 protocol proceeds as follows:

- Alice and Bob communicate over a Quantum Channel. Alice randomly chooses a bit string and a string of basis states of the same length. For each of the bits, Alice sends a polarized photon using an optical fiber (or any appropriate route for transferring photons) to Bob.
- For each polarized photon, Bob randomly selects a basis to observe its polarization. That is, Bob also chooses a string of basis states as the length of the number polarized photons sent by Alice. Bob will identify the state of the photons accurately, where he measured the states in the same basis as Alice's chosen basis states. Otherwise, when Bob chooses a different basis state for measuring, he will obtain a random bit.
- Then, Bob and Alice interact over an insecure public channel. Bob declares that the basis states that he used to measure each photon. Alice declares the position where the selected basis states of Bob for measuring the polarized photons are matched with Alice's chosen basis states at the same position. The bits at the other positions, where Alice and Bob uses two different basis states to measure photons, are discarded. The remaining bits form a string, and that is the shifted key, i.e., the secret key.

In this process, an error can occur due to the environment or any adversary's present. Therefore, Alice and Bob may compare some bits from the sifted key to check the rate of error in

the secret key. In the case of a high error rate, it indicates that an eavesdropper is present in the system. Then Alice and Bob discard the secret key and start the protocol again.

Example: Let, Alice randomly chooses a bit string $s = 010100$ and basis $B = B_1, B_1, B_2, B_2, B_2, B_1$. Bob randomly chooses a string of basis states as $B' = B_2, B_1, B_1, B_2, B_2, B_2$ and measures the encoded states. At last, Bob and Alice obtain the secret key as $k = 110$. The description of this process is given through a table below:

Alice's Bits	0	1	0	1	0	0
Alice's Basis	$\{\|0\rangle, \|1\rangle\}$	$\{\|0\rangle, \|1\rangle\}$	$\{\|+\rangle, \|-\rangle\}$	$\{\|+\rangle, \|-\rangle\}$	$\{\|+\rangle, \|-\rangle\}$	$\{\|0\rangle, \|1\rangle\}$
Bob's Basis	$\{\|+\rangle, \|-\rangle\}$	$\{\|0\rangle, \|1\rangle\}$	$\{\|0\rangle, \|1\rangle\}$	$\{\|+\rangle, \|-\rangle\}$	$\{\|+\rangle, \|-\rangle\}$	$\{\|+\rangle, \|-\rangle\}$
Match	✗	✓	✗	✓	✓	✗
Keep	✗	✓	✗	✓	✓	✗
Shared Secret Key		1		1	0	

4.2. B92 Protocol [16]

In the year 1992, Charles Bennett proposed a key distribution protocol in the quantum domain. In this protocol, Bob and Alice use two quantum bases that are not the same and are ideally orthogonal or nearly so. For example, let Alice uses the basis state $B = \{|0\rangle, |0'\rangle\}$ to send a classical bit string to Bob, where $|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Note that B is a non-orthogonal quantum basis state. For a classical bit string $s = s_1 s_2 \dots s_n$, if $s_i = 0$, Alice prepares $|0\rangle$, otherwise, he prepares $|0'\rangle$. Then the string of prepared quantum states s' is sent to Bob.

After sending the polarized photon as described in BB84 protocol, the B92 protocol is continued as follows:

- Bob uniformly selects a random bit string $x = x_1 x_2 \dots x_n$ where $x_i \in \{0, 1\}$.
- Bob randomly chooses a basis to measure each qubit, either in the computational basis states $B_1 = \{|0\rangle, |1\rangle\}$ basis or in the Hadamard basis state $B_3 = \{|+\rangle, |-\rangle\}$ basis (note that $|0'\rangle$ is the quantum state $|+\rangle$). In particular, with POVM measurement process, he measures the i-th position with measurement operator $M_0 = I - |+\rangle\langle+|$ if $x_i = 0$, and with measurement operator $M_1 = I - |0\rangle\langle 0|$ if $x_i = 1$.
- After measuring, with the measurement outcomes, Bob generates a bit string y. In particular, Bob creates a bit string y in which the $y_i = 0$ if the measurement outcome at the i-th position lies in the state $|-\rangle$ or $|1\rangle$ (-1 eigenstate of the bases operator B_1 and B_3), otherwise put $y_i = 1$ if the measurement outcome at the i-th position lies in the state $|+\rangle$ or $|0\rangle$ ($+1$ eigenstate of the bases operators B_1 and B_3).
- Bob declares the positions to Alice through a public insecure classical channel, where he gets $y_i = 1$. The secret key is a string $\{s_i\}_i$ for Alice, and a string $\{1 - x_i\}_i$ for Bob at the positions where $y_i = 1$.

Let Alice wants to send a bit string $s = 00101101$ to Bob. Then, he prepares a sequence of quantum states $s' = |0\rangle|0\rangle|+\rangle|0\rangle|+\rangle|+\rangle|0\rangle|+\rangle$, and sends it to Bob through a quantum communication channel.

- Bob uniformly selects a random bit string $x = 01100011$.

- Bob selects the measurement basis $M_0M_1M_1M_0M_0M_0M_1M_1$, where $M_1 = I - |0\rangle\langle 0|$ and $M_0 = I - |+\rangle\langle +|$. Now,

$$\begin{aligned} M_0|0\rangle &= (I - |+\rangle\langle +|)|0\rangle; \\ &= |0\rangle - |+\rangle\langle +|0\rangle; \\ &= [1\ 0]^t - [\frac{1}{2}\ \frac{1}{2}]^t; \\ &= \frac{1}{\sqrt{2}}|-\rangle; \end{aligned} \qquad \begin{aligned} M_1|+\rangle &= (I - |0\rangle\langle 0|)|+\rangle \\ &= |+\rangle - |0\rangle\langle 0|+\rangle \\ &= [\frac{1}{\sqrt{2}}\ \frac{1}{\sqrt{2}}]^t - [\frac{1}{\sqrt{2}}\ 0]^t \\ &= \frac{1}{\sqrt{2}}|1\rangle \end{aligned}$$

and,

$$M_0|+\rangle = (I - |+\rangle\langle +|)|+\rangle = |+\rangle - |+\rangle \text{ (inconclusive measurement)}$$
$$M_1|0\rangle = (I - |0\rangle\langle 0|)|0\rangle = |0\rangle - |0\rangle \text{ (inconclusive measurement)}$$

- Let the measurement result is $|-\rangle|+\rangle|1\rangle|-\rangle|0\rangle|0\rangle|+\rangle|1\rangle$. Therefore Bob generates $y = 01001110$.
- Bob declares the positions $2, 5, 6, 7$. The secret key for Alice is $k = 0110$, and for Bob is $k = \{1 - x_i\}_{i=2,5,6,7} = (1111) - (1001) = (1111) \oplus (1001) = 0110$.

4.3. E91 Protocol [17]

In BB84 protocol, the eavesdropping detection can be done due to the non-orthogonality of the original encoded qubit states. However, it is assumed that an eavesdropper Eve can not know the preparation basis of Alice. Because in that case, Eve can intercept the shared qubits and measure them in the preparation basis. Thus, he obtains the corresponding classical bit string and resends the qubits back to Bob. Although Eve is measuring the qubits, the eavesdropping can not be detected due to the same measurement basis in which Alice prepared the quantum states. In this way, Eve can get the secret key that is perfectly correlated with the secret key that Alice and Bob are sharing. Thereby, a more secure protocol was introduced in 1991 that we will discuss in this section.

The E91 protocol was proposed by Artur Ekert in 1991. His approach uses entangled pairs of photons. The key concept behind QKD in this protocol is quantum entanglement. The measurement result of an entangled state is completely correlated or anticorrelated. Therefore, when one property of a particle is measured, the effect of that property on its entangled state is known instantly, no matter the particles of the entangled state are how much far away.

However, it is impossible to know in advance what measurement outcome will be obtained. Therefore, using entangled particles for communication requires the measurement results to be shared through a classical communication channel. This idea, using entangled quantum states along with classical information exchange, is the foundation of Ekert's protocol. Quantum teleportation, which also relies on such entangled communication, builds upon the same principle.

The procedure of the quantum E91 protocol involves the following steps:

- The photon source prepares an entangled pair in an EPR state that is maximally entangled. Let, the entangled state used is:

$$\beta_{01} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB})$$

The subscript AB symbolize that first qubit belongs to Alice and second belongs to Bob.

- Alice selects her measurement basis in angles from $\phi_A = 0°, 45°, 90°$, i.e., X, $\frac{1}{\sqrt{2}}(Z+X)$, and Z basis. Bob chooses his measurement basis in angles from $\phi_B = 45°, 90°, 135°$, i.e., $\frac{1}{\sqrt{2}}(Z+X), Z$ and $\frac{1}{\sqrt{2}}(Z-X)$ basis.
- They perform measurements along a randomly chosen direction.
- They communicate over a classical channel to compare the measurement bases they used. If their measurement bases match, they keep those results to generate the secret key. Thus, according to the correlated or anti-correlated measurement bases, they obtain the shared secret key.

Chapter 5

Implementation and Recent Trends of QKD

QKD is a basic primitive to securely distribute a secret key. Many research is going on in this field. It is not possible to cover everything in one chapter or in one paper. Here, we want to give a basic idea of quantum computing and how it works to distribute a secret key to the legitimate parties securely. Some useful references are also given in this paper.

In real life, perfect communication through a quantum channel or a classical channel is not possible because of noise and imperfections. So, BB84 and many other QKD protocols are designed to be implemented practically, even with some errors. The key rate (how much secret key can be shared) depends on how many errors are present. Errors and key rate are inversely proportional to each other. Finally, a modern approach to QKD (Quantum Key Distribution) focuses on how secure the protocol is in practical settings. It should be hard to tell the difference between the real protocol and an ideal one, even with a small chance of error.

5.1. First QKD Implementations:From Single Photons to Coherent States

To make quantum key distribution work in real life, scientists used an idea from the 1970s by Stephen Wiesner. He suggested using the direction of light, called polarization, to represent quantum information. Two different polarizations can form the basis of the BB84 protocol. Light is a good way to send this information because it travels well through optical fibers or even through open space. Using two different light modes where a photon can exist is enough to send quantum data.

The prime challenge is to generate a single photon. For the successful implementation of QKD protocols like BB84, it is necessary that the quantum channel carries a single photon at a time. Till now, the sources of single photons are not efficient.

Bennet et al. in 1989 [16, 18], first took place the QKD experiment for the BB84 protocol. The experiment was based on polarization encoding. Light pulses were generated from a light-emitting diode (LED), and that pulses were polarized by a polarizer subsequently goes by an interference filter. The quantum states (qubits) were encoded as Pockels cells in those photon's polarization. Using a Wollaston prism, Bob analyzed the polarization states. The output ports of the prism were monitored by photomultipliers.

Due to the long term security against quantum computers, cryptographic protocols based on quantum computing are considered superior over classical cryptographic schemes. Although it is vulnerable because of the imperfections in practical implementations [20, 21]. In the real world, no system device is perfectly ideal. It is ideal to execute QKD schemes with a single photon. But experimentally, it is challenging to develop such a source that emits exactly a single photon per unit time till now. Therefore, most of the recent experiments are executed by using a coherent laser pulse. The sources of laser pulses make several photons with a Poisson distribution. It is proven that in every laser pulse, the probability of the occurrence of multi-photons is non-negligible. This type of vulnerability is known as 'photon number splitting (PNS) attack'. In this attack, the adversary measures the quantum states in each pulse. The adversary can store the measuring outcome and transmit the rest to the legitimate parties. Therefore, the presence of the adversary can not be caught by the legitimate parties during the protocol. Since the adversary has partial information about the data, the security properties of QKD are compromised. It is observed that the decoy state method not only overcomes the PNS attack but also improves the performance of QKD.

In 2002, it was observed that coherent states follow a predictable pattern (Poisson distribution) to guess the number of photons in a pulse. This helped the attacker find out which pulses had more than one photon. If a coherent state has an average of 0.5 photons, there is a 10% chance that it actually has more than one photon. Although there are several attacks, they can not ultimately break the security of QKD. Rather, there is a limitation on the distance for secure key transmission.

5.2. Protocols Resistant to PNS Attacks

in 2003, Hwang [22] discussed a method to overcome the PNS attack. The method stated that, with the original signal message, some arbitrary signals are also sent. The extra arbitrary signals (states) are called the decoy states. The standard signal states and decoy states are differentiated for the photon number distributions of these two states. After measuring all the quantum states (signals) the positions of the decoy states are announced. By comparing the positions of the decoy states, legitimate parties analyse the presence of an eavesdropper. Using decoy states in QKD has been proven far more beneficial.

Over the years, numerous new protocols have been developed to address the issue of Photon Number Splitting (PNS) attacks. SARG04 protocol is one such protocol that utilized the same idea as the BB84 QKD protocol with decoy states. In 2004, Scarani et al. [23] introduced this protocol.

In the SARG04 protocol, four orthogonal quantum states $\{|0\rangle, |+\rangle\}$, and $\{|1\rangle, |-\rangle\}$ have used. Alice sends the quantum states randomly chosen from either the basis states $\{|0\rangle, |+\rangle\}$ or $\{|1\rangle, |-\rangle\}$. This step of quantum computation is the same as the BB84 protocol. The only modification is the classical shifting procedure. Bob measures the quantum states in either σ_x basis or σ_z basis. Then Alice announces her choice of measuring basis to Bob. The measurement will give a valid result if the outcome does not belong to Alice's group. For example, let Bob measures in the σ_x basis and gets $|-\rangle$, and Alice's choice is $\{|0\rangle$ or $|+\rangle\}$, Bob will know that Alice sends 0.

Other types of secure quantum key distribution are called distributed phase protocols. Some such QKD's are discussed below:

- **Distributed Phase Shifting (DPS)**,
- **Coherent One Way (COW)**.

These protocols rely on the idea of coherence of quantum states. In the DPS protocol [25], the light pulses are set at a phase angle between 0 to π. The receiver observes the interference between the light pulses. If an adversary wants to obtain information by intercepting the signal, the coherence between the pulses is broken. Therefore, the eavesdropping is detected by the legitimate parties.

In the COW protocol [24], the information is encoded in time. The sender sends coherent pulses in the empty state, or the quantum state has a mean photon number less than 1. To obtain the secret key, the receiver measures the time of arrival of the photons. However, COW is harder to analyze in terms of security, so full security proofs are still being developed.

Recent research shows that the **secret key rate (SKR)** of these newer methods is similar to the improved BB84 protocol that uses coherent light. This shows the ongoing challenge of balancing security and practicality in the development of quantum communication protocols.

5.3. Continuous Variable Quantum Key Distribution (CV-QKD)

While the BB84 protocol is very popular, in early 2000s, one such method explored is **Continuous Variable Quantum Key Distribution (CV-QKD)** [26], which uses the amplitude

and phase (called quadratures) of light instead of discrete properties like polarization. In 1999, Ralph [27] first proposed CV-QKD protocol.

Coherent light states were found to be good for CV-QKD because they balance uncertainty between the quadratures, X and P. These states can be measured using standard tools like **homodyne** and **heterodyne detection**, which are already used in classical telecommunications. This made CV-QKD easier to set up compared to discrete variable QKD (DV-QKD), which needs more complex detectors.

Advantages of CV-QKD:

- Works with regular laser sources and detectors.
- Reuses technology from classical communication systems.
- Easier to implement compared to DV-QKD.

Challenges of CV-QKD:

- Harder to prove security due to complex math (infinite-dimensional space).
- Very sensitive to signal loss—higher losses lead to more errors.
- Needs strong error-correcting codes to handle high error rates.

5.4. Quantum Hacking in QKD System

It is believed that quantum-key-distribution (QKD) protocols securely distribute quantum signals through standard optical fiber (secure quantum channel). There exist many feasible attacks in the literature. In 1997, Biham and More [38] introduced a strong attack against QKD where the adversary attacks directly on the final secret key using quantum gates and quantum memories. In this attack, the adversary is assumed to act on the quantum apparatus of the legitimate parties independently and identically in each step of the protocol. As a result, the secret key rate is lower-bounded by the Devetak–Winter rate [37]. Makarov et al. [28, 29] introduced a fake-state attack (intercept-resend attack) and examined the feasibility. The time-shift attack is another one, which was introduced by Zhao et al. [31] in 2008. In this attack, the difference in efficiency between two detectors is detected in a time domain QKD system. The idea is that the adversary shifts each signal's arriving time randomly with some non-negligible probability. The probability is chosen in a way such that the receiver's measurement result is biased toward either 1 or 0, depending on the time shift. Thus, the adversary can obtain partial information. The experimental result showed that an eavesdropper can break the security of a QKD system with a non-negligible probability. This success probability is due to the detection efficiency loophole in the Bell's inequalities experimental testing. Although in [39], it is presented that the security of a QKD system against collective attacks implies that the system is secure against any attack.

5.5. Measurement Device Independent QKD

In some cases, practical attacks on QKD implementations, such as time-shift attacks, intercept-resend attacks, and side-channel attacks, can allow an adversary to recover the entire secret key. Device-independent (DI) cryptography is one of the solutions in this era to avoid these types of attacks [33–36]. The basic assumption in all QKD systems are: (*i*) all the legitimate parties and adversary also follow the basic properties of quantum computing, (*ii*) the parties can choose the measurement apparatus as per their choice, and adversary is not aware of the choice, (*iii*) The outcome is only known to the legitimate parties. A device-independent

QKD (DIQKD) system does not allow one to get knowledge of the process of how a QKD device works. In particular, with fully DI cryptography, the parties have a device whose security does not rely on any assumptions about how the quantum apparatus operates. In fully DIQKD [32], quantum apparatuses are considered as a black box, taking as input a classical message and providing a classical output. In the DIQKD system, the quantum devices may not perform as per specifications. Researchers are motivated to study DIQKD because it overcomes the adversary scenario when the quantum devices used by the parties are not trustworthy. However, the DIQKD protocols are challenging to realize experimentally as they require a detection-loophole-free Bell test [41–43] implementation, which necessitates very high efficiency of detection [36].

One-sided device-independent QKD [40] is a concept that lies between a standard QKD and a device-independent QKD. In particular, only one of the legitimate parties has trust in her measurement apparatus. In real life, the concept of one-sided DIQKD fits many situations. This leads to interest in studying one-sided DIQKD. Analogous to the concept that the security of DIQKD depends on the violation of Bell's inequality, the security properties of one-sided DIQKD depend on demonstrating quantum steering [44]. Since closing the detection loophole in a steering experiment [45, 46] is significantly easier than in a Bell test, implementing one-sided DIQKD requires less detector efficiency than for DI-QKD. Thus, the practical implementation of one-sided DIQKD is feasible with respect to the existing QKD implementations. Moreover, security guarantee of one-sided DIQKD with finite resources is an interesting area for further research.

To resolve the issues of detection efficiency loophole [48] of QKD system, a semi device-independent QKD system was introduced [47]. In this scenario, it was assumed that the dimension of the relevant Hilbert space quantum system is known (upper bounded). The properties of the quantum system and measurements are noncharacterized. Pawliwski and Brunner [47] showed that semi DIQKD is secure against any individual attacks, unlike fully DIQKD. Woodhead [49] observed that the BB84 QKD protocol is semi-device independent because it is secure, considering one of the users' devices is restricted to a qubit Hilbert space. They also derived a lower bound on the secret key rate for the entanglement-based BB84 protocol. Chaturvedi et al. [50] proposed the security conditions for this scenario of semi DIQKD. The adversary can not benefit by obtaining a small quantum memory (a qubit) to attack the semi DIQKD protocol, unlike other protocols. Practically, as the distance between the two users increases, noise also increases. The required minimum detection efficiency of the protocol is therefore limited by the distance between the two users. In the case of fully DIQKD, this distance is just a couple of kilometers [51]. Chaturvedi et al. [50] described a semi DIQKD protocol where the distance between two users can be significantly extended. Therefore, all types of DIQKD are secure against quantum hacking attacks, unlike standard QKD, where information is encoded in quantum states, transmitted through a quantum channel, and then retrieved by measuring those states. However, one-sided DIQKD and semi-DIQKD systems are more practical and efficient to implement in real-world scenarios.

Chapter 6

Applications of QKD

QKD is a cryptographic primitive that enables legitimate parties to securely share secret keys, even in the presence of an eavesdropper with unlimited computational power. It has broad applications in everyday life, including secure online banking, encrypted messaging, and protected email communication [59, 60]. A very common and widely used application is the distribution of a secret key to symmetric key cryptosystems like Advanced Encryption Standard (AES). Multiuser smartphone network, session initiation protocol (SIP) are another example of the application area of QKD [57, 58]. Here, the secret key is shared between clients and server through a star-type network. Another emerging area of application is secure communication for drones. Drones are used for imaging, surveying, surveillance, delivery, and various forms of data transmission, often involving highly sensitive information. When integrated with QKD, drone systems can achieve enhanced security and enable smart, secure, and reliable mobility [55, 56]. QKD networks are now being deployed in metropolitan areas, demonstrating their growing practicality and real-world relevance.

In the year 1989, QKD was first time experimentally demonstrated [19]. From the year of 2000s, it has been practically experimented with in a real-world environment. Peev et al. [52] presented an overview of the design and implementation of QKD carried out under the European SECOQC project (2004–2008), which unified the efforts of 41 research and industrial organizations to develop a large-scale and secure quantum communication network. The average length between two node links is 20-30 km, and the longest link path is 83 km. Sasaki et al. [53] demonstrated a secure communication network through a QKD apparatus. Their designed QKD network is known as the Tokyo QKD network. Through this QKD system, they successfully presented a live video conferencing using OTP encryption. Stucki et al. [54] introduced the performance of the SwissQuantum QKD network that ran for more than 1.5 years in a metropolitan area. The objective was to experiment with the reliability of the quantum layer in a production environment for a long period of time.

However, several major challenges exist before QKD can be widely adopted across large-scale data systems. In long-term storage networks handling big datasets, the key generation rate must be significantly increased. For example, securing petabyte-scale data is equivalent to storing the information of one million individuals, which would require key generation rates on the order of 1 Gb/s, which is far beyond the capability of current QKD systems [61]. Moreover, during the implementation of a QKD system, the security against side channel attacks is one of the major challenges. As discussed in Section 5, DIQKD inherently protects the QKD system against side channel attacks [33]. Quantum entanglement is the core of these DIQKD systems, which is a correlation between distant particles. This idea was first introduced by A. Ekert, whose protocol is known as the E91 QKD protocol [17]. Overall, QKD plays a fundamental role in building the long-lived storage network system, being combined with the state-of-the-art public-key cryptography.

In more detail, QKD has been integrated into secure communication protocols such as Transport Layer Security (TLS) or Internet Protocol Security (IPsec) [62] or used to distribute key information, One-Time Pad (OTP) [63]. The main requirement of QKD protocols is to share predefined keys while maintaining quantum security. Another significant area of application lies in the design and implementation of QKD networks that enable the incorporation of other cryptographic primitives. The DARPA BBN QKD network [64] was first established in the USA in 2002 with 10 nodes, with the concept of BB84 QKD protocol. It was demonstrated to modify the internet security and network routing. Some of the similar QKD

networks are EU SEOCQC QKD Network (2004), JAPAN TOKYO UQCC QKD Network (2010), CHINA QKD Networks (2014) [65–67].

Moreover, QKD can be used as a key primitive for the cryptographic schemes where predefined keys are required to transmit through a secure quantum communication channel, such as quantum secure multi-party computation, quantum oblivious transfer, quantum money, quantum private information retrieval, etc [68–71]. Therefore, QKD has a remarkable deployment from real-world networking systems to other cryptographic key exchange techniques.

7. Conclusion

In this manuscript, we have discussed the basic fundamental primitives of quantum computing, focusing on quantum key distribution (QKD). We have also discussed the fundamental protocols in quantum key distribution, their practical implementation and recent trends. The effect of PNS attacks on existing QKD protocols and some developed QKD protocols resistant to this attack is also discussed here. Moreover, the background and recent trends of device-independent QKD systems, and continuous variable QKD systems are also described in this manuscript. In the last chapter, we gave an overview of applications of QKD in real life and other fields of quantum cryptography.

References

[1] Christof Paar and Jan Pelzl. *Understanding Cryptography*, volume 1. Springer, 2010.

[2] Souvik Roy and P. Venkateswaran. Online payment system using steganography and visual cryptography. In *2014 IEEE Students' Conference on Electrical, Electronics and Computer Science*, pages 1–5. IEEE, 2014.

[3] Suryadip Chakraborty, Candice Jackson, Moncrief Frazier, and Kyra Clark. A study on password protection and encryption in the era of cyber attacks. In *SoutheastCon 2024*, pages 460–465. IEEE, 2024.

[4] Arjun Verma, Falguni Sharma, Prashant Sharma, Ayush Choudhary, Jyoti Khemnani, Chirag Choudhary, and Arvind Pal. Analyzing cryptographic integrity and security challenges in WhatsApp, Telegram, and OpenSSL and development of CipherX. In *Proceedings of the International Conference on Advancements in Computing Technologies and Artificial Intelligence (COMPUTATIA 2025)*, volume 189, pages 484. Springer Nature, 2025.

[5] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE, 1994.

[6] David McMahon. *Quantum Computing Explained*. John Wiley & Sons, 2008.

[7] Zhong-Xia Shang. Pauli quantum computing: I as $|0\rangle$ and X as $|1\rangle$. *arXiv preprint arXiv:2412.03109*, 2024.

[8] Michael R. Geller, Zoë Holmes, Patrick J. Coles, and Andrew Sornborger. Experimental quantum learning of a spectral decomposition. *Physical Review Research*, 3(3):033200, 2021.

[9] Jan Hilgevoord and Jos Uffink. The uncertainty principle. 2001.

[10] Arnold Neumaier. The Born rule—100 years ago and today. *Entropy*, 27(4):415, 2025.

[11] Howard E. Brandt. Positive operator valued measure in quantum information processing. *American Journal of Physics*, 67(5):434–439, 1999.

[12] Richard Jozsa. Entanglement and quantum computation. *arXiv preprint quant-ph/9707034*, 1997.

[13] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777, 1935.

[14] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014.

[15] William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[16] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121–3124, 1992.

[17] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[18] Charles H. Bennett and Gilles Brassard. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *ACM Sigact News*, 20(4):78–80, 1989.

[19] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992.

[20] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330, 2000.

[21] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5):052304, 2000.

[22] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003.

[23] Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):057901, 2004.

[24] Damien Stucki, Sylvain Fasel, Nicolas Gisin, Yann Thoma, and Hugo Zbinden. Coherent one-way quantum key distribution. In *Photon Counting Applications, Quantum Optics, and Quantum Cryptography*, volume 6583, pages 194–197. SPIE, 2007.

[25] K. Inoue, E. Waks, and Y. Yamamoto. Differential-phase-shift quantum key distribution using coherent light. *Physical Review A*, 68(2):022317, 2003.

[26] Yichen Zhang, Yiming Bian, Zhengyu Li, Song Yu, and Hong Guo. Continuous-variable quantum key distribution system: past, present, and future. *Applied Physics Reviews*, 11(1), 2024.

[27] Timothy C. Ralph. Continuous variable quantum cryptography. *Physical Review A*, 61(1):010303, 1999.

[28] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A—Atomic, Molecular, and Optical Physics*, 74(2):022313, 2006.

[29] Vadim Makarov and Johannes Skaar. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *arXiv preprint quant-ph/0702262*, 2007.

[30] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *arXiv preprint quant-ph/0512080*, 2005.

[31] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A—Atomic, Molecular, and Optical Physics*, 78(4):042333, 2008.

[32] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. *Communications of the ACM*, 62(4):133–133, 2019.

[33] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[34] Samuel L. Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Physical Review Letters*, 108(13):130502, 2012.

[35] Tobias Gehring, Vitus Händchen, Jörg Duhme, Fabian Furrer, Torsten Franz, Christoph Pacher, Reinhard F. Werner, and Roman Schnabel. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nature Communications*, 6(1):8795, 2015.

[36] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[37] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005.

[38] Eli Biham and Tal Mor. Security of quantum cryptography against collective attacks. *Physical Review Letters*, 78(11):2256, 1997.

[39] Eli Biham, Michel Boyer, Gilles Brassard, and Tal Mor. Security of quantum key distribution against all collective attacks. *Algorithmica*, 34(4):372–388, 2002.

[40] Cyril Branciard, Eric G. Cavalcanti, Stephen P. Walborn, Valerio Scarani, and Howard M. Wiseman. One-sided device-independent quantum key distribution: security, feasibility, and the connection with steering. *Physical Review A—Atomic, Molecular, and Optical Physics*, 85(1):010301, 2012.

[41] Brad G. Christensen, Kevin T. McCusker, Joseph B. Altepeter, Brice Calkins, Thomas Gerrits, Adriana E. Lita, Aaron Miller, Lynden K. Shalm, Yanbao Zhang, Sae Woo Nam, et al. Detection-loophole-free test of quantum nonlocality, and applications. *Physical Review Letters*, 111(13):130406, 2013.

[42] Bas Hensen, Hannes Bernien, Anaïs E. Dréau, Andreas Reiserer, Norbert Kalb, Machiel S. Blok, Just Ruitenberg, Raymond F. L. Vermeulen, Raymond N. Schouten, Carlos Abellán, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[43] Wenjamin Rosenfeld, Daniel Burchardt, Robert Garthoff, Kai Redeker, Norbert Ortegel, Markus Rau, and Harald Weinfurter. Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Physical Review Letters*, 119(1):010402, 2017.

[44] Eric Gama Cavalcanti, Steve J. Jones, Howard M. Wiseman, and Margaret D. Reid. Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox. *Physical Review A—Atomic, Molecular, and Optical Physics*, 80(3):032112, 2009.

[45] Adam Joseph Bennet, David Andrew Evans, Dylan John Saunders, Cyril Branciard, Eric Gama Cavalcanti, Howard Mark Wiseman, and Geoff J. Pryde. Arbitrarily loss-tolerant Einstein-Podolsky-Rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole. *Physical Review X*, 2(3):031003, 2012.

[46] Bernhard Wittmann, Sven Ramelow, Fabian Steinlechner, Nathan K. Langford, Nicolas Brunner, Howard M. Wiseman, Rupert Ursin, and Anton Zeilinger. Loophole-free Einstein-Podolsky-Rosen experiment via quantum steering. *New Journal of Physics*, 14(5):053030, 2012.

[47] Marcin Pawłowski and Nicolas Brunner. Semi-device-independent security of one-way quantum key distribution. *Physical Review A—Atomic, Molecular, and Optical Physics*, 84(1):010302, 2011.

[48] Philip M. Pearle. Hidden-variable example based upon data rejection. *Physical Review D*, 2(8):1418, 1970.

[49] Erik Woodhead. Semi device independence of the BB84 protocol. *New Journal of Physics*, 18(5):055010, 2016.

[50] Anubhav Chaturvedi, Maharshi Ray, Ryszard Veynar, and Marcin Pawłowski. On the security of semi-device-independent QKD protocols. *Quantum Information Processing*, 17(6):131, 2018.

[51] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Physical Review Letters*, 105(7):070501, 2010.

[52] Momtchil Peev, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, Winfried Boxleitner, Thierry Debuisschert, Eleni Diamanti, Mehrdad Dianati, James F. Dynes, et al. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 11(7):075001, 2009.

[53] Masahide Sasaki, Mikio Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al. Field test of quantum key distribution in the Tokyo QKD Network. *Optics Express*, 19(11):10387–10409, 2011.

[54] Damien Stucki, Matthieu Legre, Francois Buntschu, B. Clausen, Nadine Felber, Nicolas Gisin, Luca Henzen, Pascal Junod, Gérald Litzistorf, Patrick Monbaron, et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New Journal of Physics*, 13(12):123001, 2011.

[55] Masahide Sasaki. Quantum key distribution and its applications. *IEEE Security & Privacy*, 16(5):42–48, 2018.

[56] Yang Xue, Wei Chen, Shuang Wang, Zhenqiang Yin, Lei Shi, and Zhengfu Han. Airborne quantum key distribution: a review. *Chinese Optics Letters*, 19(12):122702, 2021.

[57] German Granados, Washington Velasquez, Ricardo Cajo, and Maria Antonieta-Alvarez. Quantum key distribution in multiple fiber networks and its application in urban communications: a comprehensive review. *IEEE Access*, 2025.

[58] A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K-i Yoshino, H. Iizuka, T. Sakamoto, A. Tomita, E. Shimamura, S. Asami, et al. Quantum key distribution network for multiple applications. *Quantum Science and Technology*, 2(3):034003, 2017.

[59] Sapthak Mohajon Turjya, Raj Singh, Pritam Sarkar, Sujata Swain, and Anjan Bandyopadhyay. Quantum-based QKD and sugar-salt encryption approach in cloud-fog computing to strengthen protection of online banking data. In *2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS)*, pages 1–7. IEEE, 2024.

[60] Tayyabah Hassan and Fahad Ahmed. Transaction and identity authentication security model for E-banking: confluence of quantum cryptography and AI. In *International Conference on Intelligent Technologies and Applications*, pages 338–347. Springer, 2018.

[61] Matthias Geihs. Long-term protection of integrity and confidentiality—security foundations and system constructions. 2018.

[62] Alan Mink, Sheila Frankel, and Ray Perlner. Quantum key distribution (QKD) and commodity security protocols: introduction and integration. *arXiv preprint arXiv:1004.0605*, 2010.

[63] Mohamed Elboukhari, Mostafa Azizi, and Abdelmalek Azizi. Improving TLS security by quantum cryptography. *International Journal of Network Security & Its Applications (IJNSA)*, 2(3):87–100, 2010.

[64] Chip Elliott and Henry Yeh. DARPA quantum network testbed. 2007.

[65] Miralem Mehic, Marcin Niemiec, Stefan Rass, Jiajun Ma, Momtchil Peev, Alejandro Aguado, Vicente Martin, Stefan Schauer, Andreas Poppe, Christoph Pacher, et al. Quantum key distribution: a networking perspective. *ACM Computing Surveys (CSUR)*, 53(5):1–41, 2020.

[66] Masahide Sasaki, M. Fujiwra, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, et al. Tokyo QKD network and the evolution to secure photonic network. In *CLEO: Science and Innovations*, page JTuC1. Optica Publishing Group, 2011.

[67] Mehrdad Dianati, Romain Alléaume, Maurice Gagnaire, and Xuemin Shen. Architecture and protocols of the future European quantum key distribution network. *Security and Communication Networks*, 1(1):57–74, 2008.

[68] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[69] Iordanis Kerenidis and Anupam Prakash. Quantum private information retrieval. *SIAM Journal on Computing*, 47(3):1172–1203, 2017.

[70] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, 2002.

[71] Sushmita Sarkar, Vikas Srivastava, Tapaswini Mohanty, Sumit Kumar Debnath, and Sihem Mesnager. An efficient quantum oblivious transfer protocol. *Cluster Computing*, 27(10):14037–14048, 2024.