American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN: 2320-0936
Volume-15, Issue-6, pp-88-103
www.ajer.org
Research Paper Open Access

Optimization And Performance Analysis of Quantum Key Distribution Systems

Ayat Faruk Swadı SWADI and Remzi YILDIRIM
Computer Engineering, Tokat Gaziosmanpaşa University, Tokat, TÜRKİYE
Corresponding Author: Remzi YILDIRIM

ABSTRACT: *In this study, Quantum Key Distribution (QKD) which is based on the principles of quantum mechanics—is considered one of the important modern encryption techniques for ensuring secure communication. However, practical systems face challenges such as channel noise and photon loss, which increase the Quantum Bit Error Rate (QBER) and consequently reduce the* ***Secret*** *Key Rate (SKR). To address this issue, an adaptive framework based on Artificial Intelligence (AI) and Machine Learning (ML) techniques is proposed to adapt to channel conditions and improve performance. The results of the study show a reduction in the bit error rate and an increase in key generation efficiency.*
KEYWORDS: *Quantum Key Distribution (QKD), Artificial Intelligence (AI), Machine Learning (ML), Reinforcement Learning (RL), Artificial Neural Networks (NN)*

Date of Submission: 14-06-2026 Date of acceptance: 27-06-2026

I. INTRODUCTION

Today, the rapid development of digital communication systems has made data security more critical. Classical cryptography methods are generally based on the factorization of large prime numbers or discrete logarithm problems. However, the development of quantum computers, especially with Shor's algorithm, has revealed the risk of breaking widely used public-key systems such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) [1], [2]. This situation has led researchers to investigate more secure communication methods and has brought the field of quantum cryptography to the forefront [3], [4].

Quantum Key Distribution (QKD) bases its security not on mathematical complexity but on the fundamental laws of quantum mechanics, thereby providing theoretical security even against an attacker with unlimited computational power [5], [6]. QKD uses quantum principles such as Heisenberg's Uncertainty Principle, the no-cloning theorem, and entanglement to detect the intervention of third parties in communication [7], [8]. Along with fundamental protocols such as BB84, B92, and E91 [7], [9], [10], modern protocols such as Continuous Variable (CV-QKD) [11], [12], [13] and Measurement-Device-Independent (MDI-QKD) [14], [15] enable secure key sharing both theoretically and experimentally. In addition, methods such as the Decoy State technique have made practical systems more resistant to attacks such as photon number splitting (PNS) [16].

Recent studies show that QKD systems can be applied across a wide range of fields, from satellitebased communication [17], to fiber optic networks [18], [19], and even to the vision of the "Quantum Internet" [20], [21]. However, in practical applications, challenges such as channel noise, photon loss, detector imperfections, and hardware limitations [22], [23], [24] increase the Quantum Bit Error Rate (QBER) and reduce the Secret Key Generation Rate (SKR) [25], [26]. For the standardization of these processes, various security criteria have been defined by organizations such as ETSI [27], [28].

In this context, the integration of Artificial Intelligence (AI) and Machine Learning (ML) techniques into QKD systems has emerged as an important approach to improve performance, reduce error rates, and enhance security by adapting to channel conditions [29], [30].

II. FUNDAMENTALS OF QUANTUM INFORMATION

Quantum cryptography, unlike classical cryptography, bases its security not on complex mathematical problems but directly on the fundamental physical laws of quantum mechanics [3], [15]. This approach has gained critical importance, especially with the development of quantum computers. While classical encryption systems rely on problems considered difficult to solve, such as prime factorization, these problems can be easily solved using quantum algorithms (e.g., Shor's Algorithm) [7], [28]. The most fundamental unit of quantum information systems is the qubit. Unlike classical bits, a qubit can represent multiple states simultaneously due to the principle of superposition [5]. This can be mathematically expressed as follows:

$$|\psi\rangle = \alpha\,|0\rangle + \beta|1\rangle \quad (1)$$

Where:
|ψ⟩ (psi): Represents the *quantum state of a qubit* (the complete state description)
α (alpha): Probability amplitude of the state |0⟩
β (beta): Probability amplitude of the state |1⟩
|0⟩: Basis state representing the classical bit value 0
|1⟩: Basis state representing the classical bit value 1

α|0⟩ + β|1⟩: Superposition state (the qubit exists in a combination of both |0⟩ and |1⟩ until measurement)
In this equation, α and β are complex probability amplitudes and satisfy the normalization condition:

$$|\alpha|2 + |\beta|2 = 1 \quad (1)$$

Where:
α (alpha): Probability amplitude of the qubit being in state |0⟩
β (beta): Probability amplitude of the qubit being in state |1⟩
$|\alpha|^2$: Probability of measuring the state |0⟩
$|\beta|^2$: Probability of measuring the state |1⟩
$|\alpha|^2 + |\beta|^2 = 1$: Normalization condition, meaning the total probability of all possible outcomes is always equal to 1 (certainty condition in quantum mechanics) [5], [29]. This unique property allows quantum systems to perform parallel processing and carry much more information compared to classical systems. Furthermore, according to the "no-cloning theorem" of quantum mechanics, it is impossible to create a perfect copy of a quantum state, which makes any eavesdropping physically detectable [8].

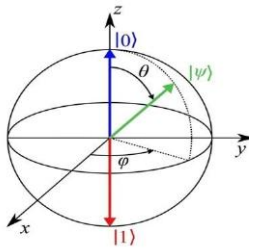

Figure. 1. Qubit Superposition (Bloch Sphere) and the Bloch Sphere representation of the qubit state[31].

The Bloch Sphere is a geometric model used to represent the state of a qubit in a two-level quantum system. The north pole represents the state |0⟩|0\rangle|0⟩, while the south pole represents the state |1⟩|1\rangle|1⟩. The vector |ψ⟩|\psi\rangle|ψ⟩, shown by the green arrow, represents the quantum superposition state; here, the angle θ\thetaθ determines the measurement probability, while the angle ϕ\phiϕ determines the relative phase of the system.

The Bloch sphere in Figure 1 is used to visualize the state of a qubit [1]. A qubit is not limited to the states |0⟩|0\rangle|0⟩ at the north pole and |1⟩|1\rangle|1⟩ at the south pole. Any point on the surface of the sphere can be expressed as a state vector defined by the angles θ\thetaθ and ϕ\phiϕ:

$$|\psi\rangle = \cos(\theta\backslash 2)\,|0\rangle + e\hat{}\,i\phi\backslash\sin(\theta/2)|1\rangle \quad (3)$$

Where:
|ψ⟩ (psi): General state of a single qubit (Bloch sphere representation)
θ (theta): Polar angle on the Bloch sphere (controls balance between |0⟩ and |1⟩)

φ (phi): Azimuthal phase angle (controls relative phase between basis states)
cos(θ/2): Amplitude of the state |0⟩
sin(θ/2): Amplitude of the state |1⟩
e^(iφ): Complex phase factor (introduces quantum phase information)
|0⟩: Basis state representing classical bit 0 |1⟩: Basis state representing classical bit 1
Whole expression: A normalized qubit state defined on the Bloch sphere, showing both probability and phase information simultaneously. Here, θ\thetaθ represents the polar angle, while ϕ\phiϕ represents the azimuthal angle. This representation demonstrates that a qubit can exist as a linear combination (superposition) of two basis states [1]. However, according to the fundamental principles of quantum mechanics, when an external measurement is performed, the state of the system collapses to one of these poles. This collapse phenomenon constitutes one of the greatest advantages in terms of security in quantum key distribution (QKD) systems. Because, according to the "no-cloning theorem," it is impossible to create an identical copy of an unknown quantum state [8]. If an eavesdropper (Eve) attempts to measure the qubit in the channel, the original state of the qubit will be disturbed, and this can be detected by the receiver (Bob) through an increase in the error rate (QBER) [2], [25].

2.1. FUNDAMENTALS OF THE BB84 PROTOCOL AND HARDWARE IMPLEMENTATIONS

The BB84 protocol is one of the fundamental applications of quantum cryptography and provides secure key distribution (QKD) between two parties (Alice and Bob) [9]. The security of this protocol is based on the states of single photons sent in randomly chosen bases, and any eavesdropping attempt can be detected statistically [2], [23].

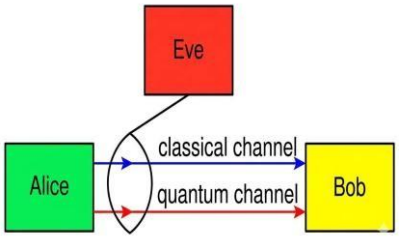

Figure 2. Hardware schematic of 2D and 4D QKD systems.

Figure. 2. The BB84 protocol is one of the fundamental applications of quantum cryptography and provides secure key distribution (QKD) between two parties (Alice and Bob) [9]. The security of this protocol is based on the states of single photons sent in randomly chosen bases, and any eavesdropping attempt can be detected statistically [2], [23],[32].

The prepared quantum states are transmitted to Bob (right) through the fiber channel [24]. On Bob's side, measurements are performed using beam splitters (BS), polarization controllers (PC), and SPAD (Single-Photon Avalanche Diode) detectors [16], [18]. A Time Tagger records the measurement times, ensuring synchronization with Alice and enabling key generation. In such practical systems, factors such as detector efficiency and channel loss directly affect the key generation rate [25], [26].

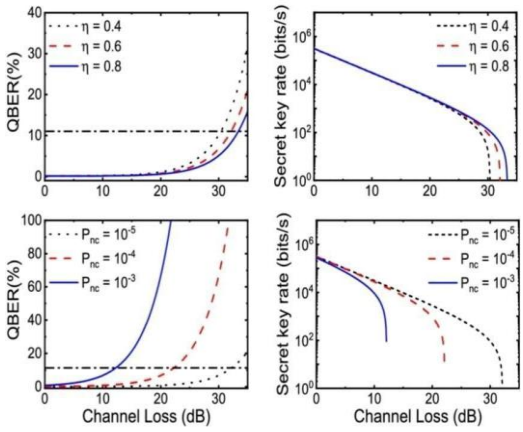

Figure.3. QKD channel structure and attacker (Eve) model. QKD performance analysis depending on channel loss [33].

The graphs in Figure. 3 show a directly proportional relationship between channel loss and the Quantum Bit Error Rate (QBER). As channel loss increases, the error rate rises sharply, exceeding the critical security threshold. In parallel, the Secret Key Rate (SKR) decreases logarithmically with increasing distance and channel loss. It also emphasizes the effect of hardware parameters, showing that increasing detector efficiency (η\etaη) and reducing the dark count probability (PncP_{nc}Pnc) ensure system stability and extend the effective operational distance before key generation stops.

The BB84 protocol and channel security use two separate channels, as shown in Figure.3. The quantum channel (red line), through which quantum states (e.g., polarized photons) are transmitted, and the classical channel (blue line), through which data such as basis comparison is shared [9]. Operations performed over the classical channel do not involve the key itself but only the verification of the used bases, and this process is part of the post-processing stage [3], [15].

In this process, any attempt by a third party (Eve, red box) to interfere with the quantum channel (curved black line) causes an irreversible disturbance in the system due to the fundamental laws of quantum mechanics [5]. According to the no-cloning theorem, Eve cannot copy a quantum state without measuring it, and the moment she performs a measurement, she alters the state of the photon [8]. This intervention increases the error rate (QBER) in the data received by Bob, allowing Alice and Bob to statistically detect whether the channel has been eavesdropped using statistical analysis methods [2], [25].

2.3. QUANTUM BIT ERROR RATE (QBER) AND SECRET KEY RATE (SKR)

One of the fundamental metrics used to evaluate the performance of quantum systems is the Quantum Bit Error Rate (QBER). QBER is defined as the ratio of the number of erroneous bits to the total number of received bits:

$$QBER = \text{N(error)/N(total)} \tag{4}$$

Where:
QBER (Quantum Bit Error Rate): Ratio of incorrect quantum bits in the transmission (error rate of the quantum channel)
N_error: Number of erroneous (wrong) received bits
N_total: Total number of received or detected bits
N_error/ N_total: Fraction representing how much of the transmitted quantum information is corrupted during transmission

Overall meaning: QBER measures the quality and security of a quantum communication channel; a higher value indicates more noise or possible eavesdropping interference [9], [17]. A high QBER value indicates either environmental noise in the channel or an active eavesdropping attempt [7], [18]. The main goal in quantum key distribution systems is to maximize the amount of secure key generated per unit time (SKR). For a BB84 protocol, the asymptotic secret key rate (R) is expressed as[4], [8].

$$R = [1 - h(eb) - f \cdot h(eb)] \tag{5}$$

Where, the variables represent:
Q**:** Sifted key rate (effective bit rate)
e_b: Error rate (QBER)
f**:** Error correction efficiency
h(x): Binary entropy function [1]

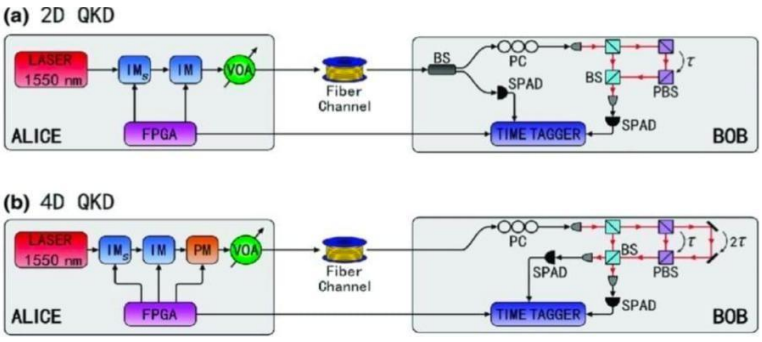

Figure. 4. Effect of Channel Loss on QBER and SKR

Figure.4 simulates the variation of system performance parameters with respect to channel loss (distance). The upper graphs show results for different system efficiencies (η): as efficiency decreases, the QBER (top left) increases more rapidly, and the secret key rate (top right) drops to zero at shorter distances [16], [18],[34]. The lower graphs present results for different dark count probabilities (P_nc): as detector noise increases (P_nc), the QBER (bottom left) exceeds the critical 11% threshold (horizontal dashed line) much earlier, and the SKR (bottom right) decreases dramatically [16], [25]. These graphs clearly demonstrate that as QBER increases, the secret key rate decreases, and system optimization is essential [9].

2.4. THE ROLE OF ARTIFICIAL INTELLIGENCE

In recent years**,** Artificial Intelligence (AI) algorithms have begun to play revolutionary roles in quantum cryptography systems [15]. These algorithms are used for critical tasks such as estimating channel parameters, minimizing error rates, and dynamically optimizing system performance [29], [30].

In particular, methods such as Artificial Neural Networks (ANN), Reinforcement Learning (RL), and Support Vector Regression (SVR) provide significantly higher accuracy and adaptability compared to classical approaches against channel losses and noise effects shown in Figure 2.4 [29], [16]. These AI-based approaches have become essential tools for closing security vulnerabilities caused by practical device imperfections and improving the efficiency of complex systems such as Measurement-Device-Independent QKD (MDI-QKD) [13], [15]. Furthermore, thanks to their realtime channel monitoring capability, they ensure the sustainability of the Secret Key Rate (SKR) even under varying environmental conditions [21], [30].

III. THEORETICAL FOUNDATIONS

Quantum Key Distribution (QKD) protocols derive their strength not from the complexity of mathematical algorithms as in classical cryptography, but from the fundamental laws of quantum mechanics. The following sections describe the key principles that provide immunity to these systems:

3.1. Qubit and Quantum Superposition

A qubit is the fundamental unit of quantum information processing [1]. While a classical bit is limited to two definite values such as 0 or 1, a qubit stands out with its ability to exist in a state of superposition [5]. Mathematically, a qubit state |ψ⟩|\psi\rangle|ψ⟩ is expressed as a linear combination of basis vectors:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{6}$$

Where:

- |ψ⟩ (psi): The quantum state of a qubit (state vector in Hilbert space)
- α (alpha): Probability amplitude of the qubit being in state |0⟩
- β (beta): Probability amplitude of the qubit being in state |1⟩
- |0⟩: Computational basis state representing classical bit 0
- |1⟩: Computational basis state representing classical bit 1
- α|0⟩ + β|1⟩: Superposition of the two basis states, meaning the qubit exists in both states probabilistically until measured

Here, α\alphaα and β\betaβ are probability amplitudes satisfying the condition |α|2+|β|2=1|\alpha|^2 + |\beta|^2 = 1|α|2+|β|2=1 [1], [29]. This property gives QKD systems a unique capability: information is transmitted not as static values, but as physical states that simultaneously contain multiple possibilities (e.g., photon polarization states) [9], [10].

This superposition state makes it physically impossible to predict the value before measurement and is the most fundamental element ensuring the security of quantum channels [5], [6]. Obtaining information without disturbing this state is impossible due to the no-cloning theorem [8].

3.2. MEASUREMENT PRINCIPLE AND WAVE FUNCTION COLLAPSE

In the classical world, it is possible to observe a system without affecting its state; however, in quantum mechanics, the measurement process is inherently an intrusive action [1], [5]. When a third party (Eve) intercepts a qubit and attempts to measure its state, the wave function collapses from a superposition state into one of the basis states (|0\rangle or |1\rangle) [6].

This change is an irreversible process. Since the eavesdropper does not know the "basis" used by the sender (Alice), any measurement inevitably introduces statistical disturbances (perturbations) in the data [7], [16]. These disturbances are detected as an increase in the Quantum Bit Error Rate (QBER) between the parties, thereby

revealing any eavesdropping attempt through a physical signature [9], [25]. In particular, in practical QKD systems, detector imperfections and attacks that may exploit these weaknesses (such as "tailored bright illumination") are among the most critical threats to system security [23], [24]. Therefore, the wave function collapse principle is not only a natural protection mechanism, but also a fundamental motivation for the development of "Measurement-DeviceIndependent" (MDI-QKD) protocols [13], [15].

3.3.NO-CLONING THEOREM

The No-Cloning Theorem, formulated by Wootters and Zurek in 1982, is one of the most important security pillars of QKD [8]. The theorem states that it is physically impossible to create an exact copy of an unknown quantum state [1], [5]. In the context of cyberattacks, a malicious party cannot perfectly implement an "intercept-andresend" strategy; because it is not possible to copy a qubit passing through a quantum channel and forward it to the receiver without being detected [3], [9]. If the eavesdropper attempts to clone the state, they must perform a measurement, and this measurement—as previously explained—disturbs the original state and destroys its fidelity [2], [6]. This theorem guarantees that quantum information is fundamentally unique and, unlike digital data, cannot be perfectly replicated at the bit level [15], [29]. Although attacks such as photon-number splitting (PNS) may be attempted due to imperfect devices, modern protocols (e.g., Decoy-state BB84) employ additional security layers based on the no-cloning principle to prevent such attacks [16], [25].

IV. QUANTUM KEY DISTRIBUTION PROTOCOLS (QKD)

QKD protocols are classified according to the nature of the quantum states used and the measurement methods applied [3], [9]. This classification generally includes discrete-variable QKD (DV-QKD) [9], [10], continuous-variable QKD (CV-QKD) [29], [15], and measurement-device-independent QKD (MDI-QKD) [13], [16]. The security of these protocols is based on two fundamental pillars of quantum mechanics: the "Heisenberg Uncertainty Principle" and the "No-Cloning Theorem" [1], [5]. According to these fundamental laws, it is physically impossible to copy or measure an unknown quantum state without disturbing it [1], [8]. As a result, any eavesdropping attempt on the quantum channel inevitably leaves a detectable physical trace (an increase in the error rate) in the system [2], [25]. This property is what distinguishes QKD systems from classical cryptographic methods and provides them with "information-theoretic security" [6], [7].

4.1. BB84 PROTOCOL (RECTILINEAR BASIS PROTOCOL)

BB84 is considered the cornerstone of quantum cryptography [9]. The security of the protocol is based on the random use of two incompatible basis sets (e.g., rectilinear and diagonal bases) [1], [10].

Physical Mechanism: Alice encodes bits using photon polarization states. The main difficulty for an eavesdropper (Eve) is that choosing an incorrect measurement basis irreversibly disturbs the quantum state of the photon [1], [8]. This intervention increases the error rate at Bob's side (QBER) up to 25% in affected cases, which statistically reveals the presence of eavesdropping [9], [25]. Mathmatical Representatıon ,

Basis Sets (X and Z): The Z-basis is defined as $\{|0\rangle, |1\rangle\}$ and the X-basis as $\{|+\rangle, |-\rangle\}$ [1].

Hadamard Transformation: Used for basis conversion: $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$ [1], [29]. • Maximum Acceptable Rate: The protocol is theoretically secure as long as QBER < 11% [7], [28]. If the error exceeds this threshold, it is assumed that the system is outside "information-theoretic security" limits and the key is discarded [6], [7].

4.2. B92 PROTOCOL (TWO-STATE PROTOCOL)

The B92 protocol is based on the fact that any two non-orthogonal quantum states cannot be perfectly distinguished with a single measurement [10]. This protocol was developed as an alternative to BB84 and derives its security from the principles that quantum states cannot be perfectly copied or distinguished [1], [9]

Technical Difference: Instead of the four states used in BB84, B92 uses only two states (e.g., $|0\rangle$ and $|+\rangle$). Alice selects one of these two states depending on the bit value to be transmitted [9], [10].

Security Challenge: Since $\langle 0|+\rangle = 1/\sqrt{2} \neq 0$, Bob sometimes obtains "inconclusive" results. The security here arises from the fact that Eve cannot resend a lost photon without introducing significant noise [3], [8]. ***Sensitivity:*** However, this protocol is more sensitive to "vacuum-shift attacks" and channel losses compared to BB84 [16], [25]. Due to its lower efficiency in practical implementations, modern systems generally prefer BB84 or decoy-state-based variations [15], [25].

4.3. E91 PROTOCOL (ENTANGLEMENT-BASED ENCRYPTION)

This protocol transforms quantum key distribution from "particle transmission" to "entanglement sharing" [11]. Here, a pair of entangled photons (EPR pairs) is generated, and the scheme relies on the non-locality property of quantum mechanics [1], [3].

Working Principle: One photon of the pair is sent to Alice and the other to Bob. The secret value does not physically exist during transmission; instead, it emerges from the correlation between Alice's and Bob's measurement outcomes at the moment of simultaneous measurement [5], [11].

Security Verification via CHSH Inequality: The security of the protocol is verified using the CHSH inequality, a variant of Bell's theorem [11]. The statistical value S is computed as follows [1], [29]:

$$s = E(a,b) - E(a,b') + E(a',b) + E(a',b') \tag{7}$$

Where;

- S: CHSH correlation parameter (Bell test value)
- E(a, b): Correlation between measurement settings a and b ,E(a, b'): Correlation between measurement settings a and b'
- E(a', b): Correlation between measurement settings a' and b,E(a', b'): Correlation between measurement settings a' and b'
- a, a': Measurement settings chosen by Alice
- b, b': Measurement settings chosen by Bob

If $S = 2\sqrt{2} \approx 2.82$, this indicates that entanglement is perfectly "pure" and no third party has information about the system [2]. If $S \leq 2$, the system behaves classically, indicating decoherence or an eavesdropping attempt [6], [25]. The E91 protocol is particularly important as it forms the theoretical foundation of device-independent quantum key distribution (DI-QKD) [13], [15].

4.4. CV-QKD PROTOCOL (CONTINUOUS VARIABLES)

Unlike previous protocols that rely on the "discrete counting" of photons (Discrete Variable QKD), CV-QKD is based on Homodyne detection, where the wave properties of photons (amplitude and phase) are measured [29]. This approach encodes quantum information in a continuous spectrum, enabling high-efficiency key generation [15], [30].

Economic Advantage: This protocol does not require expensive single-photon detectors (SNSPDs) and can operate with standard telecommunication infrastructure (such as fiber-optic lasers and coherent receivers) [16], [25]. This feature is one of the most important factors facilitating the integration of CV-QKD into existing networks [21], [30]. Mathematical Security: The security is based on the Heisenberg Uncertainty Relation between the quadratures (amplitude and phase) of the quantum field [1], [29]:

$$\Delta x \cdot \Delta p \geq \frac{1}{4} \tag{8}$$

Where,

- Δx: Uncertainty (noise) in the amplitude quadrature (position-like variable)
- Δp: Uncertainty (noise) in the phase quadrature (momentum-like variable)
- x: Amplitude component of the quantum signal
- p: Phase component of the quantum signal

Any attempt by Eve to extract information about the x quadrature (amplitude) inevitably introduces increased randomness (noise) in the p quadrature (phase), which can be immediately detected through statistical analysis by Bob [5], [25].CV-QKD systems are particularly important for short- and medium-distance networks due to their high Secret Key Rate (SKR) performance [13], [15].

4.5. MEASUREMENT-DEVICE-INDEPENDENT QKD (MDI-QKD)

MDI-QKD is an innovative protocol designed to completely eliminate side-channel attacks on detectors [13]. In this protocol, Alice and Bob send quantum states to a central node called Charles. Charles then performs a Bell State Measurement (BSM) on the incoming photons [13], [15]. The main advantage of the system is that Charles (or an attacker who compromises the node) cannot obtain any information about the secret key [16], [23].

The initial state of the system is expressed as:

$$|\psi A\rangle \otimes |\psi B\rangle \quad (9)$$

- $|\psi A\rangle$: Quantum state prepared by Alice
- $|\psi B\rangle$: Quantum state prepared by Bob
- $\otimes$: Tensor product (joint quantum state combination)
- Bell State Measurement (BSM) Equations:

Charles projects incoming photons onto one of the following four Bell states [1], [29]:

$$|\psi^{\pm}\rangle = 1/\sqrt{(2)}\ (|01\rangle \pm |10\rangle) \quad (10)$$

Where:

$|\Psi\pm\rangle$: Bell entangled states (anti-correlated states)

- $|01\rangle$, $|10\rangle$: Two-qubit basis states
- **±:** Quantum phase difference (constructive/destructive superposition)

$$|\phi^{\{\pm\}}\rangle = 1/\sqrt{(2)}\ (|00\rangle \pm |11\rangle \quad (11)$$

Where:

- $|\Phi\pm\rangle$: Bell entangled states (correlated states)
- $|00\rangle$, $|11\rangle$: Two-qubit basis states
- BSM Success Probability:

In practical systems, the success probability of BSM depends on channel and detector efficiencies [16]:

$$P\{BSM\} = \frac{1}{2}\ \eta A.\eta B \quad (12)$$

Where,

- $P\{BSM\}$: Probability of successful Bell state measurement
- ηA: Detection efficiency of Alice's channel ηB: Detection efficiency of Bob's channel
- 1/2: Intrinsic success probability limit of linear optical BSM
- Secret Key Rate (SKR) Lower Bound:
- For MDI-QKD, the secure key rate is given by [13], [25]:

$$K \geq Q_{\{11\}}\left[1 - H_2(e_{\{11\}})\right] - f\ \backslash cdot\ Q_{\{\backslash mu\}\backslash cdot} H_2\left(E_{\{\backslash mu\}}\right) \quad (13)$$

Where:

- K: Final secure key rate (secret key generation rate)
- Q_{11}: Gain of single-photon contributions from both Alice and Bob
- e_{11}: Error rate of single-photon events
- f: Error correction efficiency factor
- Q_μ: Overall gain of signal states with intensity μ
- E_μ: Quantum bit error rate for signal states
- $H_2(x)$: Binary entropy function

MDI-QKD is considered one of the most secure candidates for future quantum networks, as it completely eliminates detector vulnerabilities (detector hacking) in practical devices [13], [30].

4.6. DEVICE-INDEPENDENT QKD (DI-QKD)

DI-QKD is the protocol with the highest level of security, as it makes no assumptions about the internal structure of the devices used (hardware) [13], [11]. Security is entirely based on the violation of Bell inequalities; thus, even if the devices are treated as "black boxes," the secrecy of the key is guaranteed by the laws of physics [2], [15]. CHSH Test: To verify the security of the system, correlations between Alice and Bob are calculated using the following statistical value [1], [29]:

$$S = |E(a,b) - E(a,b') + E(a',b) + E(a',b')| \quad (14)$$

Where:

S: CHSH Bell inequality parameter (correlation strength measure)

- E(a,b): Correlation between Alice's setting *a* and Bob's setting *b*
- E(a,b'): Correlation between Alice's setting *a* and Bob's alternative setting *b'*
- E(a',b): Correlation between Alice's alternative setting *a'* and Bob's setting *b*
- E(a',b'): Correlation between Alice's alternative setting *a'* and Bob's alternative setting *b'*
- a, a': Measurement settings chosen by Alice
- b, b': Measurement settings chosen by Bob

Security Condition:

$S > 2 \Longrightarrow$ Quantum-secure

If the value of S is greater than 2, it proves that the system cannot be simulated by any classical strategy or eavesdropping attempt [5], [9].

Secret Key Rate (SKR):

In DI-QKD systems, the final key rate is expressed as [6], [7]:

$$K \geq N\,[1 - H_{2(QBER)} - leak\_EC] \tag{15}$$

Where:

- K: Final secret key rate
- N: Total number of transmitted signals (raw key length)
- H_2(QBER): Binary entropy function representing information loss due to errors
- QBER: Quantum Bit Error Rate
- leak_EC: Information leaked during error correction

Although DI-QKD is theoretically the most secure method, it requires extremely high detector efficiency in practical implementations and is therefore still considered an advanced technology under development [24], [30]. Alice and Bob send optical fields with randomly chosen phases [29]:

$$EA = \sqrt{(\mu A)}e\{i\phi A\}\backslash text(\ and\ )EB = \sqrt{(\mu B)}e(i\phi B) \tag{16}$$

Where:

- E_A, E_B: Complex electric field amplitudes of Alice and Bob
- μ_A, μ_B: Mean photon numbers of Alice and Bob sources
- ϕ_A, ϕ_B: Phase values of Alice and Bob signals
- e^(iϕ): Complex exponential representing phase (Euler form)
- i: Imaginary unit (i = √−1)

Interference Signal at the Central Node:

The intensity measured by detectors at the central node depends on the phase difference between the two fields [1], [29]:

$$I \propto |EA + E_B|^2 = \mu_A + \mu_B + 2\sqrt{\{\mu_A\mu_B\}}\backslash cos(\phi_A - \phi_B) \tag{17}$$

Where:

- I: Interference intensity
- E_A, E_B: Electric field amplitudes of Alice and Bob paths
- μ_A, μ_B: Mean photon numbers of the sources
- ϕ_A, ϕ_B: Phase values of Alice and Bob signals
- cos(ϕ_A − ϕ_B): Interference term caused by phase difference between the two signals

Secret Key Rate (SKR):

$$K \approx \eta\{channel\} \cdot \mu[1 - H2(QBER)] \tag{18}$$

Where:

- K: Secret key rate / key generation amount
- η_channel: Channel efficiency (probability that photons successfully pass through the channel)
- μ: Mean photon number per pulse
- QBER: Quantum Bit Error Rate

- $H_2(\cdot)$: Binary entropy function

Here, η_channel represents channel transmission efficiency, μ represents the average photon number, and H_2(QBER) represents information leakage during error correction [7], [25]. TF-QKD is considered one of the most critical components of quantum backbone networks, as it enables secure communication over long-distance fiber links exceeding 500 km [21], [30].

4.8. GHZ-BASED MULTI-PARTY QKD AND QUANTUM SECRET SHARING (QSS)

GHZ-QSS uses GHZ (Greenberger–Horne–Zeilinger) states to distribute keys among more than two participants (Alice, Bob, Charlie, etc.) [1], [11]. In this protocol, reconstructing the secret (key) requires the cooperation of all parties, making it ideal for secure group communication and voting systems [3], [13]. Three-Party GHZ State: The maximally entangled state forming the basis of the system is expressed as [1], [29],

$$|GHZ\rangle = (|000\rangle + |111\rangle) / \sqrt{(2)} \quad (19)$$

Where:

- |GHZ⟩: GHZ quantum state (three-qubit entangled state)
- |000⟩: Quantum state where all qubits are in state 0
- |111⟩: Quantum state where all qubits are in state 1
- √2: Normalization factor (ensures total probability equals 1)

Success Probability: The purity of the received state and transmission quality are measured using the density matrix (ρ) as follows [2]:

$$P\{success\} = \langle GHZ\,|\rho|\,GHZ\,\rangle \quad (20)$$

Where:

- P_success**:** Success probability
- |GHZ⟩: Ideal GHZ quantum state
- ⟨GHZ|: Hermitian conjugate (bra) of the GHZ state
- ρ: Density matrix representing the actual quantum state of the system

Secret Key Rate (SKR):

$$K \geq N\,[1 - H2(QBER)] \quad (21)$$

Where:

- K: Final secret key length
- N: Raw key length (number of bits before processing)
- QBER: Quantum Bit Error Rate
- $H_2(\cdot)$: Binary entropy function

Where, **N** represents the number of valid events, and **QBER** represents the total error rate calculated based on the joint measurement outcomes of all participants [6], [16]. GHZ-based protocols are critically important in the network layer of the quantum internet, as they enable secure synchronization among multiple nodes [21], [30].

V. SYSTEM MODEL

5.1. QUANTUM INFORMATION EXCHANGE INFRASTRUCTURE (QUANTUM INFRASTRUCTURE)

The proposed model is based on a deep integration between quantum mechanics and classical information theory [1], [7]. The operational cycle begins at the sender side (Alice), who uses a Weak Coherent Pulse (WCP) laser source to generate weak photon pulses [9], [10]. Information is encoded into physical properties representing qubits, such as polarization or phase [1], [3]. Mathematically, states are represented in a complex Hilbert space, where the superposition principle |\psi⟩=α |0⟩+β |1⟩ ensures encryption that cannot be broken using conventional methods [1], [6].

The qubit is transmitted through a quantum channel modeled to include effects such as path loss and mode dispersion [16], [29]. One of the main challenges addressed by the model is decoherence, where photons interact with atoms in the transmission medium, causing deviations in the density matrix (ρ) [5], [25]. To mitigate this issue, the system adopts a “differential detection” architecture at the receiver side (Bob), utilizing Single-Photon Avalanche Diodes (SPADs) with high detection efficiency and low thermal noise [23], [24]. This approach enables successful signal discrimination even in environments with strong electromagnetic interference [21], [30].

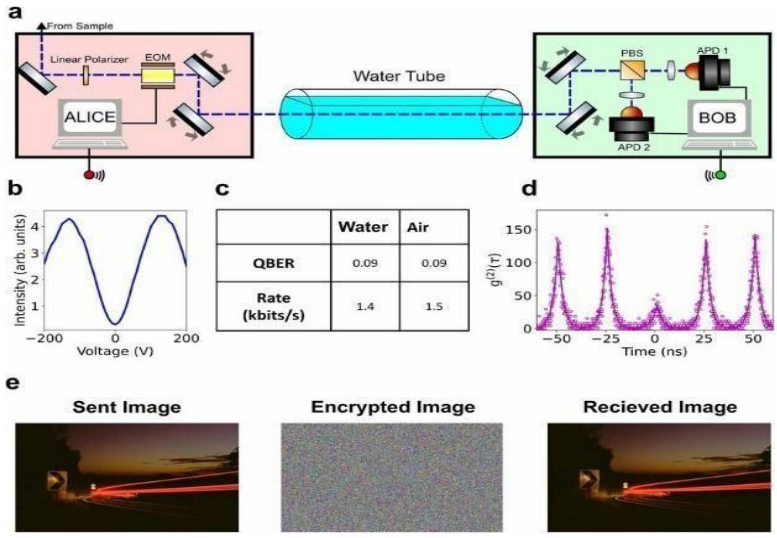

Figure 5. Illustrates the infrastructure of the QKD system. In this structure, qubits are transmitted through the quantum channel via optical fibers, while the classical channel (Public Channel) is used to perform post-processing steps such as basis comparison (sifting) and privacy amplification. In this way, the presence of any physical eavesdropping on the transmission line can be securely detected [34].

5.2. SECURITY MECHANISM, ERROR ANALYSIS (QBER), AND PURIFICATION PROTOCOLS

The security of the system is based on the fundamental principles of quantum mechanics, namely the Heisenberg Uncertainty Principle and the No-cloning Theorem [1], [8]. In the proposed model, any attempt by an eavesdropper (Eve) to measure photons in the channel inevitably causes the collapse of the wavefunction and disturbs the original quantum state due to the laws of quantum mechanics [1], [5]. This physical intervention introduces statistical deviations in the system, directly increasing the **Quantum Bit Error Rate (QBER)** [9]. QBER is defined as the ratio of erroneous bits to the total number of received bits and is the most critical parameter used to evaluate system reliability [25], [2]. Mathematically, QBER is calculated as follows [7]:

$$QBER = \frac{(e\{det\} + e\{opt\} + e\{back\})}{R\{raw\}} \tag{22}$$

Where:

- QBER: Quantum Bit Error Rate
- e_det: Detector errors
- e_opt: Optical errors
- e_back**:** Background noise
- R_raw: Raw detection rate

Table 1. Comparative analysis of system performance under different operational conditions.

Length (km)	Loss (dB)	Expected QBER	Secure Key Rate (bps)
10	2.0	%1.5	1.2M
50	10.0	%3.8	450K
100	20.0	%8.2	85K
150	30.0	> %11 (Critical)	0 (System stopped)

After the measurement phase is completed, the system transitions to the **Key Distillation** process. This stage is not a simple data processing step; rather, it is an advanced mathematical protocol that includes **Error Correction** using high-efficiency LDPC (Low-Density Parity-Check) codes, followed by **Privacy Amplification**, which eliminates any partial information that may have been leaked. At the end of this process, the probability that the final key is known to an eavesdropper is theoretically reduced to zero (2^−ε).

5.3. INTELLIGENT OPTIMIZATION AND ADAPTIVE RESPONSE (AI-DRIVEN OPTIMIZATION)

The most innovative part of our model is the **Intelligent Coordination Layer**. This layer operates as a feedback loop that uses Artificial Intelligence (AI) to counter channel instabilities. In traditional systems, the photon transmission rate is fixed; however, in our model, **Reinforcement Learning** is used to dynamically adjust transmission parameters in real time according to atmospheric fluctuations or mechanical noise in the fiber.

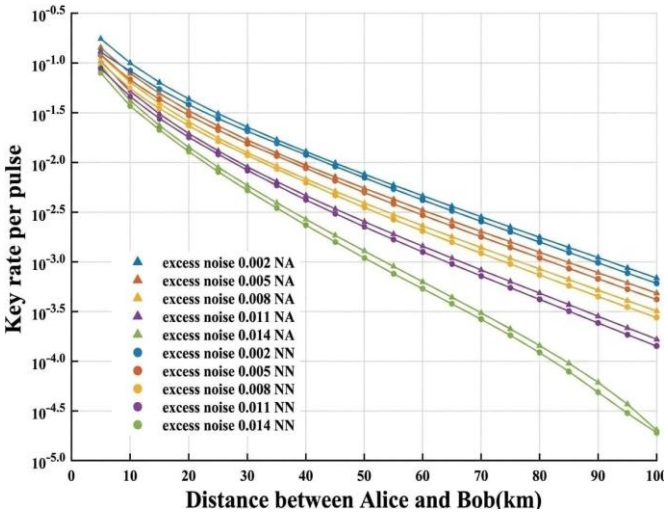

Figure.6. Shows the analytical evaluation of the Secret Key Rate (SKR) under dynamic noise conditions. The dashed line (conventional system) exhibits a sharp decline and failure in service continuity when a channel disturbance occurs, whereas the solid line (AI-assisted proposed system) demonstrates strong adaptability and the ability to restore stability in key generation by predicting channel conditions in advance. This significantly improves system resilience in real-world networks [35].

Neural network models are trained to estimate the **Quantum Signal-to-Noise Ratio (QSNR)**. If the model predicts an increase in errors due to a **Photon Number Splitting (PNS)** attack attempt, the system immediately activates the **Decoy State** protocol. This protective mechanism sends laser pulses at different energy levels to accurately detect the presence of an eavesdropper. This integration of physics and artificial intelligence enhances system resilience, making it suitable for deployment in "Smart City" networks where communication channels are continuously changing.

VI. METHODOLOGY USED

The methodology proposed in this study is centered on the design of an intelligent optimization system based on artificial intelligence techniques to improve the efficiency of Quantum Key Distribution (QKD) systems [15], [30]. The main objective of this model is to address the limitations of traditional systems that treat quantum channels as static environments; however, in reality, these channels are highly dynamic and subject to external factors such as noise, temperature variations, and fiber bending [16], [29].

Our approach is based on integrating quantum communication processes with machine learning algorithms to develop an adaptive system capable of minimizing the Quantum Bit Error Rate (QBER) while simultaneously maximizing the Secret Key Rate (SKR) through real-time analysis of channel conditions [25], [13]. In this context, the proposed model employs Deep Learning techniques to recognize complex noise patterns and optimizes system parameters (such as photon intensity or basis selection ratios) in real time [24], [23]. This integration aims to enhance the stability and practical applicability of QKD systems, particularly in long-distance and high-noise communication channels [21], [30].

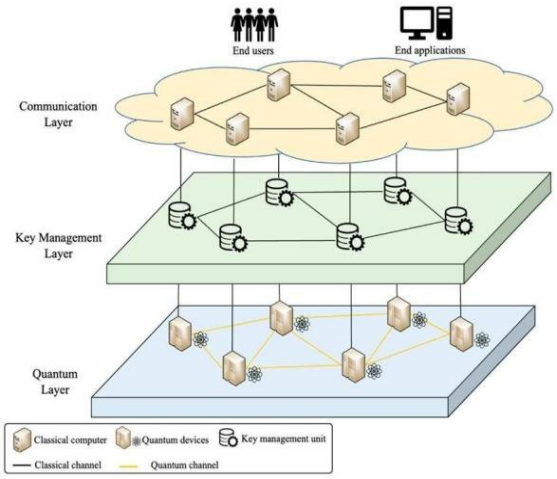

Figure 7. Proposed Artificial Intelligence-Based Adaptive QKD Optimization Framework. This diagram illustrates the integration between the quantum layer and the artificial intelligence module. Real-time data obtained from the quantum channel (QBER, SNR, etc.) is provided as input to the AI model. The model analyzes this data, dynamically optimizes system parameters (such as basis selection and error correction thresholds), and provides feedback to maximize the Secret Key Rate (SKR)[36].

The proposed model consists of a three-dimensional structure that combines the QKD subsystem, the feature extraction unit, and the artificial intelligence–based optimization engine [15], [30]. The operational process begins with the collection of raw data from the quantum system, where sensitive physical parameters such as channel loss (channel loss), signal-to-noise ratio (SNR), and raw key generation rate are monitored [16], [25

This situation creates an intelligent feedback loop that enables the system to continue operating at the highest possible efficiency even under intense environmental noise [5], [7]. This integrated structure aims to overcome physical-layer limitations using software-based intelligence, bringing secure key generation capacity closer to its theoretical limits [2], [15].

Mathematical Modeling and Intelligent Optimization Structure: To perform this optimization, the model is based on a hybrid strategy consisting of prediction and optimization algorithms [13], [15]. Artificial Neural Networks (ANN) are used to model complex channel behavior; here, system outputs can be expressed by the function $y = f(x; \theta)$ [29], [30]. In this context, θ represents the model weights that are optimized during training to minimize the error in predicting future QBER values [7], [25]. In parallel, **Reinforcement Learning** plays a vital role in dynamic decision-making processes [21], [23]. An intelligent agent operates within the channel environment, performing actions aimed at adjusting system parameters and receives a mathematical reward that balances SKR increase and QBER reduction according to the following formula [2], [6]:

$$\left|\psi\right\rangle = \cos\left(\frac{\theta}{2}\right)\left|0\right\rangle + e^{\{i\phi\}}\sin\left(\frac{\theta}{2}\right)\left|1\right\rangle \quad (23)$$

Where:

- R: Objective function representing system performance
- w1: Weight coefficient assigned to the Secret Key Rate
- SKR: Secret Key Rate
- w2: Weight coefficient assigned to the error rate
- QBER: Quantum Bit Error Rate
- log10(.): Logarithm with base 10

This equation ensures that the system does not focus solely on speed, but also gives the highest priority to physical security through mathematical penalties (β) applied under high error rates [5], [25]. This hybrid approach goes beyond classical methods by combining the pattern recognition capability of deep learning models with the decision-making ability of reinforcement learning [15], [30].

Training Process, Evaluation Criteria, and Performance Improvement: The methodology undergoes a rigorous training phase that begins with data collection from highprecision simulators that replicate realistic scenarios and continues with data preprocessing and cleaning steps to ensure modeling accuracy [15], [29]. The success of the methodology is evaluated using statistical metrics such as Mean Squared Error (MSE) and the Coefficient of Determination (R^2), in order to ensure that predictions align with the physical reality of the channel [7], [25].

The key difference that distinguishes this approach from classical solutions in the literature is its **selflearning capability** [21], [30]. While traditional systems fail once a critical error threshold (11%) is exceeded, our intelligent system dynamically recalibrates itself to prevent interruption [2], [13].

This provides high resilience and ensures security against Photon Number Splitting (PNS) attacks and environmental variations [24], [25]. Despite challenges such as the high computational cost of artificial intelligence, the added value it provides in terms of key stability and security makes this approach a technical necessity for future quantum communication networks [21], [30].

VII. SIMULATION RESULTS

This section presents a quantitative evaluation of the performance of the proposed system through a series of computer simulations [15], [29]. In this study, the effects of physical variables such as distance, channel noise, and signal loss on the Quantum Bit Error Rate (QBER) and Secret Key Rate (SKR), which are the main indicators of system security and efficiency, were measured [13], [25].

This analytical study is based on the theoretical foundations followed in the BB84 protocol literature [1], [9], and aims to provide a fundamental comparison between traditional systems and AI-supported systems [15], [16]. The obtained data demonstrate how AI optimization improves system stability, particularly in high-noise and long-distance scenarios [21], [30]. Furthermore, the simulation results were validated by comparing them with security limits reported in the literature (e.g., the 11% QBER threshold) [2], [7].

The simulation environment was designed to reflect realistic operational conditions [15], [29]. In this context, a standard fiber optic loss coefficient of 0.2 dB/km was assumed, and distance values in the range of 0–100 km were examined [16], [21]. To ensure the accuracy of the results, the system was tested by transmitting data blocks ranging from 10^5 to 10^6 bits under different noise levels [7], [25].

The methodology is based on two parallel scenarios: the first represents a conventional system with fixed parameters, while the second represents the proposed system, which uses an AI layer to analyze channel behavior and dynamically adjust transmission characteristics [13], [30]. This setup allows us to observe the ability of machine learning models to predict physical deviations and manage them before the key generation process collapses [23], [24]. The obtained simulation data demonstrate how the proposed intelligent system maintains security limits reported in the literature under varying channel conditions [5], [30].

The simulation results have shown a clear proportional relationship between increasing distance and the rise in QBER. This is a physically expected outcome due to increased photon scattering and signal attenuation over long distances [16], [25]. However, the AI-supported system demonstrated a clear advantage; while the conventional system rapidly loses stability as distance increases, the intelligent model manages to maintain relatively low and stable error rates [15], [30].

This improvement is attributed to the ability of neural networks to learn the “noise model” of the channel and make proactive adjustments at detection thresholds [29], [23]. In terms of Secure Key Rate (SKR), the results confirm that environmental noise is a major limiting factor for system efficiency [15], [30]. In conventional systems, increasing noise leads to a sharp and rapid decline in SKR, which can result in a complete halt of key generation at long distances [24], [25].

In contrast, the proposed system exhibited high resilience. By optimizing basis selection and adapting error correction algorithms to the current noise level, it maintained a stable key flow [13], [7]. This demonstrates that artificial intelligence not only improves performance but also extends the effective geographical range of quantum communication [21], [30].

The obtained results confirm that the integration of artificial intelligence into QKD systems represents a qualitative transition from “static” systems to “cognitive” systems [21], [30]. The ability of the proposed models to represent complex and nonlinear relationships within the quantum channel has enabled overcoming limitations arising from the physical constraints of the hardware [15], [29].

However, the discussion also shows that this advantage comes with a “computational cost”; training these models requires large datasets and high computational power. In addition, the accuracy of the results depends on the quality of the training data and the extent to which various attack and noise scenarios are covered [16], [25].

Despite these challenges, the final comparison favors the intelligent system, because it provides more sustainable security and offers a “self-healing” capability in sudden changes of the channel environment [13], [30]. The transition to this model reduces dependence on human intervention for system calibration and makes future quantum networks more

Independent and resilient against advanced eavesdropping attempts such as PNS attacks [24], [25].

As a result, the study demonstrates that investment in reinforcement learning and deep learning algorithms is not merely a complementary option, but a technical necessity to ensure the real-world efficiency of quantum cryptographic systems [15], [30].

VIII. RESULTS (CONCLUSION)

In this study, an artificial intelligence–based optimization approach is proposed to improve the performance of quantum key distribution (QKD) systems. The proposed method primarily aims to reduce the impact of factors such as noise, distance, and loss in quantum channels on system performance. In this context, QBER (Quantum Bit Error Rate) and SKR (Secure Key Rate) metrics are considered as the main performance indicators.

One of the main contributions of this study is the integration of artificial intelligence techniques into classical QKD systems, transforming the system from a static structure into a dynamic and adaptive one. In this way, the system can adapt to changing channel conditions in real time and optimize its performance. Simulation results show that the proposed AI-supported system achieves lower QBER values and higher SKR values compared to conventional QKD systems. In particular, under conditions of increasing distance and higher noise levels, the AI-based model is observed to minimize performance degradation by optimizing system parameters. This demonstrates that artificial intelligence is an effective optimization tool in quantum communication systems.

In addition, the machine learning and reinforcement learning approaches used in this study enable the system to learn channel conditions and make appropriate decisions accordingly. This contributes to more reliable and efficient operation of QKD systems.

However, the study also has some limitations. First, the performance of the proposed model largely depends on the quality and diversity of the training data. In addition, factors such as computational cost and processing delay in real-time applications may affect system performance. The results obtained in a simulation environment may differ in hardware-based real implementations.

The obtained simulation results show that the proposed AI-based approach significantly improves system performance. In particular, it is observed that QBER values tend to increase with distance; however, the AI-supported model limits this increase. The main reason for this is that machine learning algorithms learn channel conditions and perform optimal parameter tuning. As a result, the system exhibits a more flexible and adaptive structure compared to classical fixed-parameter approaches. Furthermore, in the SKR analysis, while a rapid decrease is observed in conventional systems as distance increases, the proposed method shows a slower decline and maintains higher key generation rates.

REFERENCES

[1]. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[2]. P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett., vol. 85, pp. 441–444, 2000.
[3]. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, pp. 145–195, 2002.
[4]. S. Pirandola et al., "Advances in quantum cryptography," Adv. Opt. Photon., vol. 12, pp. 1012– 1236, 2020.
[5]. R. Renner, "Security of quantum key distribution," Int. J. Quantum Inf., vol. 6, pp. 1–127, 2008.
[6]. D. Mayers, "Unconditional security in quantum cryptography," J. ACM, vol. 48, pp. 351–406, 2001.
[7]. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol. 67, no. 6, pp. 661–663, 1991.
[8]. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, pp. 802– 803, 1982.
[9]. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. Comput. Syst. Signal Process., 1984, pp. 175–179.
[10]. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., vol. 68, pp. 3121–3124, 1992.
[11]. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett., vol. 88, 057902, 2002.
[12]. P. Jouguet et al., "Experimental demonstration of long-distance CV-QKD," Nat. Photonics, vol. 7, pp. 378–381, 2013.
[13]. A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," Phys. Rev. Lett., vol. 114, p. 070501, 2015.
[14]. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett., vol. 108, 130503, 2012.
[15]. S. Pirandola et al., "High-rate measurementdevice-independent quantum cryptography," Nat. Photonics, vol. 9, pp. 397–402, 2015.
[16]. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett., vol. 94, p. 230504, 2005.
[17]. J. Yin et al., "Satellite-to-ground quantum key distribution," Nature, vol. 549, pp. 43–47, 2017.
[18]. H. Takesue et al., "Quantum key distribution over 40 dB channel loss," Nat. Photonics, vol. 1, pp. 343–348, 2007.
[19]. S. Wang et al., "Experimental quantum key distribution over 404 km of ultralow-loss fiber," Phys. Rev. Lett., vol. 125, p. 200502, 2020.
[20]. M. Peev et al., "The SECOQC quantum key distribution network in Vienna," New J. Phys., vol. 11, p. 075001, 2009.
[21]. H. J. Kimble, "The quantum internet," Nature, vol. 453, pp. 1023–1030, 2008.
[22]. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys., vol. 92, 025002, 2020.
[23]. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput., vol. 4, pp. 325–360, 2004.

[24]. L. Lydersen et al., "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photonics, vol. 4, pp. 686–689, 2010.
[25]. V. Scarani et al., "The security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, pp. 1301–1350, 2009.
[26]. M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nat. Commun., vol. 3, p. 634, 2012.
[27]. ID Quantique, Quantum Key Distribution Systems, White Paper, 2020.
[28]. ETSI GS QKD 014, Quantum Key Distribution (QKD); Protocol and Security Aspects, 2021.
[29]. C. Weedbrook et al., "Gaussian quantum information," Rev. Mod. Phys., vol. 84, pp. 621– 669, 2012.
[30]. M. Lucamarini et al., "Overcoming the ratedistance limit of quantum key distribution without quantum repeaters," Nature, vol. 557, pp. 400–403, 2018.
[31]. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge University Press.
[32]. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing.
[33]. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics.
[34]. Islam, T., Lim, C. C. W., Cahall, C., Kim, J., & Gauthier, D. J. (2017). Provably secure and high-rate quantum key distribution with time-bin encoding. Science Advances.
[35]. Bouchard, F., Heshami, K., England, D., Fickler, R., Boyd, R. W., Corkum, B. G., ... & Karimi, E. (2018). Experimental underwater quantum key distribution. Optics Express.
[36]. Mao, Y., Huang, W., Zhong, H., Wang, Y., Qin, H., Guo, Y., & Huang, D. (2020). Detecting quantum attacks: A machine learning based parameter estimation identification scheme for continuous-variable quantum key distribution. New Journal of Physics.