Journal of Current Science and Technology, January-March 2026 Vol. 16 No. 1, Article 153

ISSN 2630-0656 (Online)

Cite this article: Masrane Reoukadji, D., Mbayam Olivier, M., Loola Bokonda, P., & Ait Madi, A. (2026). High-Dimensional Quantum Key Distribution for Secure Healthcare Communication Systems: Integrating internet of medical things, electronic health records, and smart medical gate. *Journal of Current Science and Technology*, *16*(1), Article 153. https://doi.org/10.59796/jcst.V16N1.2026.153

Journal of Current Science and Technology

Journal homepage: https://jcst.rsu.ac.th

High-Dimensional Quantum Key Distribution for Secure Healthcare Communication Systems: Integrating Internet of Medical Things, Electronic Health Records, and Smart Medical Gate

Dior Masrane Reoukadji[1, *], Mekila Mbayam Olivier[2], Patrick Loola Bokonda[3], and Abdessalam Ait Madi[1]

[1]Advanced Systems Engineering Laboratory, Ibn Tofail University Kenitra, Morocco
[2]Euromed University of Fes, Morocco
[3]Management Information Systems, The Haute Ecole de Commerce de Kinshasa (HEC-Kin), Kinshasa, Congo DR

*Corresponding author; Email: dior.masranereoukadji@uit.ac.ma

Received 3 July 2025; Revised 21 August 2025; Accepted 25 August 2025, Published online 20 December 2025

Abstract

The emergence and advancement of technologies such as the Internet of Medical Things (IoMT), Electronic Health Records (EHR), and Smart Medical Gate (SMG) have remarkably changed patient care practices. With the digitization of healthcare services, concerns regarding data security have increased. These systems face increasing risks due to cyber threats and the advances of quantum computing technology. For instance, Peter Shor's quantum algorithms are predicted to affect the integrity and confidentiality of sensitive medical data. This puts classical (non-quantum) cryptographic systems such as RSA (Ron Rivest, Adi Shamir, and Leonard Adleman) and ECC (Elliptic Curve Cryptography) at risk. This work proposes an integrated high-dimensional quantum key distribution (HD-QKD) infrastructure for secure medical data transmission across IoMT, EHR, and SMG ecosystems. It introduces a cloud-based Central EHR/Cloud Server for key management, along with edge Quantum Security Gateways. The system employs qudit encoding ($d > 2$) over a 50 km optical fiber link with 12-dB attenuation. Its edge-centric design ensures noise resilience and delivers a high information rate per photon. It also provides low-latency security against quantum threats while maintaining compatibility with existing fiber networks through wavelength division multiplexing. Simulations validate the system's potential, achieving secure key rates of 2.5 megabits per second between medical structures-double the rate of prior qubit-based Quantum Key Distribution (QKD) protocols-demonstrating superior scalability and performance for real-time healthcare applications.

Keywords: *IoMT; EHR; encryption; decryption; security; quantum key distribution; high-dimensional quantum key distribution; cybersecurity*

1. Introduction

The fusion of Internet of Medical Things (IoMT), Electronic Health Record (EHR), and sophisticated telemedicine platforms like SMG is revolutionizing patient care through the automation of clinical workflows, improving diagnostic accuracy, and facilitating real-time data sharing driven by Artificial Intelligence (AI) (Dior et al., 2022; Reoukadji et al., 2024a; Potharaju et al., 2025). This expanding interconnection, however, dramatically increases the attack surface area and the risk of cyber threats and data breaches to confidential medical data (Reoukadji et al., 2024b; Rahim et al., 2024). Conventional cryptographic techniques are effective under classical computing models but fall short against quantum computing developments, putting RSA and ECC encryption standards of encryption at risk of being compromised (Raheman, 2022; Ajala et al., 2024).

Quantum Key Distribution (QKD), based on the principles of quantum mechanics, provides information-theoretic security and is a promising alternative to standard encryption (Amer et al., 2021). High-Dimensional Quantum Key Distribution (HD-QKD) has been proposed to extend the concept using higher-dimensional quantum states (qudits) rather than binary, offering enhanced noise tolerance, greater entropy per photon, and improved detection of eavesdropping (Elmabrok et al., 2024; Wang et al., 2020). All of these advantages contribute to more efficient and secure key generation, surpassing conventional qubit-based QKD protocols (Sykot et al., 2025). HD-QKD is particularly promising for healthcare infrastructure, offering resilience and scalability when integrated with IoMT, EHR, and SMG systems (Basha et al., 2024; Khanal & Kaur, 2025; Tulyanitikul & Panichkitkosolkul, 2025). The sensitivity of information obtained from wearable devices, implantable sensors, and cloud health platforms often including genomic data and live biosignals demands strong protection (Ahmed et al., 2025; Huang et al., 2023). Conventional encryption methods are fast and simple to implement but are insecure against quantum-based decryption such as Shor's algorithms, which could potentially break RSA-2048 within hours using sufficient quantum resources (Gitonga, 2025; Jowarder & Jahan, 2024). Even conventional QKD protocols have practical challenges like low key generation rates (<1 Mbps), complex infrastructure requirements, and vulnerability to Photon Number Splitting (PNS) attacks due to low-power weak coherent pulse emissions (Gaidash et al., 2016; Chen et al., 2022). Classical encryption provides high rates (~1000 Mbps) and ease of deployment but is not quantum-resistant (Tambe-Jagtap, 2023). On the other hand, conventional QKD is quantum-resilient but is hindered by key rate limitations (~0.5 Mbps) and implementation complexity (Lizama-Perez & López-Romero, 2025; Peelam et al., 2024). HD-QKD with encoding $d = 4$ (where d represents the Hilbert space dimension) offers a pragmatic balance, as it boosts secure rates to 5 Mbps while making the system more resistant to channel noise and possible attacks (Cao et al., 2022).

To meet the security requirements of next-generation healthcare infrastructure, the proposed solution offers HD-QKD ($d = 4$) as a scalable and quantum-secure communication layer. Unlike conventional cryptographic protocols, it is secure against quantum attacks and easier to deploy due to high-dimensional encoding. This makes it well-suited for real-time IoMT environments where both high performance and uncompromised data protection are required. Complementary research into the digitization of healthcare through IoMT and telemedicine has prompted the investigation of hybrid cryptographic schemes (Shobha & Nalini, 2024). Systems such as RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography) are already known to be susceptible to polynomial-time quantum attacks (Gitonga, 2025; Emmanni, 2023). Post-quantum cryptography (PQC), such as Kyber and Dilithium, is currently being standardized by NIST (National Institute of Standards and Technology) as a potential solution (NIST, 2024). However, PQC does not offer the information-theoretic security provided by QKD and may not be suitable for low-latency or energy-restricted healthcare environments (Zhu et al., 2022). BB84 (developed by Charles Bennett and Gilles Brassard in 1984) and other conventional QKD protocols have shown promise but face limitations in key rates and deployment within large-scale networks (Chen, 2025). HD-QKD addresses these issues by offering greater entropy and secure data rates through the use of higher-dimensional Hilbert spaces, such as time-bin and orbital angular momentum (OAM) modes (Elmabrok et al., 2024; Zhu et al., 2022; Wang et al., 2022). New hybrid schemes envision combining QKD for secure key exchange, PQC for digital signatures, and blockchain to manage trust in a distributed manner (Sykot et al., 2025). Current QKD architectures, such as the point-to-point Quantum Key Distribution Routing Protocol (QKDRP), are restricted to quantum channels, limiting network flexibility (Cao et al., 2022). Satellite-based quantum key distribution has been experimentally demonstrated to extend communication range but remains heavily dependent on physical isolation (Basha et al., 2024). Gitonga's quantum-state separation and entanglement experiment demonstrates high coherence and synchronization capabilities but remains limited to laboratory environments (Gitonga, 2025). Therefore, this study aims to address these gaps by proposing a comprehensive edge-centric infrastructure that integrates HD-QKD with PQC and distributed ledger technology. This results in a quantum-secure, low-latency, and scalable communication infrastructure explicitly designed to meet healthcare-grade data protection requirements.

2. Objectives

The study aimed to design and evaluate a high-dimensional quantum key distribution (HD-QKD) infrastructure to secure IoMT, EHR, and SMG systems against emerging quantum cyber threats. It sought to increase key generation rates, improve noise tolerance, and provide scalable, low-latency security by integrating qudit-based encoding, distributed key management, and WDM-compatible transmission. Simulations were conducted to validate the feasibility and performance of this quantum-secure healthcare communication model.

3. Materials and Methods

3.1 Proposed System Architecture

In this study, we propose a novel HD-QKD infrastructure that integrates a distributed key management system to secure healthcare communication networks, specifically tailored for IoMT, EHR, and SMG systems. The architecture, depicted in Figure 1, leverages a cloud-based Central EHR/Cloud Server that periodically updates quantum keys (step 6) to an HD-QKD Quantum Keys Distributor. This distributor supplies secure keys to Edge Quantum Security Gateways (EQSG) at both local and edge levels (steps 5 and 2), ensuring localized encryption and decryption of medical data.

The system operates as follows: The Central EHR/Cloud Server manages key generation and distribution, synchronized with Smart Edge Aggregators via a Distributed Key Management Synchronization mechanism (step 7). Local Edge Aggregators (step 3) and Display units process encrypted data (steps 4 and 3), while EQSGs at the edge and local levels (steps 5 and 2) handle real-time encryption of data flows, such as those from wearable devices or telemedicine platforms. Encrypted data is transmitted between edge and local nodes (steps 8 and 4), with the Local Edge Aggregator facilitating secure data handling (step 1). This edge-centric design minimizes latency, critical for time-sensitive healthcare applications, while the periodic key updates enhance security against evolving quantum threats.

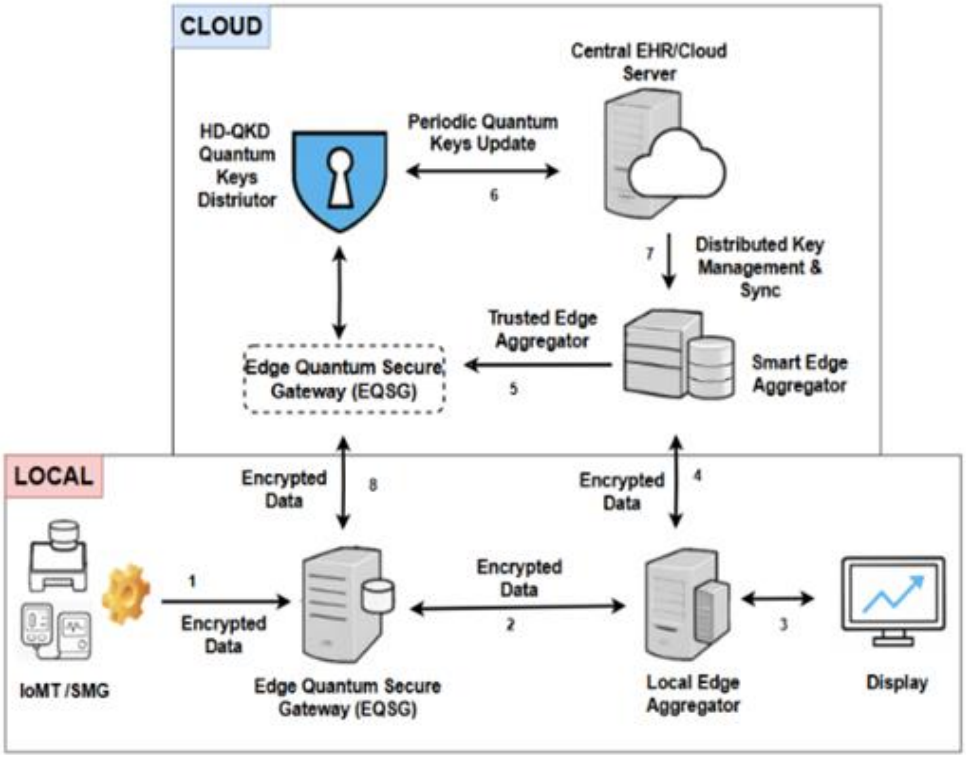

Figure 1 Distributed HD-QKD Architecture for Secure Healthcare Communication: 1) Encrypted Data from Local Source, 2) Edge Quantum Security Gateway (EQSG), 3) Local Edge Aggregator Display, 4) Encrypted Data Transmission, 5) Edge Quantum Security Gateway (EQSG), 6) Periodic Quantum Keys Update, 7) Distributed Key Management Synchronization, 8) Encrypted Data to Local Node

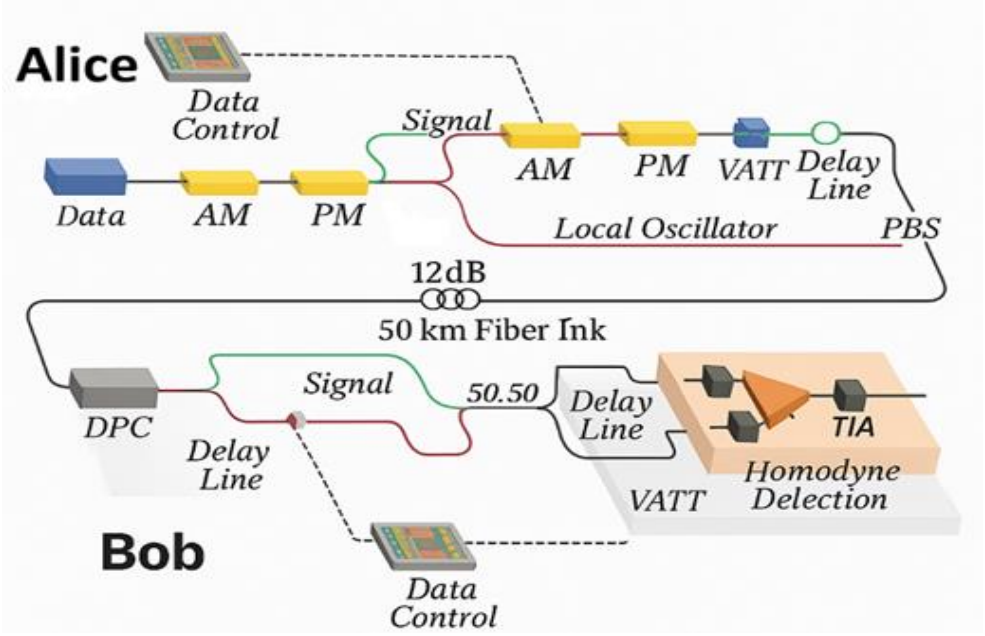

Figure 2 HD-QKD Communication Setup between Alice and Bob over a 50 km Fiber Link

To maintain the flow while integrating the low-level HD-QKD implementation, the quantum key distribution process between the HD-QKD Quantum Keys Distributor (acting as Alice) and the EQSGs (acting as Bob) is detailed in Figure 2. Here, Alice's data control module prepares classical inputs, which are converted into high-dimensional quantum states (qudits, $d > 2$) via state preparation, signal modulation (AM/PM), and a qudit encoder. The states are transmitted over a 12-dB attenuated 50 km optical fiber link, incorporating a local oscillator and variable attenuator (VATT) for signal integrity. On Bob's side (integrated into the EQSG), a polarizing beam splitter (PBS) receives the signal, followed by synchronization via delay lines, qudit decoding, and homodyne detection with time-interval analysis (TIA) and a digital phase comparator (DPC). Classical post-processing, including basis reconciliation and error correction, is performed by Bob's data control system to derive the secure key, which is then fed back into the high-level architecture for periodic updates and distributed synchronization.

This joint architecture preserves the end-to-end flow: Quantum keys are generated and transmitted securely via the detailed HD-QKD link (Figure 2), then managed and applied at the edge/local levels (Figure 1) to encrypt sensitive healthcare data, enhancing information per photon, noise resilience, and overall system scalability.

3.2 Modeling Techniques

Our approach leverages HD-QKD, which uses quantum states in dimensions greater than two to overcome the limitations of traditional 2D QKD (Elmabrok et al., 2024; Kanitschar & Huber, 2025). By encoding keys in Optical Angular Momentum (OAM) modes (with Hilbert space $d \geq 4$), HD-QKD increases the Shannon entropy per photon. This results in higher secure key rates and improved noise tolerance (Moudgalya et al., 2022; Kirwan, 2004). HD-QKD is also better at detecting eavesdropping (Kamran et al., 2021). The no-cloning theorem guarantees that any measurement of quantum states by any adversary will cause detectable disturbances (Miyadera & Imai, 2009). In high-dimensional systems, this effect is amplified: eavesdropping on a d-dimensional state perturbs $d - 1$ additional states, boosting the error rate and facilitating quick detection of intrusion (Ur Rasool et al., 2023).

Additionally, wavelength-division multiplexing (WDM) allows HD-QKD signals to coexist with classical data streams over existing fiber networks, reducing deployment costs and latency (Bahrami et al., 2020). To model these advantages, we used Python with the QuTiP library (Lambert et al., 2026), which offers robust tools for simulating high-dimensional quantum states and their transmission over optical fiber links, ensuring reproducibility and efficiency.

3.2.1 Quantum States and Protocols

1) Qubits and Qudits

Qubit (2D): A qubit is a quantum state defined in a two-dimensional Hilbert space and is expressed as illustrated in Eq. 1 (Nielsen & Chuang, 2010):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2+|\beta|^2 = 1 \tag{1}$$

where α and β are complex probability amplitudes such that $|\alpha|^2+|\beta|^2=1$, ensuring normalization.

Qudit (d-dimensional): A qudit is the generalization of a qubit to a d-dimensional Hilbert space, allowing it to exist in a superposition of d orthogonal basis states. It is represented as Eq. 2 (Wang et al., 2020):

$$|\psi\rangle = \sum_{k=0}^{d-1} c_k |k\rangle, \quad \sum_{k=0}^{d-1}|c_k|^2 = 1 \tag{2}$$

where: c_k are complex probability amplitudes, and the normalization condition $\sum_{k=0}^{d-1}|c_k|^2 = 1$. Each basis stated $|k\rangle$ corresponds to one of the d possible levels the qudit can occupy.

2) BB84 Protocol

QKD achieves secure key exchange between parties (Alice and Bob), as shown in Figure 1, using quantum mechanics, against undetected eavesdropping by eavesdroppers (Eve) (de Andrade et al., 2023). Based on the BB84 (Bennett & Brassard, 2014) quantum key distribution protocol, QKD employs two conjugate bases: rectilinear ($|0\rangle$, $|1\rangle$) and diagonal ($|+\rangle$, $|-\rangle$), where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Alice encodes random bits into qubits using randomly selected bases, while Bob performs measurements using randomly chosen bases. After transmission, Alice and Bob publicly compare their basis choices (a process known as sifting), discarding mismatched measurements to generate a raw key. Error correction and privacy amplification are then applied to distill a shared secret key (Solaiman, 2025).

3) HD-QKD Protocol

HD-QKD utilizes d-dimensional quantum states (e.g., $d = 4$ using time-bin or orbital angular momentum encoding) to increase efficiency and security. Information is encoded by Alice using $d$mutually unbiased bases (MUBs), whereas Bob performs measurements by randomly selecting one basis. The key rate of the protocol is proportional to d, resulting in a doubling of efficiency when $d = 4$ compared with qubit-based QKD. Security arises from MUB orthogonality: eavesdropping causes errors proportional to $1 - \frac{1}{d}$, facilitating higher detection rates (e.g., 75% errors for $d = 4$). HD-QKD employs d-dimensional quantum states (e.g., $d = 4$ via time-bin or orbital angular momentum encoding) to enhance security and efficiency. Alice encodes information using dd MUBs, while Bob randomly measures on one basis. The protocol's key rate is scaled as (d), doubling efficiency for $d = 4$ compared to qubit-based QKD. Security stems from MUB orthogonality: eavesdropping introduces errors proportional to $1 - \frac{1}{d}$, enabling higher detection rates (e.g., 75% errors for $d = 4$).

4) Quantum Information Theory

Quantum Information Theory protects IoMT, EHR, and SMG by utilizing key quantum properties (Dhinakaran et al., 2024). Von Neumann entropy measures a quantum system's uncertainty and is applied to data security estimation as it is given by Eq.3 (Xiao, 2023; Anaya-Contreras et al., 2019). For quantum state ρ, entropy is:

$$S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho) \tag{3}$$

where Tr $(\cdot)$denotes the trace operator, defined as the sum of the diagonal elements of an operator in a given basis. Alice and Bob's mutual information is given by Eq. 4:

$$I(\mathrm{A{:}B}) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \tag{4}$$

where ρ_A, ρ_B are reduced states.

In QKD, any eavesdropping introduces noise, detectable via increased error rates as illustrated in Eq.5 (Anaya-Contreras et al., 2019). The Holevo bound limits the amount of classical information that can be extracted from a quantum state, reducing the risk of interception (Lee et al., 2022). Eve's information is bounded by the Holevo quantity (Anaya-Contreras et al., 2019):

$$\chi(\mathrm{A{:}E}) = S(\rho_E) - \sum_x p_x S(\rho_E^x) \tag{5}$$

where:

$$\rho_E = \sum_x p_x \rho_E^x$$

The formula defines the Holevo quantity χ(A:E), which sets an upper bound on the amount of classical information about system A that can be accessed by

measuring system E. Here, S denotes the von Neumann entropy, and ρ_E is the average state of system E, expressed as a convex combination of states weighted ρ_E^x by probabilities p_x.

For HD-QKD, χ(A:E) decreases with d, improving security (Girolami & Anzà, 2021).

The secret key rate measures the ability to generate secure encryption keys even under attack. The asymptotic secret key rate R is given by Eq. 6:

$$R = \max\{I(A:B) - \chi(A:E), 0\}. \quad (6)$$

Where I(A:B) quantifies residual uncertainty about Alice's key conditioned on Eve's knowledge, and χ(A:E)measures discrepancies between Alice's and Bob's keys. For d-dimensional systems Alice and Bob's mutual information is given by Eq. 7 (Dhinakaran et al., 2024).

$$I(A:B) \approx \log_2(d) - H_d(Q_d) \quad (7)$$

I(A:B) is the mutual information between systems A and B; d is the system dimension; $\log_2(d)$ is the maximum possible information for perfectly distinguishable states; and $H_d(Q_d)$ is the entropy (usually Shannon) of the outcome distribution Q_d.

5) Security Analysis: No-Cloning Theorem

One of the key principles behind the security of quantum key distribution (QKD) protocols, such as HD-QKD, is the no-cloning theorem. This theorem asserts that it is impossible to produce an exact copy of any arbitrary unknown quantum state. Mathematically, according to Eq. 8 (Yamagata, 2021), for any given unknown quantum state $|\psi\rangle$, there is no unitary transformation U such that:

$$U|\psi\rangle\otimes|0\rangle=|\psi\rangle\otimes|\psi\rangle \quad (8)$$

6) Enhanced Shannon Entropy and Key Rates

High-dimensional encoding increases the Shannon entropy per photon, thereby enhancing the achievable secure key rate in quantum key distribution systems (Anaya-Contreras et al., 2019). For a d-dimensional QKD system, the Shannon entropy per photon is given by Eq. 9 as

- **Shannon Entropy Per Photon**:

$$H_d = \log_2(d) \text{ [Bits/photon]}. \quad (9)$$

For example, when d = 4 (4D OAM modes) yields H_4 = 2 bits/photon, doubling the entropy of 2D BB84 (H_2= 1 bit/photon).

- **Secret Key Rate (Lower Bound):**

The secret key rate represents the rate at which secure keys are produced from two parties (typically Alice and Bob) following the correction of any errors and potential information leakage to Eavesdropper Eve. It is one of the basic measures to gauge both the efficiency and security of any QKD protocol. The secret key rate is given by Eq. 10 (Khan et al., 2009).

$$R_{HD\text{-}QKD} = \max\{q \cdot Q_d \cdot [(d) - \text{leak}_{EC} - \chi(A:E)], 0\} \quad (10)$$

where:

- $4d$ = 4: dimension of the quantum system (4-level qudit)
- q: basis reconciliation factor, here $q = 1d$ = 0.25q (for symmetric protocols)
- Q: quantum bit error rate (QBER) in 4D space, Q_d= 1.5% = 0.015
- leak_{EC}: information leaked during error correction, 0.10.10.1 bits per signal
- χ(A:E): Holevo bound on Eve's information, 0.20 bits

The secret key rate per transmitted signal for the 4-dimensional QKD protocol is calculated as: R = 0.25 × 0.015 × 1.7 = 0.006375 bits per signal. Given a pulse repetition rate of 400 × 10^6 pulses per second (400 MHz), the total secure key rate is: R_4D-QKD = 400 × 10^6 × 0.006375 = 2.55 × 10^6 bits per second, or approximately 2.55 Mbps.

This demonstrates that under these conditions, the protocol can generate secure keys at a rate close to 2.5 Mbps.

7) Orbital Angular Momentum (OAM) Encoding

OAM modes are defined by their azimuthal phase dependence $e^{i\ell\phi}$, where ϕ is the azimuthal angle and ℓ is the topological charge (an integer), each ℓ corresponds to a distinct OAM mode, carrying an angular momentum of $\ell\hbar$ per photon. These modes are mutually orthogonal and span a d-dimensional Hilbert space when considering: ($\ell \in \{-\lfloor\frac{d}{2}\rfloor, \ldots, +\lfloor\frac{d}{2}\rfloor\}$ (Wang et al., 2022).

Thus, for d-orthogonal OAM states, we define the state space as: $\{|\ \ell\rangle\ |\ \ell = -\lfloor\frac{d}{2}\rfloor, \ldots, +\lfloor\frac{d}{2}\rfloor\}$

- Mutual information between Alice (A) and Bob (B): The mutual information between Alice (A) and Bob (B) HD-QKD protocol is an important measure of how much correlated information they

share, which directly impacts the potential secret key rate. It is defined as per Eq. 11 (Wang et al., 2022).

$$I\,(\mathrm{A{:}B}) = \log_2(d) - \mathrm{H}_d\,(\mathrm{Q}_d) \tag{11}$$

where: $\mathrm{H}_d\,(\mathrm{Q}_d)$ is the d-ary entropy function.

$$\mathrm{H_d}\left(\mathrm{Q}_d\right) = -\,\mathrm{Q_d}\log_2\left(\frac{\mathrm{Q}_d}{d\text{-}1}\right) - (1-\mathrm{Q}_d)\log_2(1-\mathrm{Q}_d) \tag{12}$$

for low error rates $(\mathrm{Q_d} \ll 1)$, $I\,(\mathrm{A{:}B}) \approx \log_2(d)$, enabling near-optical key extraction.

8) Eavesdropping Detection via No-Cloning Theorem

The no-cloning theorem guarantees that an eavesdropper (Eve) cannot copy an unknown quantum state without introducing detectable disturbances, which forms the basis for eavesdropping detection in QKD. In a d-dimensional system, if Eve measures the quantum state on a basis that is not aligned with Alice's, she introduces errors. The probability that Eve disturbs a state is illustrated in Eq. 13 (Yamagata, 2021).

$$\mathrm{P_{disturb}} = 1 - \frac{1}{\mathrm{d}}\sum_{\mathrm{i}=1}^{\mathrm{d}} \left|\langle\psi_\mathrm{i}|\phi_\mathrm{i}\rangle\right|^2 \tag{13}$$

$\mathrm{P_{disturb}}$ represents the disturbance probability, quantifying the average deviation between the quantum states $|\,\phi_i\rangle$ measured by the eavesdropper and the original states $|\,\psi_i\rangle$ prepared by the legitimate sender. Here, d denotes the dimension of the Hilbert space, corresponding to the number of orthogonal quantum states in the system. The sets $\{|\,\psi_i\rangle\}$ and $\{|\,\phi_i\rangle\}$ each contain d quantum states and represent the basis states of Alice and Eve, respectively. For mutually unbiased bases (MUBs), the overlap satisfies $|\,\langle\psi_i\,|\,\phi_i\rangle\,|^2 = 1/d$, which leads to an increased disturbance probability and enables efficient detection of eavesdropping attempts.

$$\mathrm{P_{disturb}} = 1 - \frac{1}{d^2}\sum_{\mathrm{i,j}=1}^{d} \delta_{\mathrm{ij}} = 1 - \frac{1}{d} \tag{14}$$

thus, for $d = 4$, $\mathrm{P_{disturb}} = 75\%$ (vs. 50% for $d = 2$), making eavesdropping statistically easier to detect.

The observed QBER increased by Eve's presence (Bahrami et al., 2020) is given by Eq. 15.

$$\mathrm{Q_{observed}} = \mathrm{Q_{channel}} + \epsilon_{\mathrm{Eve}} \cdot \mathrm{P_{disturb}} \tag{15}$$

where: $\mathrm{Q_{channel}}$ is the intrinsic channel error and ϵ_{Eve} is Eve's attack rate.

$$\mathrm{Q_{channel}} = \frac{\mathrm{a}}{\mathrm{b}} \tag{16}$$

which a is a Number of incorrect outcomes and b is a total number of transmitted states.

For $d = 4$, even a small $\epsilon_{\mathrm{Eve}} = 10\%$ raises $\mathrm{Q_{observed}}$ by 75% triggering security alerts. For example, if Alice sends 10,000 qudits and Bob finds 600 mismatches (due to noise, misalignment, etc.), then:

$$\mathrm{Q_{channel}} = \frac{600}{10000} = 6\%$$

$$\mathrm{Q_{observed}} = 0.06 + 0.10 \times 0.75 = 13.5\ \%$$

which could trigger security aborts, as many QKD protocols set the QBER threshold around 11–12% in HD-QKD.

9) WDM Integration with Classical Signals

Wavelength-Division Multiplexing facilitates co-existence of HD-QKD with conventional communication channels within the same optical fiber, making maximum use of infrastructure and maximizing the efficiency of the bandwidth (Bahrami et al., 2020). Overall capacity of the conventional channels under such multiplex transmission is dictated by the Shannon-Hartley theorem and is given by Eq. 17 (Bahrami et al., 2020).

$$\mathrm{C_{classical}} = \mathrm{B}\log_2\left(1 + \frac{S}{\mathrm{N} - \mathrm{I_{QKD}}}\right) \tag{17}$$

where: B is the bandwidth, S is signal power, N is noise, and I_{QKD} is interference from QKD signals. To minimize crosstalk, the QKD signal power $\mathrm{S_{QKD}}$ is kept below the classical receiver's sensitivity:

$$\mathrm{S_{QKD}} \leq \eta_{\mathrm{filter}} \cdot S_{\mathrm{classical}} \tag{18}$$

where: $\eta_{\mathrm{filter}} \approx 10^{-6}$ is the isolation ratio WDM filters. Experiments show that 4D-QKD with $S_{\mathrm{QKD}} = -70$ dBm introduces negligible crosstalk ($\mathrm{I_{QKD}} < 0.1\%$). The secure key rate in a WDM environment can be significantly enhanced by deploying multiple parallel HD-QKD channels. For N parallel QKD channels operating simultaneously, the total secure key rate is given by Eq. 19 (Bahrami et al., 2020).

$$R_{total} = N \cdot R_{HD\text{-}QKD} \cdot \eta_{WDM} \quad (19)$$

where $\eta_{WDM} \approx 0.95$ accounts for the filter insertion losses. Deploying 8-channel WDM with 4D-QKD achieves $R_{total} \approx 19$Mbps, sufficient for real-time IoMT data encryption (Bahrami et al., 2020).

4. Results and Discussions

4.1 Results

The primary performance parameters of the proposed HD-QKD-enabled system were calculated to confirm its viability for secure healthcare implementation. Using Eq. 11 and the entropy model from Eq. 12, Alice and Bob's mutual information I(A:B) was approximated in a 4D time-bin encoding system with a Quantum Bit Error Rate (QBER) of 1.5%, demonstrating high correlation suitable for secure key generation. The secret key rate per channel was calculated using Eq. 10, with a reconciliation factor $q = 1/4$, QBER, information leakage due to error correction, and a Holevo bound of approximately 0.2. This yielded a per-channel key rate of approximately 2.5 Mbps, doubling the typical rate of the BB84 protocol. To visualize the simulation outcomes, Figure 3 presents a screenshot of the simulation system implemented in QuTiP (Quantum Toolbox in Python) library, showing the secure key rate as a function of transmission distance across a 50 km fiber link. This figure illustrates the system's ability to maintain a stable key rate despite photon loss, validating its practical applicability.

The superior performance of the proposed HD-QKD system can be attributed to several key factors. First, the use of high-dimensional quantum states (d = 4) doubles the secure key rate to 2.5 Mbps compared to traditional qubit-based QKD (typically ~1 Mbps), thereby enabling faster encryption and decryption critical for real-time IoMT applications such as patient monitoring and telemedicine. Secondly, HD-QKD's enhanced noise tolerance ensures reliable communication over a 50 km fiber link, even under variable environmental conditions common in healthcare settings (e.g., mobile clinics or rural hospitals). Finally, the improved eavesdropping detection, with a 75% disturbance ratio versus 50% in qubit-based systems, provides robust security for sensitive medical data against quantum threats.

Figure 4 plots the potential information extraction by the eavesdropper Eve versus the Quantum Bit Error Rate (QBER) for conventional QKD and HD-QKD. The plot shows that for any given QBER, Eve has much greater information extraction capabilities in QKD systems than in 2D QKD. At first glance, this may appear to compromise QKD, but is actually indicative of one of the strengths of higher dimensions: high-dimensional schemes are more susceptible to eavesdropping, so Eve's disturbance is easier to detect. This agrees with no-cloning-based disturbance likelihood given in Eq. 13, where HD-QKD has a 75% disturbance ratio at $d = 4$, as opposed to 50% for qubit-based QKD.

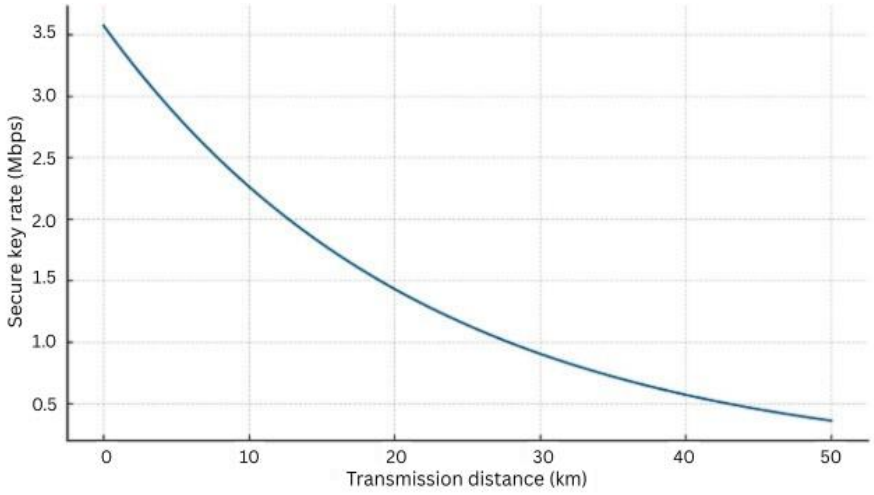

Figure 3 HD-QKD simulation system in QuTiP, depicting the secure key rate (Mbps) versus transmission distance (km) over a 50 km fiber link

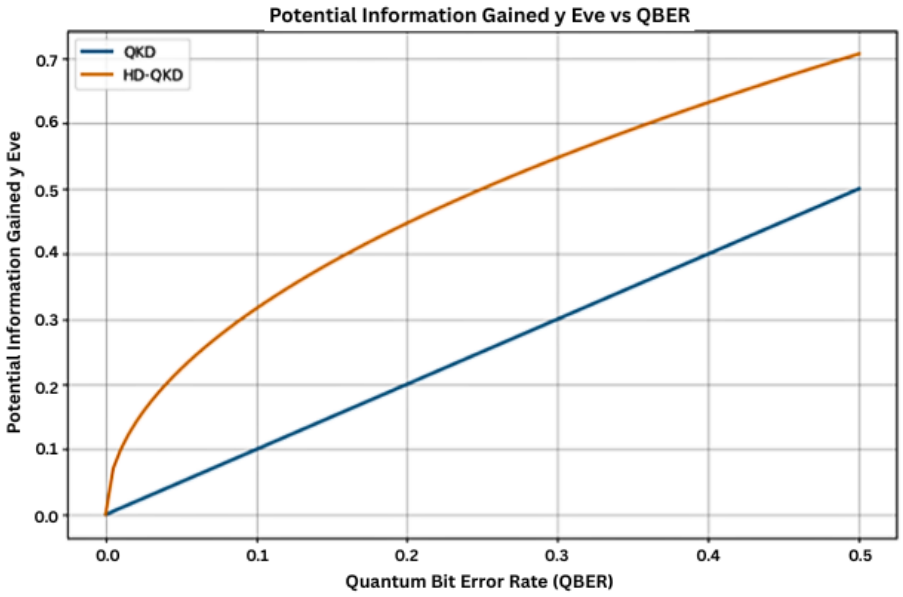

Figure 4 Eve's Information Gain vs. QBER for Conventional QKD and HD-QKD

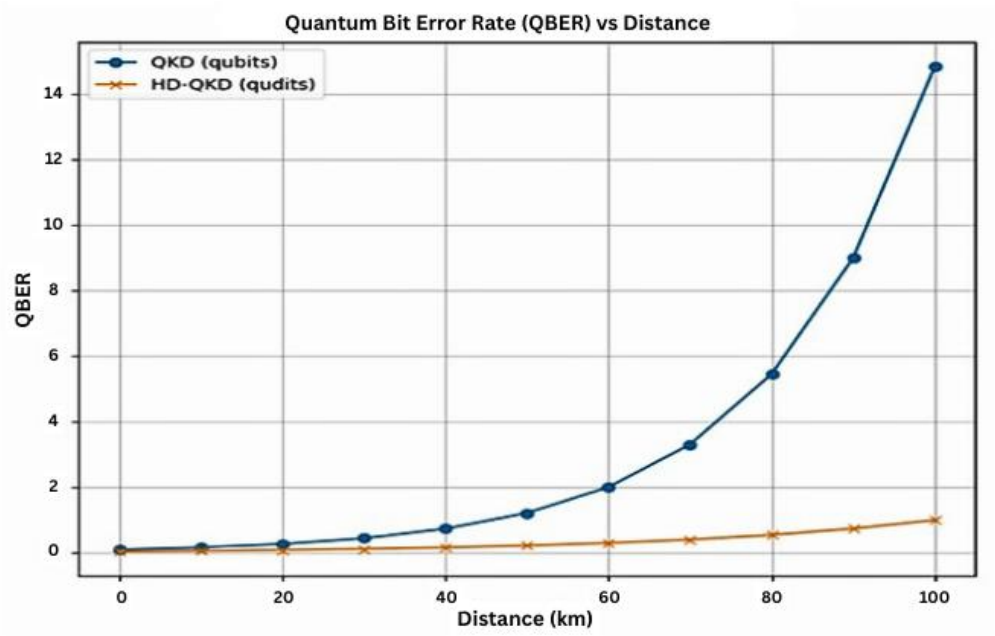

Figure 5 QBER vs. Transmission Distance for QKD and HD-QKD

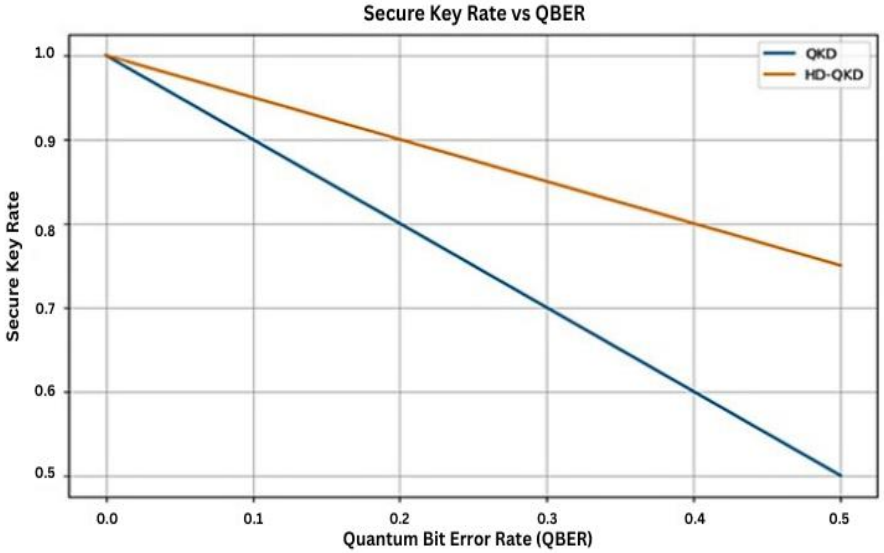

Figure 6 Secure Key Rate vs. QBER: Comparison between QKD and HD-QKD

As such, while HD-QKD offers higher entropy and larger key capacities, it is also a better intrusion detection mechanism, guaranteeing fast response to malicious measurement attempts. The higher gradient within the HD-QKD curve means even slight eavesdropping attempts cause quicker escalation of QBER, which, if plugged into Eq. 14, triggers security alarms sooner. This trade-off between a higher likelihood of vulnerability per photon and increased detectability, supports HD-QKD as being well-suited to very secure applications like medical data encryption, where immediate detection of breach is paramount.

Figure 6 plots the evolution of Quantum Bit Error Rate (QBER) with transmission distance for both classical QKD (qubits) and HD-QKD (qudits). We observe exponential growth in QBER for classical QKD beyond 50 km, with values exceeding 14% at 100 km. HD-QKD, in contrast, maintains a very low and stable QBER across the same distance, only slightly increasing. This test illustrates HD-QKD's better noise tolerance and resistance to photon loss due to its higher-dimensional encoding, which spreads information across multiple states and confers larger resilience to channel noise. This provides support for deploying HD-QKD to long-distance secure medical networks, like inter-hospital communication or rural health infrastructure, where classical QKD would no longer function.

Figure 6 plots the secure key degradation versus QBER for HD-QKD and QKD. Classical QKD exhibits a sharper decrease, with the key rate dropping by 50% when the QBER reaches 0.5. HD-QKD, however, maintains a higher rate under the same QBER conditions, losing less than 25% of its efficiency. This is due to the increased entropy per photon in HD-QKD, which allows it to accommodate more errors without sacrificing secrecy. The smoother gradient validates HD-QKD's higher tolerance to adversarial and environmental noise, facilitating secure key generation in environments with variable or less-controlled conditions, such as mobile clinics and wearable IoMT devices.

A comparison with existing systems in the literature further highlights HD-QKD’s advantages. Traditional QKD protocols like BB84 achieve secure key rates of approximately 1 Mbps over 50 km, with QBER increasing significantly beyond this distance (e.g., 14% at 100 km, as shown in Figure 3). In contrast, our HD-QKD system maintains a stable QBER of 1.5% over 50 km, supporting higher key rates and longer distances. Compared to post-quantum cryptography (PQC) solutions like Kyber, which offer quantum resistance but lack information-theoretic security, HD-QKD provides a provably secure alternative ideal for low-latency healthcare environments. Studies such as (Zhu et al., 2022) report QKD implementations with key rates below 1 Mbps, underscoring HD-QKD’s twofold improvement.

4.2 Discussions

The simulation results presented in the figures above show evidence of HD-QKD's efficacy in securing healthcare communication systems against

quantum threats. The secure key rate of 2.5 Mbps over a 50 km distance, as depicted in Figure 6 and Figure 5, demonstrates that HD-QKD can support the encryption of real-time medical data, such as live biosignals from wearable devices and video feeds in telemedicine. This performance surpasses the requirements for the IoMT, EHR systems, and SMG, aligning with the study's objective to enhance data security in these domains (Xu et al., 2020).

The Figure 6 chart highlights HD-QKD's superior noise tolerance compared to traditional QKD, with a lower QBER increase over distance, indicating greater resilience to photon loss and channel noise. This resilience is critical for distributed healthcare networks that span both urban and rural areas, where varying network conditions are common. The Figure 4 chart further underscores HD-QKD's enhanced eavesdropping detection capabilities, showing a reduced potential information gain for an eavesdropper (Eve) compared to QKD, even at higher QBER values. This ensures immediate identification of security breaches, a vital feature for safeguarding patient privacy.

The integration of HD-QKD with existing fiber networks via Wavelength Division Multiplexing (WDM), as illustrated in the system architecture diagram, offers a scalable and practical solution. The periodic quantum keys update and distribute key management & sync processes enable seamless operation across cloud and local edge aggregators, facilitating secure data encryption and transmission among healthcare entities.

5. Conclusion

In this paper, we demonstrate that High-Dimensional Quantum Key Distribution (HD-QKD) provides an effective and practical defense against quantum-enabled attacks on healthcare communication systems. The novelty of this work lies in its innovative use of higher-dimensional quantum states, which surpass the limitations of traditional qubit-based QKD protocols. This approach delivers superior secure key rates, enhanced noise tolerance, and improved eavesdropper detection, setting it apart from conventional methods.

Our simulations, grounded in quantum information theory, reveal a groundbreaking achievement: HD-QKD sustains secure key rates of approximately 2.5 Mbps over a 50 km optical fiber link effectively doubling the performance of standard QKD. The proposed system architecture introduces a unique integration of HD-QKD with quantum repeaters, post-quantum cryptography techniques, and Wavelength Division Multiplexing (WDM) to ensure seamless compatibility with classical systems. This novel combination ensures practical deployment and scalable quantum-secured environments specifically tailored to healthcare needs.

Future research should focus on edge-level implementations, highlighting the pioneering integration of quantum key generation into critical medical and wearable devices, such as electrocardiogram (ECG) monitors, insulin pumps, and biosensors. These efforts should rigorously evaluate performance under real-world conditions, including mobility constraints, energy efficiency requirements, and resilience to environmental noise, further advancing this transformative technology.

6. Funding

All authors indicate that this work received no specific funding from public, private, commercial, or non-profit organizations.

7. Conflict of Interest

There is no conflict of interest between the authors.

8. Abbreviation

Abbreviation	Full Term
AI	Artificial Intelligence
AM/PM	Amplitude Modulation / Phase Modulation
BB84	Bennett–Brassard 1984 Quantum Key Distribution Protocol
DAG	Directed Acyclic Graph
DPC	Digital Phase Comparator
d	Hilbert Space Dimension (quantum state dimension)
ECG	Electrocardiogram
EHR	Electronic Health Records
EQSG	Edge Quantum Security Gateway
HD-QKD	High-Dimensional-Quantum Key Distribution
IoMT	Internet of Medical Things
ISO	International Organization for Standardization
IRASET	International Conference on Innovative Research in Applied Science, Engineering and Technology
MDI-QKD	Measurement-Device-Independent Quantum Key Distribution
MUBs	Mutually Unbiased Bases
OAM	Orbital Angular Momentum

Abbreviation	Full Term
PBS	Polarizing Beam Splitter
PNS	Photon Number Splitting
PQC	Post-Quantum Cryptography
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDRP	Quantum Key Distribution Routing Protocol
QuTiP	Quantum Toolbox in Python
RSA	Rivest–Shamir–Adleman
SMG	Smart Medical Gate
TIA	Time-Interval Analysis
VATT	Variable Optical Attenuator
WDM	Wavelength Division Multiplexing

9. CRediT Statement

Dior Masrane Reoukadji: Conceptualization, Methodology, Writing – Original Draft, Supervision, Funding Acquisition.
Mekila Mbayam Olivier: Investigation, Data Curation, Formal Analysis, Visualization, Writing – Review & Editing.
Patrick Loola Bokonda: Resources, Validation, Laboratory Experiments, Data Curation.
Abdessalam Ait Madi: Software, Statistical Analysis, Writing – Review & Editing, Project Administration.

10. References

Ahmed, S. F., Sharmin, S., Kuldeep, S. A., Lameesa, A., Alam, M. S. B., Liu, G., & Gandomi, A. H. (2025). Transformative impacts of the internet of medical things on modern healthcare. *Results in Engineering*, *25*, Article 103787. https://doi.org/10.1016/j.rineng.2024.103787

Ajala, O. A., Arinze, C. A., Ofodile, O. C., Okoye, C. C., & Daraojimba, A. I. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. *Magna Scientia Advanced Research and Reviews*, *10*(01), 321-329. https://doi.org/10.30574/msarr.2024.10.1.0038

Amer, O., Garg, V., & Krawec, W. O. (2021). An introduction to practical quantum key distribution. *IEEE Aerospace and Electronic Systems Magazine*, *36*(3), 30-55. https://doi.org/10.1109/MAES.2020.3015571

Anaya-Contreras, J. A., Moya-Cessa, H. M., & Zúñiga-Segundo, A. (2019). The von Neumann entropy for mixed states. *Entropy*, *21*(1), Article 49. https://doi.org/10.3390/e21010049

Bahrami, A., Lord, A., & Spiller, T. (2020). Quantum key distribution integration with optical dense wavelength division multiplexing: A review. *IET Quantum Communication*, *1*(1), 9-15. https://doi.org/10.1049/iet-qtc.2019.0005

Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science, 560*(Part 1), 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

Basha, C. B., Murugan, K., Suresh, T., SrirengaNachiyar, V., Athimoolam, S., & Pappa, C. K. (2024). Enhancing healthcare data security using quantum cryptography for efficient and robust encryption. *Journal of Electrical Systems*, *20*(5s), 2070-2077. https://doi.org/10.52783/jes.2535

Busch, P., Heinonen, T., & Lahti, P. (2007). Heisenberg's uncertainty principle. *Physics Reports*, *452*(6), 155-176. https://doi.org/10.1016/j.physrep.2007.05.006

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials, 24*(2), 839–894. https://doi.org/10.1109/COMST.2022.3144219

Chen, J. (2025). A review of quantum key distribution technology and its applications. *Theoretical and Natural Science*, *92*, 101-107. https://doi.org/10.54254/2753-8818/2025.21793

Chen, X., Chen, L., & Yan, Y. (2022). Detecting a photon-number splitting attack in decoy-state measurement-device-independent quantum key distribution via statistical hypothesis testing. *Entropy*, *24*(9), Article 1232. https://doi.org/10.3390/e24091232

de Andrade, J. S., Nobrega, K. Z., Silva, J. B. R., & Ramos, R. V. (2023). *Eavesdropping detection without using error rate: The disentropy-based quantum key distribution.* Retrieved from https://www.researchgate.net/profile/Rubens-Ramos-3/publication/375520109_Eavesdropping_detection_without_using_error_rate_The_disentropy-based_quantum_key_distribution/links/654d5c52ce88b87031d8bf09/Eavesdropping-detection-without-using-error-rate-The-disentropy-based-quantum-key-distribution.pdf

Dhinakaran, D., Srinivasan, L., Sankar, S. U., & Selvaraj, D. (2024). Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis. *Quantum Information and Computation*, *24*(3&4), 227-266. https://doi.org/10.26421/QIC24.3-4-3

Dior, M. R., Bokonda, P. L., Alihamidi, I., Sidibé, M., & Ait Madi, A. (2022). *Smart medical devices to help patients and health workers: A survey* [Conference presentation]. 2022 IEEE 3rd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS), Fez, Morocco. https://doi.org/10.1109/ICECOCS55148.2022.9982963

Elmabrok, O., Razavi, M., Eltaif, T., & Alaghbari, K. A. (2024). High-dimensional quantum key distribution in quantum access networks. *IEEE Photonics Journal*, *16*(3), 1-7. https://doi.org/10.1109/JPHOT.2024.3383780

Emmanni, P. S. (2023). The Impact of Quantum Computing on Cybersecurity. *Journal of Mathematical & Computer Applications*, *2*(2), 1–4. https://doi.org/10.47363/JMCA/2023(2)140

Gaidash, A. A., Egorov, V. I., & Gleim, A. V. (2016). Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices. *Journal of Physics: Conference Series*, *735*, Article 012072. https://doi.org/10.1088/1742-6596/735/1/012072

Girolami, D., & Anzà, F. (2021). Quantifying the difference between many-body quantum states. *Physical Review Letters*, *126*(17), Article 170502. https://doi.org/10.1103/PhysRevLett.126.170502

Gitonga, C. K. (2025). The impact of quantum computing on cryptographic systems: Urgency of quantum-resistant algorithms and practical applications in cryptography. *European Journal of Information Technologies and Computer Science*, *5*(1), 1-10. https://doi.org/10.24018/compute.2025.5.1.146

Huang, C., Wang, J., Wang, S., & Zhang, Y. (2023). Internet of medical things: A systematic review. *Neurocomputing*, *557*, Article 126719. https://doi.org/10.1016/j.neucom.2023.126719

Jirakitpuwapat, W., Kumam, P., Deesuwan, T., & Dhompongsa, S. (2023). A quantum key distribution on qudits using quantum operators. *Mathematical Methods in the Applied Sciences*, *46*(15), 15924-15939. https://doi.org/10.1002/mma.6988

Jowarder, R. A., & Jahan, S. (2024). Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection. *World Journal of Advanced Engineering Technology and Sciences, 13*(1), 330–339. https://doi.org/10.30574/wjaets.2024.13.1.0421

Kamran, M., Malik, T., & Khan, M. M. (2021). Evaluation of eavesdropping error-rates in higher-dimensional QKD system implemented using dynamic spatial modes. *International Journal of Quantum Information*, *19*(06), Article 2150030. https://doi.org/10.1142/S0219749921500301

Kanitschar, F., & Huber, M. (2025). Practical framework for analyzing high-dimensional quantum key distribution setups. *Physical Review Letters, 135*(1), Article 010802. https://doi.org/10.1103/PhysRevLett.135.010802

Khan, M. M., Murphy, M., & Beige, A. (2009). High error-rate quantum key distribution for long-distance communication. *New Journal of Physics*, *11*(6), Article 063043. https://doi.org/10.1088/1367-2630/11/6/063043

Khanal, A., & Kaur, N. (2025). The role of quantum computing in enhancing encryption security: A review. *Cryptology ePrint Archive*. Retrieved form https://eprint.iacr.org/2025/706

Kirwan Jr, A. D. (2004). Intrinsic photon entropy? The darkside of light. *International Journal of Engineering Science*, *42*(7), 725-734. https://doi.org/10.1016/j.ijengsci.2003.09.005

Lambert, N., Giguère, E., Menczel, P., Li, B., Hopf, P., Suárez, G., Gali, M., Lishman, J., Gadhvi, R., Agarwal, R., Galicia, A., Shammah, N., Nation, P., Johansson, J. R., Ahmed, S., Cross, S., Pitchford, A., & Nori, F. (2026). QuTiP 5: The quantum toolbox in Python. *Physics Reports, 1153*, 1–62. https://doi.org/10.1016/j.physrep.2025.02.007

Lee, C., Sohn, I., & Lee, W. (2022). Eavesdropping detection in BB84 quantum key distribution protocols. *IEEE Transactions on Network and Service Management*, *19*(3), 2689-2701. https://doi.org/10.1109/TNSM.2022.3165202

Lizama-Perez, L. A., & López-Romero, J. M. (2025). Loop-back Quantum Key Distribution (QKD) for secure and scalable multi-node quantum networks. *Symmetry*, *17*(4), Article 521. https://doi.org/10.3390/sym17040521

Miyadera, T., & Imai, H. (2009). No-cloning theorem on quantum logics. *Journal of Mathematical Physics*, *50*(10), Article 102107. https://doi.org/10.1063/1.3245811

Moudgalya, S., Bernevig, B. A., & Regnault, N. (2022). Quantum many-body scars and Hilbert space fragmentation: A review of exact results. *Reports on Progress in Physics*, *85*(8), Article 086501. https://doi.org/10.1088/1361-6633/ac73a0

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge University Press.

NIST (2024). *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. Retrieved form https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Peelam, M. S., Sai, S., & Chamola, V. (2024). Explorative implementation of quantum key distribution algorithms for secure consumer electronics networks. *IEEE Transactions on Consumer Electronics*, *70*(3), 5576-5584. https://doi.org/10.1109/TCE.2024.3413768

Potharaju, S., Tambe, S. N., Srikanth, N., Tirandasu, R. K., Amiripalli, S. S., & Mulla, R. (2025). Smartphone based real-time detection of postural and leg abnormalities using deep learning techniques. *Journal of Current Science and Technology*, *15*(3), Article 112. https://doi.org/10.59796/jcst.V15N3.2025.112

Raheman, F. (2022). The future of cybersecurity in the age of quantum computers. *Future Internet*, *14*(11), Article 335. https://doi.org/10.3390/fi14110335

Rahim, M. J., Rahim, M. I. I., Afroz, A., & Akinola, O. (2024). Cybersecurity threats in healthcare it: Challenges, risks, and mitigation strategies. *Journal of Artificial Intelligence General science*, *6*(1), 438-462. https://doi.org/10.60087/jaigs.v6i1.268

Reoukadji, D. M., Bokonda, P. L., Ait Madi, A., & Alihamidi, I. (2024). *Automatic Collection System for Medical Consultation* [Conference presentation]. 2024 4th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET). IEEE, FEZ, Morocco. https://doi.org/10.1109/IRASET60544.2024.10549351

Reoukadji, D. M., Bokonda, P. L., Ait Madi, A., & Alihamidi, I. (2024, May). *Protecting patient privacy and data integrity with DAG technology for IoMT and EHR*: *A systematic review* [Conference presentation]. 2024 4th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), FEZ, Morocco. IEEE. https://doi.org/10.1109/IRASET60544.2024.10549660

Shobha, P., & Nalini, N. (2024). Genomic data fusion using Paillier cryptosystem. *Journal of Current Science and Technology*, *14*(3), Article 57. https://doi.org/10.59796/jcst.V14N3.2024.57

Solaiman, S. (2025). Enhancing quantum key distribution security through hybrid protocol integration. *Symmetry*, *17*(3), Article 458. https://doi.org/10.3390/sym17030458

Sykot, A., Azad, M. S., Tanha, W. R., Morshed, B. M., Shubha, S. E. U., & Mahdy, M. R. C. (2025). Multi-layered security system: Integrating quantum key distribution with classical cryptography to enhance steganographic security. *Alexandria Engineering Journal*, *121*, 167–182. https://doi.org/10.1016/j.aej.2025.02.056

Tambe-Jagtap, S. N. (2023). A survey of cryptographic algorithms in cybersecurity: From classical methods to quantum-resistant solutions. *SHIFRA*, *2023*, 43–52. https://doi.org/10.70470/SHIFRA/2023/006

Tulyanitikul, B., & Panichkitkosolkul, W. (2025). Confidence intervals for the Zeghdoudi distribution parameter: Applications in precipitation and COVID-19 data analysis. *Journal of Current Science and Technology*, *15*(1), Article 87. https://doi.org/10.59796/jcst.V15N1.2025.87

Ur Rasool, R., Ahmad, H. F., Rafique, W., Qayyum, A., Qadir, J., & Anwar, Z. (2023). Quantum computing for healthcare: A review. *Future Internet*, *15*(3), Article 94. https://doi.org/10.3390/fi15030094

Wang, J., Wang, Q., Liu, J., & Lyu, D. (2022). Quantum orbital angular momentum in fibers: A review. *AVS Quantum Science*, *4*(3), Article 031701. https://doi.org/10.1116/5.0101179

Wang, Y., Hu, Z., Sanders, B. C., & Kais, S. (2020). Qudits and high-dimensional quantum

computing. *Frontiers in Physics*, *8*, Article 589504. https://doi.org/10.3389/fphy.2020.589504

Xiao, F. (2023). Quantum X-entropy in generalized quantum evidence theory. *Information Sciences*, *643*, Article 119177.

Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, *92*(2), Article 025002. https://doi.org/10.1103/RevModPhys.92.025002

Yamagata, K. (2021). Maximum logarithmic derivative bound on quantum state estimation as a dual of the Holevo bound. *Journal of Mathematical Physics*, *62*(6), Article 062203. https://doi.org/10.1063/5.0047496

Zhu, C. X., Chen, Z. Y., Li, Y., Wang, X. Z., Wang, C. Z., Zhu, Y. L., ... & Peng, C. Z. (2022). Experimental quantum key distribution with integrated silicon photonics and electronics. *Physical Review Applied, 17*(6), Article 064034. https://doi.org/10.1103/PhysRevApplied.17.064034