Quantum Encryption – Securing the Future

Vijaya Saradhi Nanduri[1],

SOLUTION ARCHITECT, DXC Technology,
Wing A, 25th floor, Sattva Knowledge Park,
Plot No # 16, Sy Number: 83/1, Hi-Tec City, Panmaktha village,
Serilingampally Mandal, Raidurg, Hyderabad, Telangana 500081, India
[1]vnanduri@dxc.com

***Abstract*— Quantum encryption represents a significant advancement over traditional encryption methods such as RSA and ECC. Unlike conventional algorithms, which can be compromised by quantum computing techniques like Shor's and Grover's algorithms, quantum encryption offers a fundamentally stronger security model. At the heart of this technology lies Quantum Key Distribution (QKD), which leverages the laws of physics to ensure secure communication and enables early detection of any eavesdropping attempts. This document outlines the core principles of QKD, including superposition, entanglement, and the no-cloning theorem, along with widely adopted protocols such as BB84, E91, and CV-QKD. It also discusses implementation architectures, including fiber-based and satellite-based QKD systems.**

To strengthen security further, hybrid models that combine QKD with Post-Quantum Cryptography (PQC) are emerging, offering layered protection for critical sectors. The document also addresses practical challenges such as hardware vulnerabilities, side-channel attacks, and scalability issues, along with recommended mitigation strategies. Global standards from organizations like ETSI and ITU are covering the way for interoperability and secure deployments worldwide. Operating systems such as Microsoft Windows, Red Hat Linux, and cryptographic libraries like OpenSSL are now incorporating quantum-safe cryptography, demonstrating readiness for real-world applications.
For researchers, enterprises, and policymakers, this evolution opens exciting opportunities in innovation, migration planning, and future-proof security strategies. Quantum encryption is not just a technological leap, it is a necessity for safeguarding our digital future. [1] [2] [3] [7] [10][11][12]13][14] [21].

***Keywords*—Quantum cryptography, QKD, BB84, E91, CV-QKD, multi-core fiber, PQC, ML-KEM, ML-DSA, ITU-T Y.3800, ETSI GS QKD 014.**

I. INTRODUCTION

As computers become faster and quantum computing gets closer to reality, the way we protect digital information is facing serious challenges. Traditional cryptographic methods like RSA, "Diffie Hellman", and "Elliptic Curve" cryptography are built on the belief that certain mathematical problems are extremely hard to solve. These techniques have worked well so far because normal computers take a very long time to crack them.[3]
However, quantum algorithms such as Shor's (used for breaking down large numbers) and Grover's (used for searching data quickly) can solve these problems much faster than classical computers. This means that the security of these older systems could be weakened significantly in the future.

For students pursuing cybersecurity, this marks a transformative shift in how encryption will function in the future. For IT security professionals, it serves as a clear signal to start exploring quantum resistant cryptography techniques without any delay. And for daily users, experts across the globe are working to ensure that our online data such as passwords, banking details and any personal information data remains secure, even in the age of quantum computing.

To address this, researchers are now developing new cryptography techniques that will ensure more secure data. These are designed to be secure even against powerful quantum computers. This document focus in insights of Quantum Cryptography, basic concepts, evolution, core components, Implementation Architecture, Real World applications, Risks and Mitigations.

II. BASICS OF QUANTUM CRYPTOGRAPHY

Quantum cryptography is a new method of securing information, based on laws of physics, and quantum mechanics. The traditional cryptographic systems depend on solving difficult mathematical problems and becoming weak with the new age systems. Quantum cryptography uses unique properties of quantum particles which ensure great security.[1] [4] [6]
The following are some of the key concepts that it relies on include:

Superposition:
In quantum physics, particles can exist in multiple states at once. This allows information to be encoded in a probabilistic way, making it harder to predict or intercept.

Entanglement:
When two particles are entangled, changes to one instantly affect the other, even if they're far apart. This helps in securely sharing random data between two parties.

No-cloning theorem:
Quantum states cannot be copied perfectly. So, if someone tries to intercept the data, it can't be duplicated without detection.

Measurement disturbance:
Observing a quantum particle changes its state. This means any attempt to eavesdrop can be spotted immediately.

The most practical application of these ideas is Quantum Key Distribution (QKD). Protocols like BB84, E91, and

B92 allow two people to share a secret key over a quantum channel even if that channel isn't secure. If someone tries to listen in, the system detects it by noticing errors in the transmission. QKD is backed by strong theoretical proofs that shows it can remain secure even against powerful quantum computers. But quantum cryptography doesn't stop there. New developments include Quantum Secure Direct Communication (QSDC), Quantum Digital Signatures (QDS), Device-Independent Quantum Cryptography, Quantum Secret Sharing (QSS), Coherent One-Way (COW), and Continuous Variable (CV-QKD) are few to note. Globally, efforts are underway to standardize these technologies. Organizations like ETSI and ITU are working on guidelines, and quantum cryptography is being tested in real world networks like optical Fiber systems and satellites. Quantum cryptography is no longer just theory it's becoming a key part of how we'll secure communication in the years to come.

III. EVOLUTION OF QUANTUM CRYPTOGRAPHY

In today's digital world, secure communication is essential. Traditionally, we've relied on encryption methods like RSA, ECC, and AES, which are based on solving very tough mathematical problems. These are considered safe because regular computers take an extremely long time to crack them.

But now, with quantum computing on the horizon, things are changing. Quantum computers can solve these "hard" problems much faster using special algorithms like Shor's. This means that the encryption we've trusted for decades could become vulnerable. That's why scientists and engineers are now focusing on building quantum resistant security systems.

Classical Cryptography falls short due to Computational Security and Eavesdropping Risk.

Computational Security:

Classical encryption depends on problems like factoring large numbers. But quantum algorithms can solve these quickly, putting current systems at risk.

Eavesdropping Risk:

In traditional systems, if someone secretly listens in during key exchange, it's hard to detect. This opens the door to man-in-the-middle attacks.

Now, it's essential to explore new ways of securing data, and that's why Quantum Cryptography is emerging as one of the most promising solutions.

IV. CORE COMPONENTS

Quantum Cryptography contains the basic core components spans across Protocol design, Security Proofs and Implementation frameworks.

A. Quantum Key Distribution (QKD)

This is the heart of quantum cryptography. It allows two people to share a secret key using quantum particles like photons. If anyone tries to eavesdrop between source and target, then the system detects it immediately because quantum states get disturbed when observed. QKD works on three types of protocols categorized as 'Prepare and Measure protocols, Entanglement based protocols and Advanced QKD protocols.

Prepare and Measure Protocols:

- *BB84 Protocol:* This protocol is one of the first methods developed for Quantum Key Distribution. It works by using the polarization of light particles (photons) to represent bits of data. If anyone tries to tamper with the transmission, it causes noticeable errors, which can be easily detected.[1]
- *B92 Protocol*: This protocol was introduced by Bennett and contains only two non-orthogonal states. Its efficiency is lower when compared with BB84, but it proves the minimal requirements for quantum cryptographic security.[1]
- *Decoy State QKD*: This protocol is developed to deal with "Photon Number Splitting (PNS)" attacks against weak coherent pulse sources. This method randomizes signal intensities to detect eavesdropping. Decoy-state methods have enabled fiber-based QKD over distances exceeding 400 km.[1]
- *Coherent One-Way (COW):* This protocol is a practical method developed for QKD. It works by sending sequences of light pulses through optical Fibers, where the presence or absence of a photon in a time slot represents a bit of data. To ensure security, the coherence between successive pulses is monitored. If anyone tries to tamper with the transmission, the coherence is disturbed, creating detectable errors that reveal the intrusion.
- *Continuous Variable (CV-QKD):* This protocol is a modern method developed for QKD. It works by using the amplitude and phase of light waves to represent bits of data. These signals are measured with standard telecom detectors, and any attempt to tamper with the transmission introduces extra noise, which can be easily detected.[7]

Entanglement-Based Protocols:

- *E91 Protocol:* This protocol uses a unique quantum property called entanglement, where two particles stay connected even if they're far apart. By checking this connection through Bell's inequality tests, it helps detect if someone is secretly trying to listen in.

- *BBM92 Protocol:* This protocol is the variant of BB84 using entangled photon pairs instead of single-photon states. This protocol combines features of BB84 with entanglement-based verification.

Advanced QKD Protocols:

- *Device Independent Quantum Key Distribution (DI-QKD):* This method secures communication between the devices even if they are not fully trusted. It does this by verifying quantum connections between particles, making sure that the secure key exchange remains safe.
- *Measurement Device Independent Quantum Key Distribution (MDI-QKD)*: This is one of the protocols designed to eliminate vulnerabilities associated with the quantum state detection devices which makes more secure communication against hacking attempts. In MDI-QKD, both people send their quantum signals to a third person who checks them. Based on that, they create a secure secret key without worrying about hacking through the measuring device.[1]

- *Asymptotically Optimal Quantum Key Distribution (PM-QKD):* This protocol is a newly designed method for QKD. It works by preparing and measuring quantum states in a way that maximizes the secure key rate under realistic noise and error conditions. By optimizing the encoding and measurement process, it achieves the best possible efficiency when the number of transmitted signals becomes very large.
- *Round Robin Differential Phase Shift (RR-DPS):* This protocol works by encoding information in the relative phase between multiple light pulses, rather than in single photon states. The receiver measures the phase difference between randomly chosen pairs of pulses to generate the key.
- *Twin Field Quantum Key Distribution:* It works by sending weak light pulses from two distant parties to a central station, where the pulses interfere with each other. The interference pattern is used to generate the secret key.

B. *Quantum Secret Sharing (QSS)*

It uses entangled qubits to distribute the quantum encoded secret key among multiple participants. A predefined group can collaboratively perform quantum operations to reconstruct the original information. It uses principles like quantum entanglement and the no-cloning theorem to ensure unconditional security against eavesdropping.

C. *Quantum Secure Direct Communication (QSDC)*

This is one of the cryptography protocols that allows secret messages to be transmitted directly over a quantum channel without needing a pre-shared key.

D. *Quantum Digital Signatures (QDS)*

Quantum Digital Signatures (QDS) are the quantum version of regular digital signatures. They use quantum mechanics like entanglement and 'no cloning to' guarantee message authenticity, integrity, and non-repudiation. This means the sender can’t deny sending it, the message can’t be changed secretly, and the receiver knows it’s genuine.

E. *Quantum Oblivious Transfer (QOT)*

It is a cryptographic method where the sender has multiple messages, but the receiver can choose and access only one without the sender knowing which one was picked. It uses quantum principles like superposition and the no-cloning theorem to ensure privacy and security. The receiver cannot learn about the other messages, and the sender remains unaware of the receiver’s choice.

F. *Quantum Random Number Generators (QRNGs)*

These are the devices that use the fundamental unpredictability of quantum mechanics to produce truly random numbers. These devices exploit quantum phenomena such as the behaviour of photons, electrons, or other quantum particles to generate random numbers.

V. IMPLEMENTATION ARCHITECTURE

The following diagram shows a simple Quantum Key Distribution (QKD) setup between two users, Alice and Bob. It highlights the different layers that work together to make quantum communication secure and manage encryption keys effectively within the QKD system.[9] [10] [12] [15]

Optical Layer:
This layer contains fiber routes and it is required to use multi-core fibers (MCF) to separate quantum and classical signals. It is required to check noise models like Raman and Four-Wave Mixing (FWM) to ensure both can coexist without interference.

QKD Nodes:
It is required to choose a suitable protocol such as DPS, COW, or CV-QKD for secure key exchange. The system follows TEC/ETSI standards and includes a Quantum Random Number Generator (QRNG).

Controller & APIs:
Deploy a QKD Network Manager that supports FCAPS for fault and performance management. Implement ETSI GS QKD 014 interfaces for smooth integration and control.

Security Stack:
Enable post-quantum cryptography by using OQS Provider with OpenSSL 3.x. Use hybrid TLS/IPsec connections and maintain crypto agility in PKI setup. [11] [19]

Operating System & Applications:
On platforms like MS Windows Server 2025 or Windows 11, use ML-KEM and ML-DSA algorithms via CNG. It is required to add telemetry and manage certificate lifecycles for better security and monitoring.

Operations & QoS:
Follow ITU-T Y.3828 guidelines to ensure quality of service across QKD and user networks. Continuously monitor Quantum Bit Error Rate (QBER) and secure key generation rates.

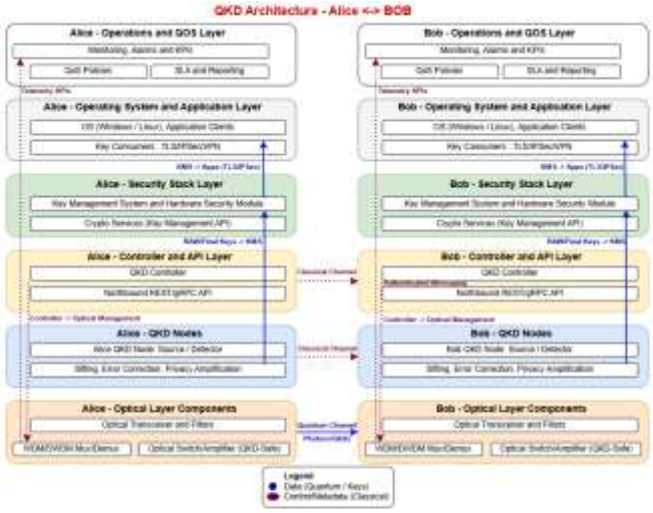
QKD Architecture - Alice <-> BOB
Alice - Operations and QOS Layer
Monitoring, Alarms and KPIs
QoS Policies
SLA and Reporting
Telemetry KPIs
Alice - Operating System and Application Layer
OS (Windows / Linux), Application Clients
Key Consumers : TLS/IPSec/VPN
Alice - Security Stack Layer
Key Management System and Hardware Security Module
Crypto Services (Key Management API)
Alice - Controller and API Layer
QKD Controller
Northbound REST/gRPC API
Controller -> Optical Management
Alice - QKD Nodes
Alice QKD Node: Source / Detector
Sifting, Error Correction, Privacy Amplification
Alice - Optical Layer Components
Optical Transceiver and Filters
WDM/DWDM Mux/Demux
Optical Switch/Amplifier (QKD-Safe)
Classical Channel
Quantum Channel
Photons/Qubits
Bob - Operations and QOS Layer
Monitoring, Alarms and KPIs
QoS Policies
SLA and Reporting
Telemetry KPIs
Bob - Operating System and Application Layer
OS (Windows / Linux), Application Clients
Key Consumers : TLS/IPSec/VPN
Bob - Security Stack Layer
Key Management System and Hardware Security Module
Crypto Services (Key Management API)
Bob - Controller and API Layer
QKD Controller
Authenticated Messaging
Northbound REST/gRPC API
Controller -> Optical Management
Bob - QKD Nodes
Bob QKD Node: Source / Detector
Sifting, Error Correction, Privacy Amplification
Bob - Optical Layer Components
Optical Transceiver and Filters
WDM/DWDM Mux/Demux
Optical Switch/Amplifier (QKD-Safe)
Legend
Data (Quantum / Keys)
Control/Metadata (Classical)

Figure 1: Simple QKD setup and data flow between Alice and Bob

While implementing the Quantum Cryptography it is required to understand the layered implementation approach and the following diagram depicts the tightly integrated three coupled planes architecture.

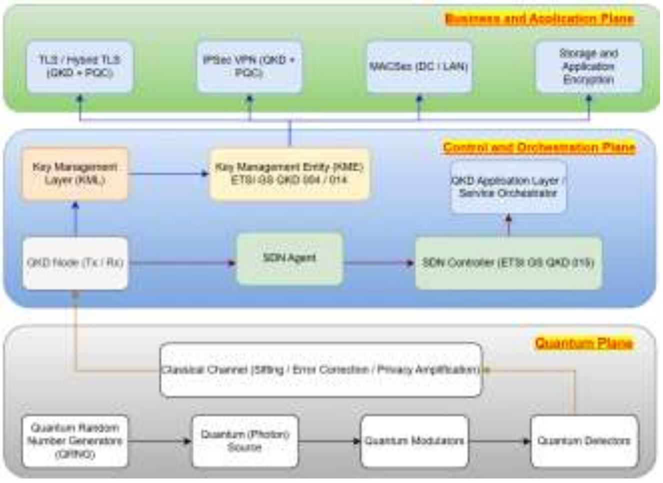
Business and Application Plane
TLS / Hybrid TLS (QKD + PQC)
IPSec VPN (QKD + PQC)
MACSec (DC / LAN)
Storage and Application Encryption
Control and Orchestration Plane
Key Management Layer (KML)
Key Management Entity (KME) ETSI GS QKD 004 / 014
QKD Application Layer / Service Orchestrator
QKD Node (Tx / Rx)
SDN Agent
SDN Controller (ETSI GS QKD 015)
Quantum Plane
Classical Channel (Sifting / Error Correction / Privacy Amplification)
Quantum Random Number Generators (QRNG)
Quantum (Photon) Source
Quantum Modulators
Quantum Detectors

Figure 2:Quantum Cryptography Layered Implementation Approach

A. Quantum Plane (Hardware and Optical Path)

This plane contains devices that can generate, transmits, and detects quantum states used to derive keys.

Hardware Components:

Photon Sources:

Laser Diodes (1310 nm / 1550 nm): Used for Weak Coherent pulses QKD(BB84, COW).

Attenuators and Modulators: It controls photon intensity and phase for encoding quantum states.

Single Photon Sources: Quantum DOT emitters for entanglement-based QKD.

Photon Detectors:

Single Photon Avalanche Diodes (SPADs): Silicon SPADs for visible wavelengths.

Super Conducting Nanowire Single Photon Detectors(SNSPDs): Ultra-high efficiency, low dark counts, cryogenic cooling is required.

Transition Edge Sensors (TES): These are advanced research setups and are extremely sensitive photon detection.

*Quantum Random Number Generators (QRNGs):*Integrated with QKD systems for randomness.

Classical Co-Channel: For sifting, error correction (LDPC/Cascade), parameter estimation, and privacy amplification can coexist with data channels by using careful filtering or physical separation. India has demonstrated QKD over multi-core fibre (MCF) with classical traffic in separate cores, which is greater than 100 kms, proving practical coexistence.

QKD System Kits:

ID Quantique Cerberis XG: Complete QKD appliance for secure key distribution.

Toshiba QKD System: BB84-protocol based QKD hardware for telecom networks.

QuintessenceLabs qOptica: CV-QKD hardware for high-speed optical networks.

B. Control and Orchestration Plane (Network Layer and Orchestration)

This plane devices manages sessions, Sifting, error correction, privacy amplification, and exposes keys via APIs to applications.

Layered model (per ITU-T Y.3800): ITU-T Y.3800 defines a multi-layered architecture to cleanly separate the technical/process responsibilities within the QKD ecosystem.

QKD Modules: QKD-Tx (Transmitter) & QKD-Rx (Receiver).

Quantum Key Distribution Node (QKD Node).

Key Manager Layer (KML): Responsible for key store, relay, synchronization and supply.

QKD Network controller and Manager: Resides in higher layers to facilitate network control and monitoring/management functions across the QKDN.

User Network Devices: The end-user infrastructure (applications, routers, endpoints) that consume the keys generated by the QKDN to encrypt and authenticate data over application links.

SDN control & QKD orchestration (ETSI GS QKD 015/018): The ETSI GS QKD-015 and QKD-018 are used to build the Software Defined Networking (SDN) to control and orchestrate Quantum Key Distribution (QKD) networks. For multi-site deployments, integrate QKD nodes with SDN controller that uses ETSI GS QKD 015 (control interface) and 018 (orchestration interface). This deployment provides resource discovery, capability distribution, and workflow automation for provisioning QKD paths across metro links. This contains,

SDN Agent: It operates on the QKD nodes, and it abstracts hardware via YANG models. It interacts with the SDN controller.

SDN Controller: It uses QKD-015 to manage QKD resources (discovery, configuration, link creation)

SDN Orchestrator: It uses QKD-018 to manage and provision end-to-end QKD services across multiple domains.

Key Management Entity (KME) & APIs (ETSI GS QKD 004/014): A Key Management Entity (KME) acts as the secure interface between a QKD network's Key Manager and the end user applications.

ETSI GS QKD 004 – Application Interface (API between KME and Applications): Specifies an API layer between the KME and applications that consume QKD-generated keys. It defines how applications can request and retrieve keys securely from the KME.

ETSI GS QKD 014 – REST-Based Key Delivery API: It defines a RESTful API over HTTPS for applications to interact with the KME. It specifies endpoints and data formats (JSON). It is designed for multi-vendor interoperability, and hence any compliant client can consume keys from any compliant KME.

C. *Application/Security Plane (Integration and Crypto Use):* This plane components consumes QKD keys in TLS/IPsec/MACsec/Storage and/or combines with Post Quantum Cryptography (PQC) for hybrid protection.

TLS (Web/Service Traffic): There are two practical patterns in this traffic.

QKD Assisted TLS: It modifies the TLS stack to retrieve pre distributed QKD keys via APIs at handshake time by using hybrid flows that retain PQC for public-key operations. It also keeps TLS 1.3 compatibility.

Hybrid TLS (QKD and PQC): It uses PQC KEM (Kyber, FIPS 203) for key agreement and QKD keys as additional traffic keys or for rekeying, achieving dual protection.

IPSec (Site to Site tunnels): Uses PQC KEM (Kyber, FIPS 203) for key agreement and QKD keys as additional traffic keys or for rekeying, achieving dual protection.

MACsec (LAN/Datacentre links): A few whitepapers validate a Quantum Safe MACsec workflow using ETSI GS QKD 014 and notes control plane behaviours (e.g., key-ID communication) that must be aligned with MACsec standards.

Storage and Application-level Encryption: Use QKD keys as high-grade symmetric keys (e.g., AES-GCM/ChaCha20-Poly1305) for envelope encryption of databases, backups, HSM key wrapping, or frequent session rekeying. It can be combined with PQC signatures (FIPS 204/205) for integrity if required.

VI. REAL-WORLD APPLICATIONS AND INTEGRATION

The following is the explanation on the Real World QKD applications and how they integrate with today's networks. [13] [14] [15] [16]

Fiber-optic QKD: In many cities, quantum keys are already being sent over regular optical fibers alongside internet traffic. Because light weakens with distance and quantum signals are very faint, practical fibre links usually work best over 100 to 200 km before the key rate drops too low. The operators extend coverage using trusted nodes to hop keys across the network, and researchers are developing quantum repeaters to push ranges much farther in the future.

When sharing fiber with classical data, engineers must manage coexistence noise (like spontaneous Raman scattering) using careful wavelength/time planning and filtering, so quantum and classical channels don't disturb each other as this is a key part of integrating QKD into existing telecom infrastructure.

Satellite QKD: Space-based links solve the long-distance problem by sending quantum signals through mostly empty space. Few facilities established secure keys between ground stations separated by 7,600 km and even enabled a quantum secured intercontinental video conference proof that ultra long distance QKD works in practice. Building on that, more recent demonstrations using micro nano satellites have shown quantum secured communication over 12,900 km (across hemispheres), pointing to future constellations that can deliver global QKD services at lower cost.

Hybrid systems (QKD + classical encryption): In real deployments, QKD typically supplies fresh symmetric keys, while high-speed classical ciphers (e.g., AES-256) encrypt the bulk data. This gives the best of both worlds: information theoretic key security with practical throughput. Standards and industry guidance increasingly describe hybrid approaches (QKD with PQC and conventional cryptography) as "defence in depth," ensuring continuity even if one layer faces new attacks. Researchers are also proposing formally analysed hybrid protocols to combine QKD with post-quantum cryptography (PQC) for authentication and key-combining, so future networks can be both quantum-safe and operationally efficient.

VII. RISKS AND MITIGATIONS

Hardware Vulnerabilities:
QKD systems rely on physical devices like photon detectors and sources. If these devices are faulty or tampered with, attackers can exploit them. To mitigate these risks, use certified hardware, regular audits, and implement device-independent QKD protocols that reduce confidence on hardware trust.

Side Channel Attacks:
Attackers may not break the quantum principles but can exploit leaks from the system such as timing information, power consumption, or electromagnetic emissions. This risk can be mitigated by using Shield devices, monitor for unusual patterns, and apply countermeasures like randomization in signal timing.

Implementation Flaws:
Even if the theory is perfect, poor coding or integration with classical networks can create loopholes. This risk can be mitigated by following the secure coding practices, conduct penetration testing, and use hybrid encryption models (QKD + classical cryptography).

Distance & Loss:
Fiber-based QKD works only for a few hundred kilometers. Beyond that, signal loss becomes a problem. To mitigate this risk, use trusted nodes or Satellite QKD for long-distance communication. Few world class facilities are still exploring the ways to implement the Satellite QKDs.

Cost and Scalability:
QKD systems are expensive and complex to deploy widely. The implementation should start with critical sectors (banks, defence, and healthcare) and gradually expand as technology becomes cheaper. Few government initiatives aim to make this practical.

Human Factors:
Human factor errors such as mismanagement, lack of training, or insider threats can compromise security. Human error risk can be mitigated by conducting regular training, enforce strict access controls, and implement multi-layer security policies.

VIII. WHAT THIS MEANS FOR THE FUTURE

Unbreakable Security:
Quantum cryptography provides security that does not rely on computing power or complex algorithms. It is based on the fundamental laws of nature, making it practically impossible to hack without detection.

Quantum Internet:
With fiber-based and satellite-based Quantum Key Distribution (QKD), technology is moving towards a global communication network that is secure by design. This means future internet connections could be inherently protected against cyber threats.

AI and IoT Integration:
As smart devices and IoT systems become more common now across industries, homes and cities, QKD can ensure their communication remains secure. Artificial Intelligence

will play a key role in monitoring these networks and detecting any suspicious activity in real time.

Global Standards:
International organizations like ETSI are creating rules and frameworks to make quantum cryptography widely accepted and regulated. This ensures that countries and companies follow common standards for security and interoperability.

Hybrid Security Models:
Combining quantum-based methods with traditional cryptography creates a layered security approach. This protects systems today from current threats and prepare for the future when quantum computers become mainstream.

IX. CONCLUSION

Quantum Key Distribution (QKD) ensures encryption key security based on the fundamental laws of physics that makes it nearly impossible for attackers to intercept or alter keys without being detected. The Post-Quantum Cryptography (PQC) focuses on safeguarding applications and communication protocols against potential quantum computer threats. It uses highly complex mathematical algorithms that even quantum systems cannot easily break. Leading technology platforms such as Microsoft Windows and OpenSSL have already started supporting quantum safe cryptographic standards. This means, organisations can begin adopting these solutions without compromising on performance or compatibility.

These future advancements demonstrate that quantum safe architectures are ready for practical implementation. It offers robust security aligned with global standards. For students, this is an exciting domain to explore as part of future cybersecurity careers. For professionals, the time has come to plan migrations to quantum safe systems to protect the sensitive data. And for general readers, the world is preparing for a future where quantum computers could break traditional encryption, and the global facilities are actively contributing to this global effort to stay secure. [11] [12] [20]

References

[1] M. Pivoluska, M. Huber, and M. Malik, "Layered quantum key distribution," Phys. Rev. A, vol. 97, no. 3, 032312, 2018.

https://journals.aps.org/pra/abstract/10.1103/PhysRevA.97.032312

[2] A. Ekert, 'Quantum cryptography based on Bell's theorem,' Phys. Rev. Lett., vol. 67, no. 6, pp. 661–663, 1991

https://cqi.inf.usi.ch/qic/91_Ekert.pdf

[3] P. Shor, 'Algorithms for quantum computation: Discrete logarithms and factoring,' Proc. 35th FOCS, 1994

https://ieeexplore.ieee.org/document/365700

[4] C. Bennett and G. Brassard, 'Quantum cryptography: Public key distribution and coin tossing,' Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, 1984

[5] University of Technology Sydney (UTS), "Scientists reveal it is feasible to send quantum signals from Earth to a satellite," Nov. 5, 2025; SciTechDaily, Nov. 8, 2025.

https://www.uts.edu.au/news/2025/11/scientists-reveal-it-is-possible-to-beam-up-quantum-signals

[6] Qi Wu et al., "Integration of QKD and high-throughput classical communications in field-deployed multi-core fibers," Light: Science & Applications, vol. 14, 274, 2025.

https://www.nature.com/articles/s41377-025-01982-z

[7] Press Information Bureau (PIB), Govt. of India, PRID 2122447, "C-DOT and STL achieve India's first QKD over Multi-Core Fibre," Apr. 17, 2025.

https://tele.net.in/c-dot-and-stl-achieve-indias-first-qkd-over-multi-core-fibre/

[8] Telco Magazine, "STL & C-DOT Achieve 100km Quantum MCF Milestone," May 8, 2025.

https://telcomagazine.com/news/stl-c-dot-achieve-100km-quantum-mcf-milestone

[9] ETSI GS QKD 014, 'REST-Based Key Delivery API,' ETSI Standards, 2025

[10] ITU-T Y.3800, 'Architecture of QKD networks,' ITU Standards, 2025

[11] Open Quantum Safe, "TLS integrations and oqs-provider for OpenSSL 3," 2024–2025.

https://github.com/open-quantum-safe/oqs-provider

[12] Microsoft Community Hub, "Post-Quantum Cryptography APIs Now Generally Available on Microsoft Platforms," Nov. 18, 2025.

https://techcommunity.microsoft.com/blog/microsoft-security-blog/post-quantum-cryptography-apis-now-generally-available-on-microsoft-platforms/4469093

[13] Austrian Academy of Sciences, "Secure quantum communication over 7,600 kilometers," Jan. 19, 2018; CNSA news, Jan. 23, 2018.

https://www.oeaw.ac.at/en/news-1/secure-quantum-communication-over-7600-kilometers-2

[14] Department of Science & Technology (DST), India, "Startup supported by DST under NQM demonstrates 500 km Quantum-Safe Network," Nov. 5, 2025; PIB PRID 2186652, Nov. 5, 2025.

https://dst.gov.in/startup-supported-dst-under-nqm-demonstrates-500-km-quantum-safe-network

[15] Press Information Bureau, Govt. of India, 'India's first QKD over Multi-Core Fibre,' Apr. 2025

[16] SoftBank Corp. & SandboxAQ, "Designing a Hybrid Path to PQC Built for the Real World," White Paper, Apr. 2025.

https://www.softbank.jp/en/corp/set/data/technology/research/news/076/pdf/WhitePaper_PQC_SB_SAQ_250425_en.pdf

[17] C-DOT product page: "Quantum Key Distribution (QKD)," accessed Dec. 2025.

https://deveservices.dot.gov.in/products/quantum-key-distribution-qkd

[18] ITU-T SG13 Liaison, "Work progress on QKD networks (as of Nov. 2025)," Dec. 18, 2025.

https://www.ietf.org/lib/dt/documents/LIAISON/liaison-2025-12-18-itu-t-sg-13-opsawg-ls-on-work-progress-on-quantum-key-distribution-qkd-network-in-sg13-as-of-november-2025-attachment-11.pdf

[19] IBM Developer, "Developing with quantum-safe OpenSSL," 2025.

https://developer.ibm.com/tutorials/awb-quantum-safe-openssl/

[20] SandboxAQ Press Release, "SoftBank and SandboxAQ jointly verify hybrid mode quantum-safe technology," Feb. 27, 2023.

https://www.softbank.jp/en/corp/technology/research/topics/008/

[21] NIST News, "NIST selects HQC as fifth algorithm for post-quantum encryption," Mar. 11, 2025; SecurityWeek, Mar. 17, 2025.

https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption