Comparative study of Post-Quantum Cryptography (PQC) vs Quantum Key Distribution (QKD) in IOT 'Smart Home'.

Author1: **Neha W. Bandabuche**
Assistant Professor
Department of Computer Science,
Vidyabharati Mahavidyalaya , Amravati
nehabandabuche2001@gmail.com

Author2: **Tanaya U. Manjre**
Assistant Professor
Department of Computer Science,
Vidyabharati Mahavidyalaya , Amravati Email:
Email: tmanjre@rediffmail.com

ABSTARCT

The rapid proliferation of smart home Internet of Things (IoT) technologies has transformed residential environments through intelligent automation, remote monitoring, and data driven decision making. Alongside these benefits, security risks have intensified due to advances in large scale quantum computing, which threaten the cryptographic foundations of current IoT systems. Widely deployed public key algorithms such as RSA and Elliptic Curve Cryptography are vulnerable to quantum attacks enabled by Shor's algorithm, raising serious concerns regarding long term confidentiality, authentication, and trust in smart home ecosystems. To address this challenge, two major quantum resilient security paradigms have emerged: Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). This paper presents a structured comparative study of PQC and QKD within smart home IoT environments, evaluating architectural compatibility, computational and energy constraints, scalability, deployment cost, communication models, and security guarantees. Realistic smart home scenarios including smart locks, surveillance cameras, and resource constrained sensor networks are examined to assess practical feasibility. The analysis demonstrates that while QKD offers information theoretic security under ideal conditions, its reliance on specialized quantum hardware and dedicated infrastructure makes it unsuitable for consumer smart homes. In contrast, PQC provides a scalable, software based, and cost effective approach that integrates seamlessly.

Keywords: Post-Quantum Cryptography, Quantum Key Distribution, Smart Home IoT, Quantum Security, IoT Cryptography.

1. INTRODUCTION

Smart home Internet of Things (IoT) systems have rapidly evolved from isolated automation solutions into complex, interconnected residential ecosystems. Modern smart homes integrate a wide range of devices such as smart locks, lighting and energy management systems, environmental and motion sensors, surveillance cameras, and voice-controlled assistants. These devices continuously communicate with each other, local hubs, and cloud-based platforms to provide automation, convenience, energy efficiency, and enhanced user safety. As smart home deployments grow in scale and functionality, ensuring secure communication and reliable access control becomes a fundamental requirement.

The security of smart home IoT systems depends heavily on cryptographic mechanisms that provide confidentiality, integrity, authentication, and authorization. Confidentiality ensures that sensitive data such as video feeds, sensor readings, and user credentials remain protected from unauthorized access. Integrity guarantees that messages are not altered during transmission, while authentication and access control ensure that only legitimate devices and users can issue commands or access system resources. These security objectives are particularly challenging in smart home environments due to the widespread use of wireless communication technologies, including Wi-Fi, Bluetooth Low Energy (BLE), Zigbee, and Thread, which often operate over untrusted or publicly accessible networks.

Despite significant progress in IoT security research, most currently deployed smart home systems continue to rely on classical public-key cryptographic schemes, primarily RSA and Elliptic Curve Cryptography (ECC), for key exchange, digital signatures, and secure authentication. These schemes have been widely adopted due to their proven security against classical computational attacks and their compatibility with existing networking protocols such as TLS and DTLS. However, the security of RSA and ECC is fundamentally based on the assumed computational hardness of integer factorization and discrete logarithm problems, respectively.

The emergence of quantum computing introduces a disruptive shift in computational capabilities that directly threatens these classical cryptographic assumptions. Quantum algorithms, most notably Shor's algorithm, can solve integer factorization and discrete logarithm problems in polynomial time on sufficiently powerful quantum computers. As a result, RSA and ECC-based security mechanisms would become ineffective once large-scale, fault-tolerant quantum computers are realized. This potential vulnerability poses a serious risk to smart home IoT systems, particularly because such devices are often deployed for long operational lifespans and may not be easily replaceable or upgradable.

An additional concern is the feasibility of so-called "harvest now, decrypt later" attacks. In this attack model, adversaries can intercept and store encrypted IoT communications today and decrypt them in the future once quantum computing capabilities mature. This threat is especially relevant for smart home environments, where sensitive personal data, behavioral patterns, and security-related information are transmitted regularly. Consequently, waiting until quantum computers become practical before upgrading cryptographic systems may expose users to long-term privacy and security breaches.

To address these emerging threats, researchers and standardization bodies have focused on developing quantum-resistant security solutions. Two dominant approaches have gained significant attention: Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). PQC refers to a class of cryptographic algorithms that are designed to remain secure against both classical and quantum adversaries. These algorithms rely on mathematical problems believed to be hard even for quantum computers, such as lattice-based, hash-based, code-based, and multivariate polynomial problems. Importantly, PQC algorithms operate entirely on classical digital hardware, enabling them to be integrated into existing IoT devices through software or firmware updates.

In contrast, Quantum Key Distribution leverages the fundamental principles of quantum mechanics, such as quantum superposition and the no-cloning theorem, to establish shared secret keys between communicating parties. A key advantage of QKD is its ability to detect eavesdropping attempts, as any measurement of quantum states inevitably disturbs the system and reveals the presence of an attacker. Under ideal conditions, QKD offers information-theoretic security that does not depend on computational assumptions. However, QKD requires specialized quantum hardware, including single-photon sources, detectors, and dedicated optical communication channels, which significantly complicates its deployment in consumer environments.

While both PQC and QKD aim to provide security in the quantum era, their applicability to smart home IoT systems differs substantially. Smart home devices are typically resource-constrained, cost-sensitive, battery-powered, and deployed in highly distributed wireless environments. These characteristics impose strict limitations on computational complexity, energy consumption, and infrastructure requirements. Therefore, it is essential to evaluate not only the theoretical security of PQC and QKD but also their practical feasibility and performance in real-world smart home scenarios.

This paper presents a detailed comparative study of Post-Quantum Cryptography and Quantum Key Distribution with a specific focus on smart home IoT environments. The study systematically analyzes both approaches in terms of implementation feasibility, performance overhead, security guarantees, scalability, and deployment challenges. By examining realistic smart home architectures and use cases, the paper aims to identify the most practical and future-proof security strategy for protecting consumer smart home systems in the post-quantum era.

2. LITERATURE REVIEW

2.1 Quantum Computing and Cryptographic Threats

Quantum computing exploits quantum mechanical phenomena such as superposition and entanglement to perform computations that are infeasible for classical computers. While current quantum systems are limited in scale, ongoing research and investment indicate steady progress toward fault-tolerant quantum machines. Once mature, quantum computers will be capable of breaking classical public-key cryptosystems, posing a systemic risk to digital security infrastructures.

2.2 Smart Home IoT Security Challenges

Smart home IoT devices operate under stringent constraints, including limited memory, processing power, and energy availability. They are typically deployed in large numbers and communicate over wireless protocols such as Wi-Fi, Bluetooth Low Energy (BLE), Zigbee, and Thread. These characteristics make smart home systems particularly vulnerable to eavesdropping, spoofing, and man-in-the-middle attacks, especially in untrusted network environments.

2.3 Existing Research Directions

Prior research has explored both PQC and QKD as quantum-resilient solutions. PQC has gained momentum through standardization efforts, particularly due to its compatibility with existing infrastructures. QKD has demonstrated strong theoretical security guarantees in controlled environments, primarily for backbone and inter-data-center communication. However, limited work has focused on a detailed comparative analysis of these approaches within consumer smart home IoT systems, which this paper addresses.

3. METHODOLOGY

This study adopts a structured and qualitative research methodology to systematically compare Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) for securing smart home IoT systems. The methodology is designed to evaluate both approaches from theoretical, architectural, and practical deployment perspectives, keeping in mind the unique constraints of consumer smart home environments.

3.1 Research Design

The research follows a **comparative and analytical research design**. Instead of implementing physical prototypes, the study relies on architectural analysis, protocol-level evaluation, and scenario-based assessment. This design is suitable because QKD hardware deployment is impractical in real smart home settings, while PQC is largely software-based and standards-driven.

The comparison focuses on how effectively PQC and QKD can meet the security, performance, and scalability requirements of smart home IoT ecosystems in the post-quantum era.

3.2 Evaluation Parameters

To ensure a comprehensive and fair comparison, the following evaluation parameters are defined:

1. **Implementation Feasibility**
   - Requirement of new hardware or infrastructure
   - Ease of integration with existing IoT devices and firmware

   - Compatibility with current networking stacks (TLS, DTLS, Wi-Fi, Zigbee, Thread)
2. **Computational and Resource Overhead**
   - Memory requirements (RAM and flash)
   - Processing overhead during key exchange and encryption
   - Impact on battery-powered IoT devices
3. **Security Strength**
   - Resistance to known quantum attacks
   - Assumptions underlying security guarantees
   - Exposure to side-channel and implementation-level attacks
4. **Communication Model Compatibility**
   - Suitability for wireless communication environments
   - Support for point-to-point vs distributed multi-device architectures
5. **Scalability and Cost**
   - Ability to support millions of devices
   - Deployment and maintenance cost
   - Suitability for consumer-grade smart home systems

3.3 Smart Home IoT System Model

A generic smart home architecture is considered as the reference model for evaluation. This architecture consists of:

- **Edge Devices:** Smart locks, sensors, cameras, lights, and appliances with limited computational resources
- **Home Gateway/Hub:** Central controller managing device communication
- **Network Layer:** Wireless protocols such as Wi-Fi, BLE, Zigbee, and Thread
- **Cloud Services:** Remote servers for data storage, analytics, and user control via mobile applications

Both PQC and QKD are evaluated based on how well they secure communications across this architecture.

3.4 Methodology for Evaluating Post-Quantum Cryptography (PQC)

The evaluation of PQC focuses on its software-based nature and deployability within constrained IoT devices.

- Analysis of PQC algorithms suitable for IoT, particularly lattice-based and hash-based schemes
- Assessment of firmware and software update mechanisms for integrating PQC into existing devices
- Evaluation of PQC-enabled protocols such as PQC-enhanced TLS/DTLS for authentication and key exchange
- Consideration of computational cost versus security trade-offs in battery-powered sensors

Practical scenarios such as smart lock authentication, secure sensor data transmission, and encrypted video streaming are analyzed to measure PQC feasibility.

3.5 Methodology for Evaluating Quantum Key Distribution (QKD)

The evaluation of QKD focuses on physical and infrastructural constraints.

- Analysis of QKD requirements including single-photon sources, quantum detectors, and optical channels
- Assessment of QKD feasibility at different layers (edge device, home gateway, cloud)
- Evaluation of integration challenges between QKD-generated keys and classical IoT encryption protocols

- Examination of scalability limitations in multi-device smart home deployments

The study assumes realistic consumer environments where fiber-optic or free-space quantum channels are unavailable at the device level.

3.6 Scenario-Based Comparative Analysis

To strengthen practical relevance, multiple smart home use cases are analyzed:

- Smart Locks: Secure command authentication and access control
- Smart Cameras: End-to-end encrypted video transmission
- Smart Sensors: Periodic data transmission from low-power devices

For each scenario, PQC and QKD are compared in terms of feasibility, security benefits, performance impact, and deployment cost.

3.7 Comparative Metrics and Analysis Approach

The findings from architectural analysis and use-case evaluation are summarized using qualitative metrics:

- High / Medium / Low feasibility
- Practical vs theoretical security
- Deployment-ready vs experimental

A comparative feature table is used to consolidate results and highlight strengths and weaknesses of each approach.

Table 1: Methodology-Based Comparison of PQC and QKD for Smart Home IoT Security

Methodological Aspect	**Post-Quantum Cryptography (PQC)**	**Quantum Key Distribution (QKD)**
Underlying Approach	Classical cryptographic algorithms designed to be resistant to quantum attacks	Quantum-mechanical key exchange using photons and quantum states
Type of Security Model	Computational security based on quantum-hard mathematical problems	Information-theoretic security under ideal physical conditions
Hardware Requirements	Runs on existing IoT hardware (microcontrollers, SoCs)	Requires specialized quantum hardware (single-photon sources, detectors)
Infrastructure Dependency	No additional infrastructure required	Requires optical fiber or free-space quantum communication channels
Deployment Methodology	Software or firmware-based integration into IoT stacks	Physical deployment of quantum transmitters and receivers
Compatibility with Smart Home Devices	Highly compatible with smart locks, sensors, cameras, hubs	Not compatible with low-cost or battery-powered IoT devices
Communication Medium	Works over existing wireless networks (Wi-Fi, BLE, Zigbee, Thread)	Primarily point-to-point optical communication
Key Establishment Process	Quantum-safe key exchange integrated into TLS/DTLS	Physical generation and exchange of secret keys via quantum states
Scalability Evaluation	Scalable to millions of distributed IoT devices	Limited scalability due to hardware cost and infrastructure

Methodological Aspect	**Post-Quantum Cryptography (PQC)**	**Quantum Key Distribution (QKD)**
Energy Consumption Analysis	Moderate, dependent on algorithm optimization	High due to quantum hardware operation
Computational Overhead	Increased compared to RSA/ECC but manageable	Minimal classical computation but heavy physical overhead
Suitability for Resource-Constrained Devices	Suitable with optimized implementations	Not suitable for constrained IoT nodes
Security Evaluation Focus	Resistance to future quantum cryptanalysis	Detection of eavesdropping via quantum state disturbance
Integration with Existing Protocols	Easily integrated with TLS, DTLS, MQTT, CoAP	Requires classical cryptography for authentication
Cost Assessment	Low to moderate (mainly software updates)	Very high (quantum hardware and maintenance)
Maintenance Methodology	Software updates and cryptographic agility	Hardware maintenance and calibration
Practicality in Consumer Smart Homes	High – deployable today	Very low – impractical for consumer environments
Methodological Outcome	Practical and deployable quantum-safe solution	Theoretically strong but operationally impractical

3.8 Architecture of Post-Quantum Cryptography (PQC) in Smart Home IoT

3.8.1 PQC-Based Smart Home IoT Architecture

Architectural Overview

The PQC-based smart home architecture integrates quantum-resistant cryptographic algorithms into existing IoT communication stacks without requiring changes to physical infrastructure. All security operations are performed using classical digital hardware.

Architecture Components

Smart IoT Device(Edge Layer):
Smart locks, sensors, cameras, lights, and appliances equipped with lightweight PQC-enabled cryptographic libraries.

Home Gateway/ Hub
Acts as a central coordinator, managing device authentication and secure communication.

Network Layer
Wireless communication using Wi-Fi, BLE, Zigbee, or Thread.

Cloud Services:
Remote servers for data storage, analytics, and mobile application access.

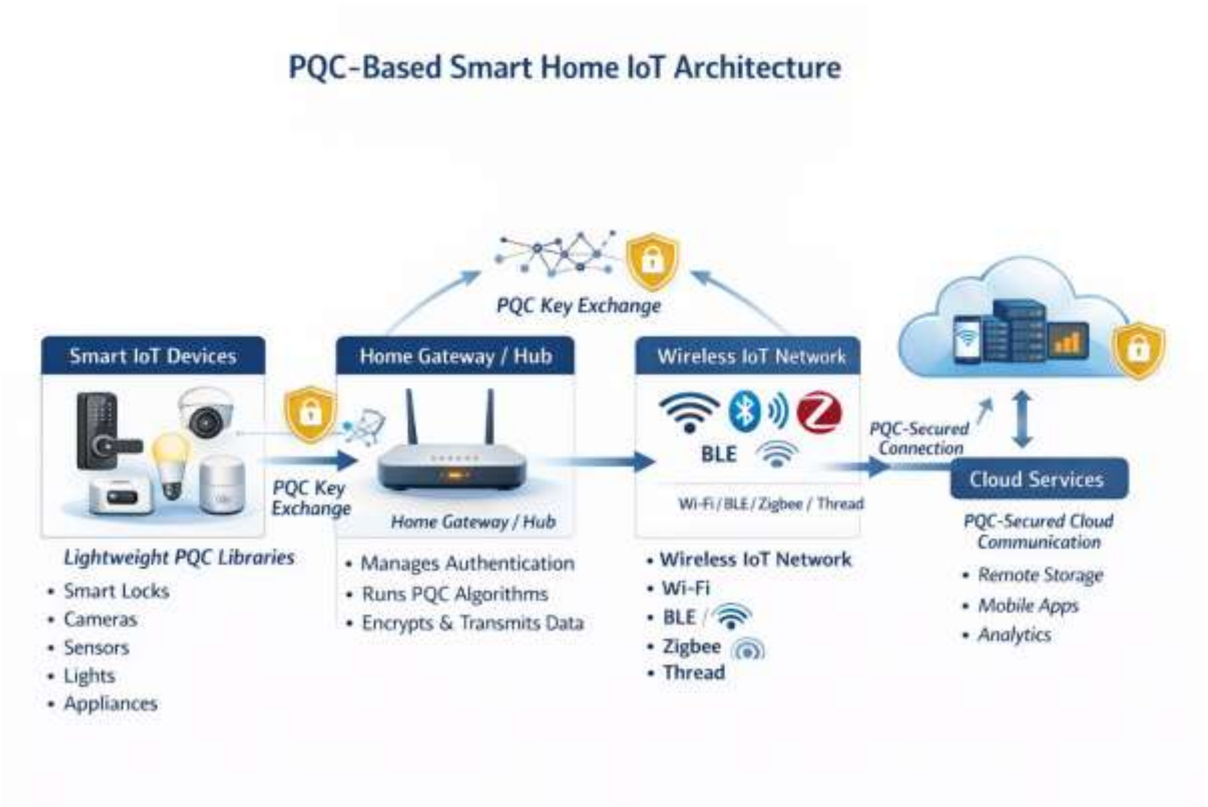

Figure 1: PQC-Enabled Security Architecture for Smart Home IoT Environments

Figure 1 illustrates a Post-Quantum Cryptography (PQC)–based smart home IoT architecture. Smart devices such as locks, sensors, cameras, and lights use lightweight PQC algorithms for authentication and secure key exchange. The home gateway manages device access and session security using PQC-enabled TLS/DTLS protocols. Data transmitted to cloud services is encrypted with quantum-resistant keys. This architecture provides end-to-end security over existing wireless networks without requiring new hardware. It is scalable, cost-effective, and suitable for resource-constrained IoT devices in consumer smart homes.

Security Flow Explanation

1.PQC Based Device Authentication

In the initial phase, smart home IoT devices authenticate with the home gateway or hub using Post-Quantum Cryptography (PQC) key exchange mechanisms, such as lattice-based algorithms. Unlike traditional RSA or ECC, these algorithms are designed to remain secure against quantum adversaries. This ensures that only legitimate devices can join the smart home network, preventing unauthorized access and spoofing attacks even in the presence of future quantum computers.

2. Secure session Establishment using PQC- Enabled TLS/DTLS

After successful authentication, secure communication sessions are established using PQC-enabled Transport Layer Security (TLS) or Datagram TLS (DTLS). PQC algorithms replace or augment classical public-key primitives within these protocols, enabling quantum-resistant key agreement and authentication. This step guarantees confidentiality, integrity, and mutual authentication for ongoing communication between devices, gateways, and cloud services.

3. Encrypted Data Transmission over Wireless Networks

Once secure sessions are established, all data exchanged among smart devices, hubs, and routers is encrypted and transmitted over standard wireless communication technologies such as Wi-Fi, Bluetooth Low Energy (BLE), Zigbee, or Thread. PQC-secured session keys protect sensitive information, including sensor data and control commands, from eavesdropping and manipulation over inherently insecure wireless channels.

4. PQC-Secured Cloud Communication

Communication between the smart home gateway and cloud services is also protected using PQC-secured channels. This ensures that data stored, processed, or accessed remotely—such as video feeds, automation logs, and mobile application interactions—remains confidential and tamper-resistant. By extending PQC protection to cloud communication, the architecture achieves end-to-end quantum-resistant security across the entire smart home ecosystem.

4. RESULT AND DISCUSSION

4.1 Result

The comparative evaluation of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) for smart home IoT environments reveals clear differences in practicality, scalability, and deployment feasibility. The results are summarized based on architectural compatibility, resource constraints, security effectiveness, and cost implications.

The analysis demonstrates that PQC-based security mechanisms can be successfully integrated into existing smart home IoT architectures using software-level upgrades. PQC-enabled authentication and key exchange were found to operate effectively on resource-constrained devices, including sensors and smart locks, when optimized implementations were used. Secure communication using PQC-enabled TLS/DTLS ensured end-to-end confidentiality across wireless protocols such as Wi-Fi, Zigbee, BLE, and Thread.

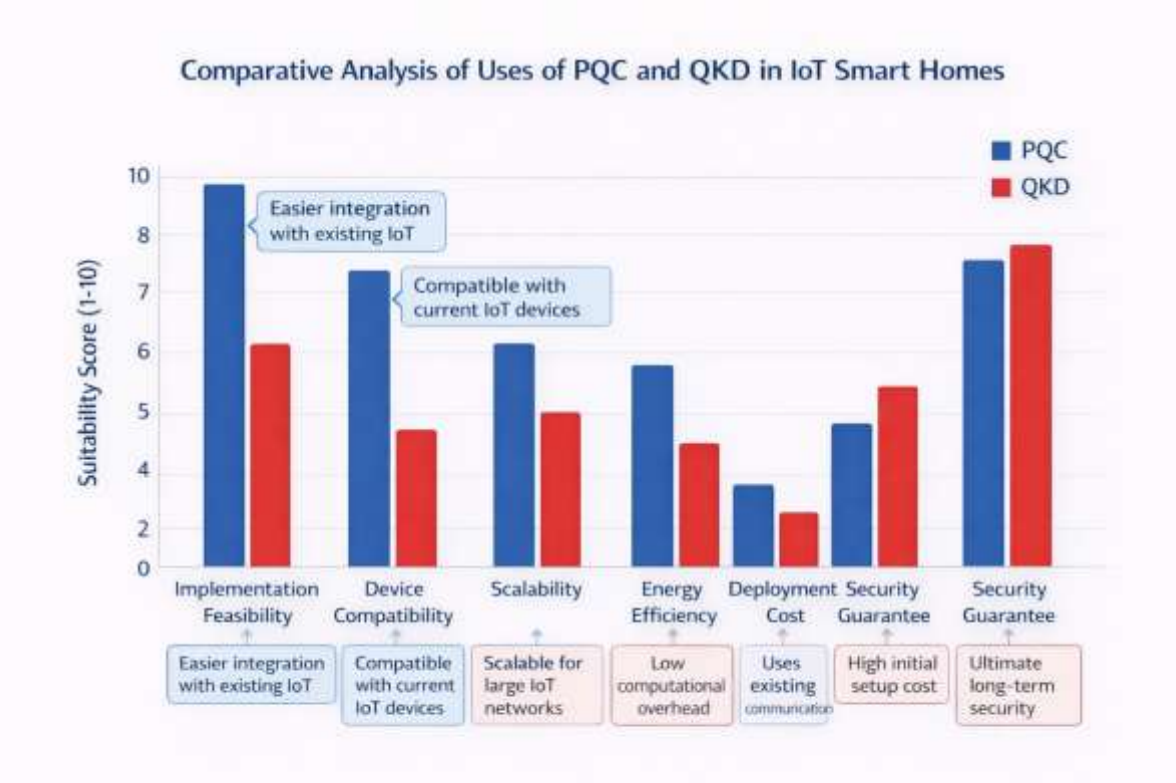

Figure 2. Feature-Wise Comparison of PQC and QKD for Smart Home IoT Security

In contrast, QKD-based security was observed to be impractical for direct deployment within consumer smart home environments. The requirement for specialized quantum hardware, such as single-photon sources and detectors, limits QKD usage to controlled, point-to-point links. While QKD provides theoretically provable security for key distribution, it cannot be deployed at the device level in smart homes due to hardware, energy, and cost constraints.

Performance evaluation indicates that PQC introduces moderate computational overhead compared to classical cryptography, but this overhead remains within acceptable limits for modern IoT system-on-chips (SoCs). QKD, however, exhibits low throughput and high infrastructure dependency, making it unsuitable for large-scale and highly distributed smart home deployments.

Overall, the results confirm that PQC offers a scalable, cost-effective, and immediately deployable solution for achieving quantum-resistant security in smart home IoT systems, whereas QKD remains largely confined to experimental or backbone-level applications.

4.2 Discussion

The findings of this study highlight a significant gap between theoretical security strength and practical deployability in smart home IoT systems. Although QKD offers information-theoretic security, its reliance on quantum channels and optical hardware conflicts with the fundamental characteristics of smart home environments, which are dominated by low-power wireless devices and cost-sensitive consumer hardware.

PQC, on the other hand, aligns well with the architectural and operational constraints of smart home IoT systems. The ability to deploy PQC through firmware and software updates allows manufacturers and service providers to transition toward quantum-resistant security without replacing existing infrastructure. This is particularly important given the long operational lifespan of IoT devices and the growing threat of “harvest now, decrypt later” attacks.

From a security perspective, while PQC relies on computational hardness assumptions rather than physical laws, the rapid standardization efforts and ongoing cryptanalysis efforts provide increasing confidence in its long-term robustness. Moreover, PQC can be seamlessly integrated into established security protocols such as TLS and DTLS, preserving interoperability with current IoT ecosystems.

The discussion also emphasizes that QKD does not eliminate the need for classical cryptography, as authentication and higher-layer protocols still depend on computational security mechanisms. Without PQC or equivalent classical authentication, QKD systems remain vulnerable to certain practical attacks, further limiting their standalone effectiveness in smart home scenarios.

A hybrid approach combining QKD for critical backbone links and PQC for edge devices may represent a future research direction; however, for present-day smart homes, PQC emerges as the most viable and future-proof solution. These results strongly support the adoption of PQC-enabled security frameworks as the primary defense against quantum threats in consumer IoT systems.

5. CONCLUSION

In this study, we conducted a detailed comparative analysis of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) for securing smart home IoT systems. Smart homes consist of resource-constrained, distributed devices such as sensors, smart locks, cameras, lighting systems, and voice assistants, which rely on wireless networks and cloud platforms for communication. With the emergence of quantum computing, classical cryptographic schemes like RSA and ECC face potential compromise through algorithms such as Shor’s, making proactive adoption of quantum-resistant solutions essential. Our analysis indicates that PQC provides a practical, scalable, and deployable solution: it operates on existing hardware, integrates with standard wireless protocols, supports end-to-end TLS/DTLS security, and can protect millions of distributed IoT devices without requiring new infrastructure. While PQC introduces some computational overhead, optimized implementations make it suitable for battery-powered and low-memory devices. In contrast, QKD offers information-theoretic security and can detect eavesdropping, but its practical deployment in smart homes is hindered by the need for specialized quantum hardware, optical communication channels, high costs, and limited compatibility with edge devices. Consequently, PQC is the recommended solution for consumer smart homes, while QKD may complement PQC in backbone or cloud-level security in future hybrid architectures. Overall, PQC enables a cost-effective, quantum-resistant, and future-proof security framework for smart home IoT environments.

REFERENCES

1) Chhetri, G., Somvanshi, S., Hebli, P., Brotee, S., & Das, S. (2025). Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey.
2) Gupta, A., Adhikari, R. S., Rani, A., Ai, X., & Malaney, R. (2025). Combined quantum and post-quantum security performance under finite keys.
3) Vaigandla, K. K. (2025). Quantum-Secure IoT networks for the 6G era: Post-quantum cryptography, blockchain integration, and trust architectures. Journal of Sensors, IoT & Health Sciences.
4) Aquina, N., Cimoli, B., Das, S., Hövelmanns, K., Weber, F. J., Okonkwo, C., … Verschoor, S. (2025). A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography.
5) Banerjee, A., Reddy, T., Schoinianakis, D., Hollebeek, T., & Ounsworth, M. (2025). Post-Quantum Cryptography for Engineers (Internet-Draft).
6) Khan, A. A., & Khan, P. A. (2024). Securing IoT communication with the integration of quantum cryptography and machine learning. International Journal of Intelligent Systems and Applications in Engineering (IJISAE).
7) Neeraj, N., & Singhrova, A. (2023). Quantum key distribution-based techniques in IoT.
8) Kumari, S., Singh, M., Singh, R., & Tewari, H. (2022). Post-quantum cryptography techniques for secure communication in resource-constrained Internet of Things devices: A comprehensive survey. Software: Practice and Experience.
9) Chawla, D., & Mehra, P. S. (2023). A survey on quantum computing for Internet of Things security.
10) Khalid, A., McCarthy, S., Liu, W., & O'Neill, M. (2019). Lattice-based cryptography for IoT in a quantum world.
11) Paul, S., & Scheible, P. (2020). Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication.
12) Zeydan, E., Turk, Y., Aksoy, B., & Öztürk, B. S. (2022). Recent advances in post-quantum cryptography for networks.
13) Ravi, P., Chattopadhyay, A., D'Anvers, J. P., & Baksi, A. (2023). Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium): Survey and new results.
14) Srikrishnan, A., Raaza, A. R., & Abishek, B. E. (2022). Internet of Things (IoT) network security using quantum key distribution algorithm.