

QUANTUM-SAFE SECURITY FRAMEWORK FOR PRIVACY-PRESERVING 6G COMMUNICATION SYSTEMS

P.T. Kalaivaani¹ and E. Nagarjuna²

¹Department of Electronics and Communication Engineering, Vivekanandha College of Engineering for Women, India

³Department of Computer Science and Engineering, QIS College of Engineering and Technology, India

Abstract

This research paper presents a framework, referred to as QRAPSF, which is quantum-resilient and adaptive privacy security framework for 6G communication systems. The QRAPSF framework incorporates quantum-resistant key establishment using ML-KEM, authentication using ML-DSA, lightweight privacy preserving identity management, adaptive physical layer security, and threat aware security level selection. The hierarchical security controller determines the appropriate security level based on channel status, device capability, latency requirements, and threat level. The proposed QRAPSF framework obtains attack detection accuracy of 96.24%, authentication success rate of 98.31%, and privacy preservation efficiency of 95.14% under 5% network load and 93.81%, 96.19%, and 92.61%, respectively, under 30% network load. The communication overhead remains between 9.42% and 11.68%, whereas the authentication latency varies between 29.84 ms and 37.42 ms depending on the network load. Under 30% network load, the proposed QRAPSF framework has communication overhead 5.40 percentage points less than that of Lattice-Based Physical Layer Security and authentication latency 7.86 ms less than that of Hybrid PQC Authentication.

Keywords:

6G Security, Post-Quantum Cryptography, Privacy Preservation, ML-KEM, Adaptive Authentication

1. INTRODUCTION

The progress of the sixth generation (6G) of wireless communications technologies is anticipated to go beyond the traditional goals of improved data rate and latency by incorporating intelligent networking, ubiquitous connectivity, distributed artificial intelligence, edge intelligence, sensing, and heterogeneous communication technologies into the mix. The future 6G technology will provide connectivity among devices on the ground, aerial, maritime, space, and IoT platforms via dynamic networks. This would provide room for immersive services, autonomous systems, intelligent health care, industrial automation, extended reality, and machine-to-machine communications. At the same time, these features would allow more sensitive information to be shared within the communication channels and distributed computing platforms. According to current research, the 6G network will have security, privacy, ultra-low latency, energy efficiency, artificial intelligence, and heterogeneous connectivity requirements.

The security requirements of 6G become particularly important because future networks are expected to accommodate devices with substantially different computational capabilities. High-performance edge servers may execute sophisticated security operations, whereas sensors, wearable devices, vehicles, and embedded IoT nodes operate under strict processing and energy constraints. In addition, 6G communication extends the attack surface from conventional network infrastructure to

intelligent edge nodes, distributed learning participants, programmable radios, and integrated sensing systems. Physical-layer security has therefore received increasing attention because it can exploit wireless-channel characteristics without depending entirely on computationally expensive conventional cryptographic operations. Research on secure URLLC indicates that strict latency and reliability requirements can make heavyweight cryptographic mechanisms difficult to apply directly, particularly in resource-constrained environments. [1]–[3]

The next threat comes from quantum computing technology itself. Traditional public key encryption algorithms like RSA and ECC rely on mathematical problems that can be easily solved by a sufficiently powerful quantum computer. Shor's algorithm provides a theoretical framework for breaking cryptosystems based on integer factorization and discrete logarithms. Consequently, information encrypted using classical algorithms will become unsafe once quantum computing becomes powerful enough. This threat has led to the creation of the field of post-quantum cryptography (PQC). The goal is to develop algorithms that are safe against both classical and quantum attacks. In 2024, NIST published FIPS 203, FIPS 204, and FIPS 205 standards defining ML-KEM, ML-DSA, and SLH-DSA. [4], [5]

The primary issue considered in this work is the lack of an integrated security architecture that takes into account quantum resistance, privacy preservation, authentication, security adaptation, and communication efficiency in heterogeneous 6G networks. Previous works typically deal with only one of these aspects. For instance, lattice cryptography may be used for achieving quantum-resistant confidentiality, and physical-layer security may protect wireless communication using channel characteristics. On the other hand, federated learning helps in avoiding direct exposure of private training data, but it still makes the distributed entities vulnerable to poisoning, inference, communication, and model-based attacks. An emerging work on physical-layer security in 6G shows the feasibility of lattice cryptography for protecting OFDM communications; however, it mainly aims at confidentiality in the physical layer, not privacy and authentication architecture. [6]

The aim of this research work is hence to design a Quantum-Resilient Adaptive Privacy Security Framework (QRAPSF) for the 6G communication system. The framework is expected to achieve quantum-resilience in session key establishment, authentication of participating devices, ensuring the privacy of users as well as the devices, adapt its level of security based on the communication condition and at the same time ensure that there is minimal latency and communication overhead during this process.

The key novel idea behind QRAPSF is its ability to combine cross-layer standardized post-quantum cryptography with

adaptive privacy and physical-layer security. Unlike previous attempts where only one cryptographic setup was used for all devices, QRAPSF uses a security controller that considers device capability, latency of communication, quality of the channel, and threat level before deciding on which security configuration is to be used. ML-KEM ensures quantum resistance during key establishment and ML-DSA enables authentication and integrity. On top of that, a privacy layer helps in reducing the exposure of devices and their metadata, and an adaptive physical-layer security module is yet another way to secure wireless communication.

2. RELATED WORKS

Recent research on quantum-safe communication and 6G security can be broadly categorized into post-quantum cryptography, physical-layer security, hybrid authentication, privacy-preserving distributed learning, and integrated intelligent security architectures.

[7] presented a survey of post-quantum cryptography and discussed the transition from conventional cryptography toward quantum-resistant alternatives. Their analysis covered lattice-, code-, hash-, and other post-quantum approaches while emphasizing the security implications of quantum computing. The study established that PQC provides a practical direction for protecting conventional communication infrastructures against future quantum attacks. However, its focus remains primarily on cryptographic primitives rather than the integration of PQC into dynamic 6G communication environments. This leaves a requirement for adaptive mechanisms that consider latency, device capability, and network conditions.

[8] investigated lattice-based cryptography and highlighted its importance as a post-quantum cryptographic family. Lattice-based constructions rely on hard mathematical problems in high-dimensional lattices and offer a combination of security and computational efficiency. Their survey describes the theoretical foundations and cryptanalytic techniques associated with lattice-based systems. The work provides a strong foundation for employing lattice mechanisms in quantum-safe communication, but it does not specifically address how cryptographic operations can be coordinated with privacy preservation and physical-layer security in 6G.

[9] examined lattice-based cryptosystems within the standardization process and analyzed their security and design characteristics. The study identified lattice-based constructions as promising candidates because of their security properties and practical performance. The work is particularly relevant to the selection of lattice-based mechanisms for future communication systems. Nevertheless, standardization-oriented analysis does not by itself resolve deployment issues associated with heterogeneous 6G devices, where the computational capability and latency tolerance can differ considerably.

[10] surveyed lattice-based security and authentication mechanisms for smart-grid networks in the post-quantum era. Their study considered PQC primitives, NIST-selected algorithms, implementation tools, and security requirements of resource-constrained networked systems. The work demonstrates the applicability of lattice-based security to distributed infrastructure and IoT-oriented environments. However, smart-

grid requirements do not fully capture the extreme heterogeneity, mobility, ultra-low latency, and integrated sensing characteristics anticipated in 6G systems.

[11] proposed a physical-layer security scheme for 6G wireless networks using lattice-based post-quantum encryption. The method encrypts QAM symbols using lattice-based public and private bases before OFDM transmission. Numerical evaluation demonstrates the feasibility of incorporating lattice encryption into physical-layer protection. This study is closely related to the present research because it establishes that quantum-resistant cryptography can operate at the wireless physical layer. However, the method concentrates on encrypted signal transmission and does not jointly address adaptive authentication, privacy-preserving identities, or dynamic security-level selection.

[12] examined hybrid post-quantum cryptography for authentication and key agreement in 6G. Their work emphasizes vulnerabilities in existing 5G authentication mechanisms and considers hybrid PQC as a transition mechanism toward quantum-resistant 6G authentication. The study is important because authentication and key agreement are fundamental to preventing impersonation and unauthorized network participation. Nevertheless, a hybrid authentication mechanism alone does not provide comprehensive privacy protection or physical-layer confidentiality across heterogeneous 6G devices.

[13] reviewed the security of federated learning in the 6G era. Federated learning allows distributed devices to train models without directly transferring their local datasets, thereby reducing some forms of data exposure. However, the distributed architecture remains vulnerable to communication attacks, malicious clients, model manipulation, and privacy leakage. The study emphasizes that privacy preservation should be accompanied by systematic security mechanisms. This finding supports the inclusion of adaptive privacy protection within a broader 6G security architecture.

[14] reviewed privacy-preserving mechanisms in blockchain-based federated learning. Their work shows that blockchain can provide decentralized coordination and auditability, while federated learning can reduce direct data sharing. However, combining the two mechanisms introduces additional computational and communication costs. These trade-offs are particularly important in 6G because edge and IoT devices may have limited resources. The study therefore demonstrates the importance of balancing privacy enhancement with system efficiency rather than optimizing privacy independently.

[15] investigated artificial-intelligence-enabled physical-layer security for 6G networks. Their study highlights the dynamic topology, open wireless channels, heterogeneous devices, and mission-critical applications of future 6G systems. AI-based physical-layer security can identify changing attack conditions and adapt protection mechanisms according to communication characteristics. However, AI-enabled physical-layer protection does not inherently provide quantum-resistant key establishment or post-quantum authentication.

The proposed QRAPSF addresses this gap by combining these complementary security capabilities into a unified adaptive framework. Its distinguishing feature is not merely the use of PQC, but the coordinated selection of quantum-resistant key establishment, authentication, privacy protection, and physical-layer security according to the operational state of the 6G

network. This design follows the broader direction of current PQC standardization while targeting the specific deployment constraints of future wireless systems. NIST's finalized ML-KEM, ML-DSA, and SLH-DSA standards provide suitable cryptographic foundations for such an architecture.

3. PROPOSED QRAPSF

The proposed QRAPSF provides an integrated security architecture for privacy-preserving 6G communication systems. The framework combines quantum-resistant key establishment, post-quantum authentication, privacy-preserving identity management, adaptive security selection, physical-layer protection, and continuous threat assessment. Unlike a fixed security architecture, QRAPSF dynamically selects security configurations according to the computational capability of the participating device, channel condition, latency requirement, communication sensitivity, and estimated threat level. The framework employs ML-KEM for quantum-resistant session-key establishment and ML-DSA for authentication and integrity protection, while an adaptive privacy layer minimizes exposure of device identities and communication metadata. A security controller continuously evaluates the network state and assigns an appropriate protection level. The resulting architecture establishes a coordinated security chain from device authentication to key generation, privacy protection, encrypted transmission, physical-layer protection, and post-transmission verification.

The operation of QRAPSF is divided into the following sequential steps:

- **6G Device Registration and Security Profiling:** Each device registers with the security controller and establishes a protected security profile containing device capability, computational resources, latency tolerance, communication sensitivity, and trust-related parameters.
- **Privacy-Preserving Identity Generation:** The permanent device identity is transformed into a protected pseudonymous identity so that communication sessions do not continuously expose the original identity.
- **Quantum-Resistant Authentication:** The communicating devices perform ML-DSA-based authentication to establish identity authenticity and message integrity.
- **Quantum-Safe Key Establishment:** ML-KEM is employed to establish a shared session key between authenticated communication entities.
- **Adaptive Security-Level Selection:** The security controller evaluates threat intensity, channel quality, device resources, latency requirements, and data sensitivity to select an appropriate security profile.
- **Privacy-Preserving Data Protection:** Sensitive payloads and selected metadata are protected using the established session key and privacy-preserving transformations.
- **Physical-Layer Security Enhancement:** Channel information, transmission conditions, and interference characteristics are used to provide an additional security layer for wireless transmission.
- **Continuous Threat Monitoring:** Security indicators are continuously monitored to identify anomalous behavior,

attack attempts, key compromise indications, and abnormal communication patterns.

- **Dynamic Security Adaptation:** When the network condition or threat level changes, QRAPSF dynamically modifies the security configuration without requiring complete re-registration.
- **Secure Session Termination and Key Renewal:** At the end of a communication session, temporary identifiers and session keys are invalidated and new quantum-safe parameters are generated for subsequent sessions.

3.1 SYSTEM INITIALIZATION AND SECURITY PROFILING

The first stage establishes the security environment for participating 6G devices. The network consists of user equipment, IoT devices, intelligent edge nodes, access points, base stations, and a centralized or distributed security controller. Each entity is assigned a unique internal identifier during registration. However, this identifier is not directly transmitted over the wireless channel. The security controller also determines the computational capability of each device, available memory, battery condition, latency requirement, and sensitivity of the information handled by the device. Let the complete set of participating 6G entities be represented by $D = \{D_1, D_2, \dots, D_N\}$. For every device D_i , QRAPSF generates a security profile containing its resource and communication characteristics. The profile is represented by a multidimensional vector containing computational capacity, residual energy, communication latency tolerance, data sensitivity, trust state, and current channel quality. This profile provides the basis for adaptive security selection.

The initial security vector for device D_i is defined as

$$\mathbf{S}_i^{(0)} = [C_i, E_i, L_i, \Delta_i, T_i, Q_i, R_i]^T, D_i \in D,$$

where C_i denotes computational capability, E_i represents available energy, L_i denotes the maximum acceptable security-processing latency, Δ_i represents data sensitivity, T_i denotes the current trust value, Q_i denotes wireless-channel quality, and R_i represents the resource availability of the device. The security controller stores this vector in a protected profile database.

The security profile is subsequently normalized because the parameters have different numerical ranges. Let x_{ij} represent the j^{th} security attribute of device D_i . The normalized value is obtained as

$$\tilde{x}_{ij} = \frac{x_{ij} - \min_{1 \leq k \leq N} x_{kj}}{\max_{1 \leq k \leq N} x_{kj} - \min_{1 \leq k \leq N} x_{kj} + \epsilon}, i = 1, \dots, N, j = 1, \dots, 7,$$

where ϵ is a small positive constant introduced to prevent division by zero. The normalized profile allows QRAPSF to compare heterogeneous devices using a common representation.

3.2 PRIVACY-PRESERVING IDENTITY GENERATION

Direct transmission of a permanent identity may enable tracking, profiling, correlation, and impersonation. QRAPSF therefore generates temporary pseudonymous identities for communication sessions. The permanent identifier remains inside

the trusted security domain, while the wireless network observes only a temporary identifier.

For device D_i , let ID_i denote the permanent identity and K_i^{ID} denote an identity-protection secret maintained by the security controller. A pseudonymous identifier $PID_i^{(t)}$ is generated for session t by applying a keyed cryptographic transformation to the permanent identity and a session-specific nonce. The resulting pseudonym changes periodically, preventing straightforward correlation between sessions. The protected pseudonymous identity is represented as

$$PID_i^{(t)} = \text{HMAC}_{K_i^{ID}}(ID_i \parallel N_i^{(t)} \parallel \tau_t \parallel C_i^{(t)}) \bmod 2^\lambda,$$

where $N_i^{(t)}$ is a cryptographically secure nonce, τ_t is the session timestamp, $C_i^{(t)}$ is a session context value, λ denotes the pseudonym length, and $\parallel$ represents concatenation. The use of a changing nonce and session context produces a different pseudonym across successive communication periods. QRAPSF also maintains a controlled mapping between the temporary pseudonym and the permanent identity. This mapping is never broadcast over the communication channel. If the system detects malicious behavior, the security controller can resolve the pseudonym internally and revoke the associated device without exposing the permanent identity to other network participants. The pseudonym renewal mechanism is expressed as

$$PID_i^{(t+1)} = H(PID_i^{(t)} \parallel N_i^{(t+1)} \parallel K_i^{ID} \parallel \Gamma_i^{(t)}),$$

$$\Gamma_i^{(t)} = [T_i^{(t)}, Q_i^{(t)}, \Delta_i],$$

where H denotes a cryptographic hash function and $\Gamma_i^{(t)}$ represents the current security context. Consequently, even if an adversary observes multiple communication sessions, direct identity correlation becomes substantially more difficult.

3.3 QUANTUM-RESISTANT DEVICE AUTHENTICATION

After generating the pseudonymous identity, QRAPSF performs quantum-resistant authentication. Authentication ensures that only legitimate entities participate in protected communication. The framework uses ML-DSA for digital signatures because it is a standardized post-quantum signature mechanism. During registration, each device obtains an ML-DSA signing and verification key pair. The private signing key remains within the protected device environment, while the verification key is associated with the device's authenticated security record. During session establishment, the device generates a signed authentication token containing the pseudonymous identity, session nonce, timestamp, and relevant security context. The authentication message is expressed as

$$M_i^{(t)} = PID_i^{(t)} \parallel N_i^{(t)} \parallel \tau_t \parallel \text{SID}_t \parallel H(PID_i^{(t)} \parallel N_i^{(t)} \parallel \text{SID}_t),$$

where SID_t denotes the current session identifier. The device then computes an ML-DSA signature over $M_i^{(t)}$:

$$\sigma_i^{(t)} = \text{ML-DSA.Sign}(SK_i^{\text{DSA}}, M_i^{(t)}),$$

$$\text{ML-DSA.Verify}(PK_i^{\text{DSA}}, M_i^{(t)}, \sigma_i^{(t)}) = 1.$$

Authentication succeeds only when the signature verification result equals one and the timestamp and nonce satisfy the freshness constraints. A stale timestamp, repeated nonce, invalid signature, or revoked pseudonym causes the session request to be rejected. The authentication mechanism therefore addresses both identity authenticity and replay resistance. Because the permanent identity is replaced with a temporary pseudonym, successful authentication does not require exposing the permanent identifier to other communication entities.

3.4 QUANTUM-SAFE SESSION-KEY ESTABLISHMENT

Following successful authentication, QRAPSF establishes a shared session key using ML-KEM. The purpose of this stage is to ensure that the symmetric encryption key used for data transmission is established through a quantum-resistant mechanism. The receiving entity generates or maintains an ML-KEM key pair consisting of a public key and a private decapsulation key. The initiating device uses the public key to encapsulate a randomly generated shared secret. The resulting ciphertext is transmitted through the protected communication channel. The receiver subsequently decapsulates the ciphertext using its private key. The encapsulation operation can be represented as

$$(K_{i,j}^{(t)}, CT_{i,j}^{(t)}) = \text{ML-KEM.Encaps}(PK_j^{\text{KEM}}, \rho_{i,j}^{(t)}),$$

where PK_j^{KEM} represents the recipient's ML-KEM public key and $\rho_{i,j}^{(t)}$ denotes fresh randomness. $K_{i,j}^{(t)}$ is the shared secret and $CT_{i,j}^{(t)}$ is the resulting encapsulation ciphertext. The receiver obtains the same secret through decapsulation:

$$K_{j,i}^{(t)} = \text{ML-KEM.Decaps}(SK_j^{\text{KEM}}, CT_{i,j}^{(t)}),$$

$$K_{i,j}^{(t)} \approx K_{j,i}^{(t)}.$$

The shared secret is not directly used as the application encryption key. QRAPSF derives multiple independent session keys using a key-derivation process. Separate keys can therefore be used for payload confidentiality, integrity verification, and metadata protection. This separation limits the consequences of a potential compromise of one cryptographic function. A central component of QRAPSF is the adaptive security controller. Conventional security architectures generally apply a predefined configuration regardless of the current communication condition. Such an approach may unnecessarily consume computational resources during low-risk communication while providing insufficient protection during high-risk situations. QRAPSF evaluates five major factors: threat intensity, data sensitivity, device capability, channel quality, and latency requirement. Let the current network state be represented by

$$\mathbf{Z}^{(t)} = [\Theta^{(t)}, \Delta^{(t)}, \bar{C}^{(t)}, Q^{(t)}, L^{(t)}, T^{(t)}],$$

where $\Theta^{(t)}$ denotes estimated threat intensity, $\Delta^{(t)}$ denotes data sensitivity, $\bar{C}^{(t)}$ represents available computational capacity, $Q^{(t)}$ denotes channel quality, $L^{(t)}$ denotes latency tolerance, and $T^{(t)}$ represents the aggregated trust condition. After the security level is determined, QRAPSF protects application data using the derived session keys. The framework separates sensitive payload

data from non-sensitive operational metadata. Only the minimum metadata required for routing and network operation is exposed.

For a plaintext payload $X_i^{(t)}$, a session-specific nonce $r_i^{(t)}$, and an encryption key $K_E^{(t)}$, the protected data can be represented as

$$C_i^{(t)} = \text{Enc}_{K_E^{(t)}} \left(X_i^{(t)} \square \text{PID}_i^{(t)} \square H(M_i^{(t)}) \right),$$

where $C_i^{(t)}$ denotes the protected communication payload. The construction binds the payload to the authenticated session without revealing the permanent identity. The framework also minimizes metadata leakage by applying controlled aggregation to selected operational attributes. Let $m_i^{(t)}$ denote a metadata vector generated by device D_i . QRAPSF generates a protected metadata representation using a session-specific transformation:

$$\hat{m}_i^{(t)} = P \left(m_i^{(t)}, \text{PID}_i^{(t)}, K_M^{(t)}, \zeta_i^{(t)} \right),$$

$$P^{-1} \left(\hat{m}_i^{(t)}, K_M^{(t)} \right) \rightarrow m_i^{(t)},$$

where P denotes the privacy transformation, $K_M^{(t)}$ denotes the metadata-protection key, and $\zeta_i^{(t)}$ denotes controlled session randomness. This approach reduces unnecessary exposure of device-specific information while preserving the metadata required by authorized network functions.

Cryptographic protection operates above the physical transmission process. QRAPSF therefore adds a physical-layer security component to increase protection against wireless interception. The controller evaluates channel quality, interference, signal-to-noise ratio, and suspicious transmission behavior.

For a legitimate receiver R and potential eavesdropper E , the achievable secrecy rate can be represented as

$$R_s^{(t)} = \left[B \log_2 \left(1 + \frac{P_s^{(t)} h_{s,r}^{(t)}}{I_r^{(t)} + N_r} \right) - B \log_2 \left(1 + \frac{P_s^{(t)} h_{s,e}^{(t)}}{I_e^{(t)} + N_e} \right) \right]^+,$$

where B denotes bandwidth, $P_s^{(t)}$ denotes transmission power, $h_{s,r}^{(t)}$ and $h_{s,e}^{(t)}$ represent channel gains toward the legitimate receiver and eavesdropper, respectively, $I_r^{(t)}$ and $I_e^{(t)}$ denote interference levels, N_r and N_e represent noise power, and $[x]^+ = \max(x, 0)$. QRAPSF adjusts the physical-layer protection according to the observed secrecy condition. A physical-layer security coefficient is calculated as

$$\Omega_{\text{PLS}}^{(t)} = \alpha_1 \tilde{R}_s^{(t)} + \alpha_2 \tilde{Q}^{(t)} + \alpha_3 \tilde{I}^{(t)} + \alpha_4 \tilde{A}^{(t)}, \sum_{k=1}^4 \alpha_k = 1,$$

where $\tilde{R}_s$ denotes normalized secrecy rate, $\tilde{Q}$ denotes channel quality, $\tilde{I}$ represents normalized interference characteristics, and $\tilde{A}$ represents abnormal transmission indicators. A lower value of Ω_{PLS} triggers stronger physical-layer protection.

Security cannot remain static after session establishment because 6G networks operate under changing traffic conditions. QRAPSF therefore continuously monitors network activity. The monitoring module collects authentication failures, packet anomalies, sudden changes in traffic volume, unusual device

mobility, channel abnormalities, repeated key-establishment failures, and unexpected communication patterns.

For device D_i , the threat observation vector is defined as

$$\mathbf{O}_i^{(t)} = [F_i^{(t)}, V_i^{(t)}, A_i^{(t)}, K_i^{(t)}, M_i^{(t)}, H_i^{(t)}],$$

where F_i denotes authentication failures, V_i denotes traffic-volume deviation, A_i denotes anomalous packet behavior, K_i represents abnormal key-establishment events, M_i denotes mobility or location-pattern deviation, and H_i denotes channel-related anomalies.

The adaptive controller continuously compares the current security state with the previously selected configuration. If the threat score increases, the system can increase authentication frequency, reduce pseudonym lifetime, renew session keys, activate stronger privacy protection, and increase physical-layer protection.

The security adaptation cost can be formulated as

$$J^{(t)} = \lambda_1 C^{(t)} + \lambda_2 L^{(t)} + \lambda_3 E^{(t)} + \lambda_4 O^{(t)} + \lambda_5 (1 - S^{(t)}), \sum_{k=1}^5 \lambda_k = 1,$$

where C represents computational cost, L represents latency, E represents energy consumption, O represents communication overhead, and S represents the achieved security level.

The controller selects a security configuration that minimizes the operational cost subject to the minimum required security constraint:

$$A^{(t)*} = \arg \min_{A \in F} J^{(t)}(A) \quad \text{s.t.} \quad S^{(t)}(A) \geq S_{\min}^{(t)}, \quad L^{(t)}(A) \leq L_{\max}^{(t)},$$

where F represents the feasible set of security configurations. This formulation ensures that QRAPSF does not select a stronger security configuration merely because it is available. Instead, it searches for a configuration satisfying the required security condition while considering operational constraints. After security adaptation, the protected payload is transmitted through the 6G communication infrastructure. The receiving node verifies the message integrity before allowing the data to reach the application layer. This procedure prevents corrupted or modified packets from being processed as legitimate information.

For transmitted ciphertext $C_i^{(t)}$, the receiver computes an integrity value using the session-specific integrity key $K_i^{(t)}$:

$$\tau_i^{(t)} = \text{MAC} \left(K_i^{(t)}, C_i^{(t)} \square \text{PID}_i^{(t)} \square N_i^{(t)} \square \text{SID}_i \right).$$

The receiver accepts the packet only when the received integrity value $\tau_i^{(t)}$ corresponds to the locally computed value:

$$A(C_i^{(t)}) = \begin{cases} 1, & \tau_{i,\text{rx}}^{(t)} = \tau_{i,\text{calc}}^{(t)} \wedge N_i^{(t)} \notin N_{\text{used}} \wedge \text{PID}_i^{(t)} \in P_{\text{valid}}, \\ 0, & \text{otherwise.} \end{cases}$$

where, N_{used} denotes the set of previously consumed nonces and P_{valid} denotes the set of currently valid pseudonymous identities. This condition provides simultaneous integrity and replay protection.

Long-lived cryptographic sessions can increase the impact of a compromised key. QRAPSF therefore periodically renews session keys according to elapsed time, transferred data volume, threat level, and security policy. A key renewal event can also be

triggered immediately when the threat controller identifies abnormal behavior. The key-renewal condition is defined as

$$R_K^{(t)} = \mathbf{1} \left[t - t_0 \geq T_K \vee V_{\text{data}}^{(t)} \geq V_K \vee \bar{\Theta}^{(t)} \geq \Theta_K \vee L^{(t)} \neq L^{(t-1)} \right],$$

Where T_K represents the maximum key lifetime, V_K denotes the maximum permitted data volume under one session key, Θ_K denotes the threat threshold, and $\mathbf{1}[\cdot]$ denotes the indicator function.

When renewal is activated, QRAPSF establishes a new ML-KEM-derived secret and generates independent encryption, integrity, and metadata-protection keys. The new key set is represented as

$$\begin{aligned} \mathbf{K}^{(t+1)} &= \text{KDF} \left(K_{\text{KEM}}^{(t+1)} \parallel \text{PID}_i^{(t+1)} \parallel \text{SID}_{t+1} \parallel H(\mathbf{K}^{(t)}) \right) \\ &= \left[K_E^{(t+1)}, K_I^{(t+1)}, K_M^{(t+1)}, K_P^{(t+1)} \right]. \end{aligned}$$

The previous session keys are subsequently invalidated. This forward progression reduces the possibility that compromise of an old session key can be used to access subsequent communication sessions. The overall QRAPSF objective is represented by

$$\begin{aligned} \max_A U_{\text{QRAPSF}} &= \omega_1 S_{\text{sec}} + \omega_2 P_{\text{priv}} + \omega_3 R_{\text{rel}} \\ &\quad + \omega_4 T_{\text{thr}} - \omega_5 C_{\text{comp}} - \omega_6 O_{\text{comm}} - \omega_7 L_{\text{proc}}, \end{aligned}$$

$$\begin{aligned} \text{subject to } S_{\text{sec}} &\geq S_{\text{min}}, P_{\text{priv}} \geq P_{\text{min}}, R_{\text{rel}} \geq R_{\text{min}}, L_{\text{proc}} \leq L_{\text{max}}, \\ E_{\text{device}} &\leq E_{\text{max}}. \end{aligned}$$

where, S_{sec} denotes the achieved security level, P_{priv} represents privacy protection, R_{rel} represents communication reliability, T_{thr} represents threat-response capability, C_{comp} denotes computational cost, O_{comm} denotes communication overhead, and L_{proc} represents processing latency. The constraints ensure that adaptive optimization does not violate the minimum security, privacy, reliability, latency, or energy requirements of the 6G application.

4. RESULTS AND DISCUSSION

The proposed QRAPSF is evaluated through a simulation-based 6G security environment using Python 3.11, NumPy, Pandas, and Scikit-learn on a workstation. The communication environment is modeled using 6G heterogeneous IoT traffic, while post-quantum operations are represented using ML-KEM and ML-DSA security profiles. The experiment varies network load from 5% to 30% in increments of 5%. Three representative approaches from the related works are used for comparison: lattice-based physical-layer security, hybrid PQC authentication, and AI-enabled physical-layer security.

Table.1. Experimental setup and simulation parameters

Parameter	Value
Simulation environment	Python 3.11
Communication model	6G heterogeneous IoT network
Number of devices	100
Number of edge nodes	10
Simulation duration	1000 s
Channel bandwidth	100 MHz

Carrier frequency	28 GHz
Transmission range	250 m
Initial transmission power	23 dBm
Network load	5–30%
Load increment	5%
ML-KEM security mechanism	Quantum-safe key establishment
ML-DSA security mechanism	Post-quantum authentication
Pseudonym renewal interval	60 s
Key renewal threshold	60 s / threat-triggered
Threat levels	Low, medium, high, critical
Attack traffic	5–30%
Packet size	1024 bytes
Evaluation runs	10
Reported value	Mean of simulation runs
Random seed	42

As shown in Table.1, the simulation maintains identical network conditions for all four methods and changes only the security mechanism under evaluation. Ten independent runs are performed at every load level, and the mean value is reported to reduce the influence of random traffic variation.

4.1 DATASET DESCRIPTION

The UNSW-NB15 dataset is used as the primary network-security dataset because it contains normal and malicious network traffic with multiple attack categories and flow-level characteristics. The dataset contains 49 features and nine attack categories, including Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms. The dataset is preprocessed by removing non-informative identifiers, handling categorical attributes through encoding, normalizing numerical features, and mapping attack categories to legitimate and malicious classes. The resulting samples are incorporated into the simulated 6G traffic environment.

Table.2. UNSW-NB15 dataset description

Dataset characteristic	Description
Dataset	UNSW-NB15
Domain	Network intrusion detection
Traffic type	Normal and malicious
Original feature count	49
Attack categories	9
Major attack classes	Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms
Numerical attributes	Continuous network-flow features
Categorical attributes	Protocol and service-related attributes
Preprocessing	Encoding, normalization, feature cleaning
Classification task	Normal vs. attack

Application in this study	6G security-threat simulation
Dataset role	Threat detection and security evaluation

The characteristics summarized in Table 2 provide the traffic foundation for evaluating the threat-monitoring component of QRAPSF. The dataset is not treated as a direct representation of deployed 6G traffic. Instead, its attack patterns are mapped into the simulated heterogeneous 6G communication environment. Various methods are selected from the reviewed literature for comparative evaluation. Lattice-Based Physical-Layer Security represents quantum-resistant wireless protection using lattice-based encryption. Hybrid PQC Authentication represents post-quantum authentication and key-agreement mechanisms designed for 6G. AI-Enabled Physical-Layer Security represents intelligent physical-layer protection that adapts security decisions according to wireless conditions. QRAPSF integrates these security principles with privacy-preserving identity management and adaptive security selection.

Table.3. Attack detection accuracy (%) at different network loads

Network Load (%)	Lattice-Based Physical-Layer Security	Hybrid PQC Authentication	AI-Enabled Physical-Layer Security	QRAPSF
5	91.42	92.16	93.08	96.24
10	90.87	91.73	92.64	95.81
15	90.15	91.24	92.11	95.37
20	89.36	90.58	91.43	94.92
25	88.47	89.74	90.61	94.38
30	87.51	88.92	89.74	93.81

The Table.3 demonstrates that attack detection accuracy decreases as network load increases for all four methods. Lattice-Based Physical-Layer Security decreases from 91.42% at 5% load to 87.51% at 30% load, representing a reduction of 3.91 percentage points. Hybrid PQC Authentication decreases from 92.16% to 88.92%, while AI-Enabled Physical-Layer Security decreases from 93.08% to 89.74%. QRAPSF shows a smaller reduction, from 96.24% to 93.81%, corresponding to 2.43 percentage points. At 30% network load, QRAPSF records 93.81%, which is 5.89 percentage points above Lattice-Based Physical-Layer Security, 4.89 percentage points above Hybrid PQC Authentication, and 4.07 percentage points above AI-Enabled Physical-Layer Security. At 15% load, QRAPSF achieves 95.37%, whereas the three existing methods obtain 90.15%, 91.24%, and 92.11%, respectively. The relatively smaller degradation of QRAPSF is attributed to its continuous threat monitoring and adaptive security-level selection. Instead of relying on a fixed security configuration, QRAPSF responds to increasing traffic abnormalities by modifying its security profile. The results therefore indicate that the proposed architecture maintains more sTable.threat-detection performance as communication load increases.

Table.4. Authentication success rate (%) at different network loads

Network Load (%)	Lattice-Based Physical-Layer Security	Hybrid PQC Authentication	AI-Enabled Physical-Layer Security	QRAPSF
5	94.18	95.26	94.73	98.31
10	93.52	94.84	94.21	98.02
15	92.77	94.17	93.65	97.68
20	91.94	93.46	92.91	97.21
25	90.83	92.71	92.06	96.73
30	89.76	91.88	91.17	96.19

The authentication results in Table.4 indicate that QRAPSF maintains the highest authentication success rate across all network-load conditions. At 5% load, the proposed framework achieves 98.31%, compared with 94.18% for Lattice-Based Physical-Layer Security, 95.26% for Hybrid PQC Authentication, and 94.73% for AI-Enabled Physical-Layer Security. When the load reaches 30%, the respective values become 96.19%, 89.76%, 91.88%, and 91.17%. QRAPSF consequently experiences a reduction of only 2.12 percentage points between 5% and 30% load. In comparison, the reductions are 4.42, 3.38, and 3.56 percentage points for the three existing approaches. The difference is associated with the combination of pseudonymous identity management, ML-DSA authentication, freshness verification, and adaptive session management. At 20% load, QRAPSF reaches 97.21%, which is 5.27 percentage points higher than Lattice-Based Physical-Layer Security and 3.75 percentage points higher than Hybrid PQC Authentication. The results indicate that increasing traffic load causes more authentication contention and communication delay in every method. QRAPSF limits this degradation by adapting authentication and session-management operations according to the current network state.

Table.5. Privacy-preservation efficiency (%) at different network loads

Network Load (%)	Lattice-Based Physical-Layer Security	Hybrid PQC Authentication	AI-Enabled Physical-Layer Security	QRAPSF
5	86.73	89.15	87.92	95.14
10	85.94	88.67	87.31	94.72
15	85.08	87.91	86.64	94.26
20	84.16	87.12	85.88	93.74
25	83.21	86.28	85.07	93.18
30	82.37	85.46	84.19	92.61

The privacy-preservation results in Table.5 show that QRAPSF provides higher privacy-preservation efficiency across all evaluated network loads. At 5% load, the proposed method reaches 95.14%, while Lattice-Based Physical-Layer Security, Hybrid PQC Authentication, and AI-Enabled Physical-Layer Security achieve 86.73%, 89.15%, and 87.92%, respectively. At

30% load, QRAPSF maintains 92.61%, whereas the corresponding values of the existing methods decline to 82.37%, 85.46%, and 84.19%. The proposed method therefore loses only 2.53 percentage points as network load increases from 5% to 30%. The reductions for the three existing methods are 4.36, 3.69, and 3.73 percentage points. The difference is related to QRAPSF's privacy-preserving pseudonymous identity mechanism, which prevents permanent identifiers from being repeatedly exposed during communication. The independent metadata-protection key also separates privacy protection from payload encryption. At 15% load, QRAPSF records 94.26%, exceeding the three comparison methods by 9.18, 6.35, and 7.62 percentage points, respectively. At 25% load, the proposed value remains above 93%, whereas all existing methods fall below 87%. These results suggest that privacy protection is more stable under increasing traffic when identity management and metadata protection are integrated directly into the security architecture. The gradual reduction in all methods indicates that heavier traffic still increases the opportunity for metadata exposure and communication correlation, but QRAPSF limits the degradation through dynamic pseudonym renewal and adaptive protection.

Table.6. Communication overhead (%) at different network loads

Network Load (%)	Lattice-Based Physical-Layer Security	Hybrid PQC Authentication	AI-Enabled Physical-Layer Security	QRAPSF
5	12.84	11.76	13.18	9.42
10	13.57	12.43	13.84	9.86
15	14.31	13.16	14.57	10.28
20	15.12	13.94	15.36	10.73
25	16.04	14.82	16.21	11.19
30	17.08	15.76	17.15	11.68

The communication-overhead results in Table.6 show an increasing overhead trend as network load increases. At 5% load, Lattice-Based Physical-Layer Security produces 12.84% overhead, Hybrid PQC Authentication produces 11.76%, and AI-Enabled Physical-Layer Security produces 13.18%. QRAPSF records 9.42%, indicating that its adaptive control mechanism limits security-related communication traffic. At 30% load, the overhead values increase to 17.08%, 15.76%, 17.15%, and 11.68% for the four methods, respectively. QRAPSF therefore remains 5.40 percentage points below Lattice-Based Physical-Layer Security, 4.08 percentage points below Hybrid PQC Authentication, and 5.47 percentage points below AI-Enabled Physical-Layer Security. From 5% to 30% load, QRAPSF increases by only 2.26 percentage points, whereas the increases for the existing methods are 4.24, 4.00, and 3.97 percentage points. The lower overhead is primarily associated with adaptive security activation. QRAPSF does not continuously transmit maximum-security control information when the threat condition does not require it. Instead, security messages, pseudonym renewal, key renewal, and additional protection are activated according to the security state. The results also demonstrate that quantum-resistant protection does not necessarily require a

uniformly high communication overhead when the cryptographic mechanisms are integrated with adaptive control. The proposed architecture consequently maintains lower additional traffic throughout the tested load range.

Table.7. Authentication latency (ms) at different network loads

Network Load (%)	Lattice-Based Physical-Layer Security	Hybrid PQC Authentication	AI-Enabled Physical-Layer Security	QRAPSF
5	38.42	34.76	36.85	29.84
10	40.18	36.24	38.47	31.16
15	42.31	38.17	40.26	32.54
20	44.67	40.31	42.18	34.08
25	47.26	42.64	44.73	35.71
30	50.14	45.28	47.36	37.42

The authentication-latency results in Table.7 show that latency increases with network load for all evaluated approaches. At 5% load, Lattice-Based Physical-Layer Security requires 38.42 ms, Hybrid PQC Authentication requires 34.76 ms, and AI-Enabled Physical-Layer Security requires 36.85 ms, while QRAPSF requires 29.84 ms. At 30% load, the corresponding values become 50.14, 45.28, 47.36, and 37.42 ms. QRAPSF consequently limits authentication latency to below 38 ms throughout the tested load range. Its latency increases by 7.58 ms from 5% to 30% load, compared with increases of 11.72, 10.52, and 10.51 ms for the three existing approaches. At 30% load, QRAPSF reduces latency by 12.72 ms relative to Lattice-Based Physical-Layer Security, 7.86 ms relative to Hybrid PQC Authentication, and 9.94 ms relative to AI-Enabled Physical-Layer Security. The lower latency is attributed to adaptive security selection and separation of authentication from unnecessary security operations. QRAPSF establishes the quantum-safe session key after successful authentication and does not continuously execute the strongest available protection profile for every request. The use of cached security profiles and controlled pseudonym renewal also reduces repeated processing. The results indicate that increasing traffic produces unavoidable queueing and processing effects, but QRAPSF limits the resulting latency growth. This behavior is particularly relevant to latency-sensitive 6G services in which security processing must coexist with stringent communication-delay requirements.

5. CONCLUSION

This study presents QRAPSF, a quantum-resilient adaptive privacy security framework designed for heterogeneous 6G communication systems. The framework integrates ML-KEM-based key establishment, ML-DSA authentication, pseudonymous identity management, adaptive security selection, physical-layer protection, continuous threat monitoring, and dynamic key renewal. The experimental evaluation uses a simulated 6G environment and UNSW-NB15-based attack traffic to examine security and communication behavior under network loads ranging from 5% to 30%. The results show that QRAPSF achieves 96.24% to 93.81% attack detection accuracy, 98.31% to

96.19% authentication success, and 95.14% to 92.61% privacy-preservation efficiency as network load increases from 5% to 30%. Communication overhead increases from 9.42% to 11.68%, while authentication latency increases from 29.84 ms to 37.42 ms. The relatively gradual changes across the five metrics indicate that the adaptive mechanism limits performance degradation under increasing traffic. The framework demonstrates how quantum-resistant cryptography can be combined with privacy and adaptive wireless security rather than being deployed as an isolated cryptographic layer. The results also indicate that security mechanisms for 6G should account for device resources, traffic conditions, threat intensity, and latency requirements simultaneously. Future experimental validation with real 6G testbeds, standardized PQC implementations, larger heterogeneous datasets, and hardware-constrained IoT devices can further establish the practical behavior of QRAPSF.

REFERENCES

- [1] J. Wang, L. Liu, S. Lyu, Z. Wang, M. Zheng, F. Lin and C. Ling, "Quantum-Safe Cryptography: Crossroads of Coding Theory and Cryptography", *Science China Information Sciences*, Vol. 65, No. 1, pp. 1-7, 2021.
- [2] T. Karthikeyan and N.V. Kousik, "Improved Privacy Preservation Framework for Cloud-Based Internet of Things", CRC Press, 2020.
- [3] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F.D. Pinuaga, O. Lacombe and R. Hansen, "Transitioning Organizations to Post-Quantum Cryptography", *Nature*, Vol. 605, No. 7909, pp. 237-243, 2024.
- [4] K. Seyhan and S. Akleylek, "Post-Quantum Cryptography: A Snapshot of Standardization Efforts", *Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems*, Vol. 9, pp. 90-99, 2021.
- [5] B. Mao, J. Liu, Y. Wu and N. Kato, "Security and Privacy on 6G Network Edge: A Survey", *IEEE Communications Surveys and Tutorials*, Vol. 25, No. 2, pp. 1095-1127, 2018.
- [6] K. Ramezanpour, J. Jagannath and A. Jagannath, "Security and Privacy Vulnerabilities of 5G/6G and WiFi 6: Survey and Research Directions from a Coexistence Perspective", *Computer Networks*, Vol. 221, pp. 1-7, 2023.
- [7] B. Yuan, F. Wu and Z. Zheng, "Post Quantum Blockchain Architecture for Internet of Things over NTRU Lattice", *Plos One*, Vol. 18, No. 2, pp. 1-6, 2021.
- [8] M.S. Akbar, Z. Hussain, M. Ikram, Q.Z. Sheng and S.C. Mukhopadhyay, "On Challenges of Sixth-Generation (6G) Wireless Networks: A Comprehensive Survey of Requirements, Applications and Security Issues", *Journal of Network and Computer Applications*, Vol. 233, pp. 1-11, 2021.
- [9] W. Abdallah, "A Physical Layer Security Scheme for 6G Wireless Networks using Post-Quantum Cryptography", *Computer Communications*, Vol. 218, pp. 176-187, 2019.
- [10] S. Zhang, D. Zhu and Y. Liu, "Artificial Intelligence Empowered Physical Layer Security for 6G: State-of-the-Art, Challenges and Opportunities", *Computer Networks*, Vol. 242, pp. 1-13, 2024.
- [11] S.H.A. Kazmi, F. Qamar, R. Hassan, K. Nisar and M.A. Al-Betar, "Security of Federated Learning in 6G Era: A Review on Conceptual Techniques and Software Platforms used for Research and Analysis", *Computer Networks*, Vol. 245, pp. 1-11, 2024.
- [12] K.M. Sameera, S. Nicolazzo, M. Arazzi, A. Nocera, P. Vinod and M. Conti, "Privacy-Preserving in Blockchain-based Federated Learning Systems", *Computer Communications*, Vol. 222, pp. 38-67, 2024.
- [13] P.R. Babu, S.A. Kumar, A.G. Reddy and A.K. Das, "Quantum Secure Authentication and Key Agreement Protocols for IoT-Enabled Applications: A Comprehensive Survey and Open Challenges", *Computer Science Review*, Vol. 54, pp. 1-7, 2023.
- [14] T.N. Turnip, B. Andersen and C. Vargas-Rosales, "Toward 6G Authentication and Key Agreement Protocol: A Survey on Hybrid Post Quantum Cryptography", *IEEE Communications Surveys and Tutorials*, Vol. 28, pp. 3311-3345, 2025.
- [15] C. De Alwis, O. Aouedi, J. Xu, S. Wang, Y. Siriwardhana, T. Hewa and M. Liyanage, "Federated Learning for 6G Security: A Survey on Threats, Solutions and Research Directions", *IEEE Communications Surveys and Tutorials*, Vol. 8, pp. 1-13, 2025.