A PQC-Aware Secure Communication Architecture for NB-IoT: Control-Plane Post-Quantum Onboarding with Lightweight Data-Plane Protection

Thi-Bac Do
Thai Nguyen University of Information and Communication Technology, Thai Nguyen, Vietnam
dtbac@ictu.edu.vn (corresponding author)

Received: 28 December 2025 | Revised: 8 February 2026, 25 February 2026, and 28 February 2026 | Accepted: 4 March 2026

 DOI: https://doi.org/10.48084/etasr.17220

ABSTRACT

The advent of large-scale quantum computing poses a fundamental threat to widely deployed public-key cryptographic mechanisms, particularly in Internet of Things (IoT) systems with long operational lifetimes and limited upgrade capabilities. Narrowband Internet of Things (NB-IoT), as a representative Low-Power Wide-Area Network (LPWAN) technology, is especially vulnerable to this transition due to its strict constraints on packet size, bandwidth, and Radio-Frequency (RF) energy consumption. Although Post-Quantum Cryptography (PQC) has progressed rapidly through standardization efforts led by the National Institute of Standards and Technology (NIST), the direct and frequent application of PQC primitives in NB-IoT communication remains impractical. Large ciphertexts and digital signatures, although cryptographically sound, conflict with the fundamental design principles of LPWANs and may significantly degrade reliability, scalability, and device lifetime. This paper proposes a PQC-aware secure communication architecture for NB-IoT that reconciles long-term quantum resistance with the operational realities of constrained radio networks. Rather than treating PQC as a drop-in replacement for classical public-key cryptography, the proposed design adopts a two-plane security architecture that explicitly separates control-plane onboarding from data-plane communication. Post-quantum primitives are confined to infrequent onboarding operations, where higher overhead can be tolerated, while routine data transmission relies exclusively on lightweight symmetric authenticated encryption. Specifically, the architecture employs CRYSTALS-Kyber for post-quantum key encapsulation and CRYSTALS-Dilithium for device authentication during onboarding, selected for their standardization status and comparatively compact message sizes. After onboarding, all data traffic is protected using ChaCha20-Poly1305, combined with a key-derivation-based ratcheting mechanism that provides per-message forward secrecy without recurring PQC overhead. This design is explicitly aligned with NIST guidance on the intended use of post-quantum signatures and the constraints of LPWAN deployments. The proposed framework was implemented and evaluated on an ESP32-based NB-IoT platform with a commercial cellular module. Experimental results demonstrate that post-quantum onboarding can be completed within NB-IoT packet-size constraints with acceptable reliability, while routine data transmission incurs minimal computational, bandwidth, and energy overhead. The findings confirm that quantum-resistant security for NB-IoT is achievable only when PQC is applied selectively and system-aware, rather than uniformly across all communication phases.

Keywords-Post-Quantum Cryptography (PQC); NB-IoT; LPWAN security; PQC-aware architecture; Kyber; Dilithium; ChaCha20-Poly1305; IoT onboarding; forward secrecy

I. INTRODUCTION

The security of modern digital infrastructure fundamentally relies on public-key cryptography to provide authentication, confidentiality, and integrity guarantees. Classical schemes such as RSA and Elliptic-Curve Cryptography (ECC) underpin today's Internet, cellular networks, and large-scale Internet of Things (IoT) deployments. However, the advent of large-scale quantum computing poses a fundamental threat to these mechanisms, as Shor's algorithm enables polynomial-time attacks against both RSA and ECC. Recognizing this risk, governmental, industrial, and standardization bodies have emphasized the urgency of transitioning to quantum-resistant security mechanisms for systems requiring long-term confidentiality and authenticity [1, 2]. This transition is particularly critical for IoT systems, where devices are typically deployed for long operational lifetimes—often exceeding a decade—and are rarely updated once installed. In

such environments, the threat of harvest-now, decrypt-later attacks is no longer hypothetical: encrypted traffic collected today may be retroactively compromised once cryptographically relevant quantum computers become available [1].

Among IoT connectivity technologies, the Narrowband Internet of Things (NB-IoT) represents one of the most challenging environments for post-quantum security. As a Low-Power Wide-Area Network (LPWAN) standardized by 3GPP, NB-IoT is designed for ultra-low data rates, small payload sizes, and multi-year battery lifetimes. These characteristics impose severe constraints on packet size, bandwidth availability, and Radio-Frequency (RF) energy consumption. Previous studies consistently show that communication overhead dominates computational cost, and that even modest increases in transmitted data can significantly degrade reliability, scalability, and device lifetime [3].

Substantial progress has been made in the standardization of post-quantum cryptographic primitives. The National Institute of Standards and Technology (NIST) has finalized lattice-based key encapsulation mechanisms and digital signature standards, as well as stateless hash-based signatures [4, 5]. However, compared to classical ECC-based mechanisms, PQC schemes typically involve larger public keys, ciphertexts, or signatures, raising concerns about their suitability for constrained wireless environments such as NB-IoT [3-8].

A growing body of research has demonstrated that PQC primitives are computationally feasible on resource-constrained platforms. Hardware accelerators for lattice-based cryptography significantly reduce latency and energy consumption [1, 4], while optimized software implementations on microcontroller-class devices show that memory footprint and execution time can be reduced to levels compatible with embedded deployment [5-8]. A recent comprehensive review further emphasizes that lattice-based schemes stand out among PQC candidates for IoT due to their favorable trade-offs between security, key size, and computational efficiency [6]. However, these studies largely abstract away system-level considerations. In NB-IoT and other LPWAN technologies, the cost of transmitting cryptographic artifacts—particularly large public keys, ciphertexts, or signatures—often outweighs the local computational cost. Packet fragmentation, retransmissions, and RF energy usage play a dominant role in determining reliability and lifetime [3].

Another relevant line of work addresses secure bootstrapping and authentication in cellular and IoT systems. Prior studies have shown that insecure or poorly scoped onboarding mechanisms represent a fundamental weakness in cellular networks, enabling impersonation, downgrade, and fake base-station attacks [9]. In response, improved bootstrapping and authentication protocols have been proposed for 5G and IoT environments, including transitional solutions under post-quantum threat models [10]. These works highlight that initial trust establishment is a security-critical phase and that weaknesses at the control plane can undermine the entire security architecture.

At the same time, most existing approaches either rely on classical cryptography or treat post-quantum mechanisms as direct replacements for existing public-key schemes. Such designs often assume that post-quantum authentication and key exchange can be performed repeatedly or on demand, without fully accounting for the communication overhead imposed by large PQC artifacts. This assumption conflicts with the operational realities of NB-IoT, where frequent transmission of large cryptographic messages is incompatible with payload size limits, energy budgets, and long-term reliability.

Industry-oriented analyses and migration roadmaps explicitly emphasize this mismatch. Studies on constrained radio networks stress that small ciphertexts, signatures, and minimal interaction rounds are essential for scalable LPWAN deployments [3]. Performance evaluations of PQC algorithms similarly note that message size and communication overhead remain significant barriers to deployment in constrained networks [8]. Standards and regulatory bodies have therefore advocated for incremental, architecture-aware adoption of post-quantum cryptography in cellular systems, rather than uniform substitution of cryptographic primitives [10-12]. NIST guidance further notes that certain post-quantum signatures are best suited for infrequent operations due to their message size [5].

Despite these insights, existing literature falls short of proposing concrete, deployable security architectures that reconcile post-quantum requirements with the stringent communication constraints of NB-IoT. Prior work typically focuses either on algorithmic feasibility, cryptographic performance, or high-level migration strategies, without integrating cryptographic choices into an end-to-end NB-IoT communication model. In particular, the distinction between infrequent control-plane operations and frequent data-plane communication is rarely reflected explicitly in post-quantum security designs.

Motivated by this gap, this paper argues that quantum-resistant security for NB-IoT must be achieved through a PQC-aware system architecture rather than by treating post-quantum cryptography as a drop-in replacement for classical public-key mechanisms. The core design principle is a clear separation between control-plane security, which occurs infrequently and can tolerate higher overhead, and data-plane protection, which must remain lightweight, reliable, and energy-efficient. Post-quantum cryptographic primitives are therefore confined to onboarding and initial trust establishment, where their cost can be amortized over long operational lifetimes, while routine data communication relies exclusively on efficient symmetric authenticated encryption.

Unlike prior studies that evaluate post-quantum cryptography primarily at the algorithmic level or treat it as a direct replacement for classical public-key mechanisms, this work approaches post-quantum security in NB-IoT as a system-architecture problem. The proposed design explicitly aligns cryptographic strength with communication frequency, lifecycle constraints, and operational realities of constrained radio networks. Specifically, this paper makes the following contributions:

1. Architectural contribution: Proposes a PQC-aware secure communication architecture for NB-IoT that introduces a strict separation between control-plane onboarding and data-plane communication, confining post-quantum cryptographic mechanisms to infrequent trust-establishment phases rather than applying them uniformly across all communication stages.
2. System-level integration: Demonstrates how NIST-standardized lattice-based post-quantum primitives can be integrated into NB-IoT onboarding without violating packet-size, reliability, or energy constraints, while routine data transmission remains lightweight through symmetric authenticated encryption combined with key-derivation-based ratcheting.
3. Practical validation: Implements and evaluates the proposed architecture on a representative NB-IoT platform, providing system-level evidence that quantum-resistant security is feasible in LPWAN environments only when post-quantum cryptography is applied selectively and with awareness of communication frequency and device lifecycle.

II. SYSTEM ARCHITECTURE AND PROTOCOL DESIGN

Unlike existing post-quantum security proposals that apply cryptographic mechanisms uniformly across protocol layers, the proposed architecture is explicitly driven by communication frequency and lifecycle considerations. The central design decision is a strict separation between control-plane onboarding, which is security-critical but infrequent, and data-plane communication, which is frequent and highly constrained. This distinction enables post-quantum cryptographic mechanisms to be deployed where their cost can be amortized over long operational lifetimes, while preserving lightweight and efficient protection for routine NB-IoT data transmission.

The design of secure communication mechanisms for NB-IoT systems must reconcile stringent radio constraints with the emerging requirement for long-term, quantum-resistant security. Prior studies on LPWAN and cellular IoT security have consistently shown that communication overhead, rather than computation, dominates system cost and energy consumption [3, 8]. At the same time, recent post-quantum migration guidelines emphasize the necessity of introducing quantum-resistant mechanisms in a controlled and incremental manner, particularly for long-lived devices [11, 12].

Motivated by these observations, this study proposes a PQC-aware secure communication architecture that explicitly separates infrequent trust establishment from frequent data transmission. Figure 1 shows an overview of the proposed architecture, while Table I summarizes the corresponding mapping between architectural phases, cryptographic mechanisms, and operational characteristics.

A. Architectural Overview

As illustrated in Figure 1, the proposed architecture adopts a two-phase communication model consisting of a control plane and a data plane, each with distinct security objectives and operational constraints. This separation reflects established design principles for constrained wireless networks, where security mechanisms must be tailored to message size, transmission frequency, and device lifecycle [3, 12]. The control plane is responsible for device onboarding and long-term trust establishment, while the data plane supports routine application-layer communication. By confining post-quantum cryptographic mechanisms to the control plane, the architecture avoids imposing excessive overhead on high-frequency NB-IoT data transmissions.

B. Control-Plane PQC-Based Onboarding

The control plane implements a post-quantum secure onboarding procedure that provides strong device authentication and establishes a long-term shared secret between the device and the network-side onboarding service. This procedure leverages NIST-standardized lattice-based cryptographic primitives, which have been shown to offer favorable trade-offs between security level and message size for constrained environments [10, 13, 14].

As depicted in Figure 1, control-plane onboarding is performed infrequently—typically at initial deployment or during rare re-onboarding events triggered by operator policy. Because these events occur on the order of years rather than hours or days, the larger message sizes associated with post-quantum signatures and key encapsulation mechanisms remain compatible with NB-IoT operational constraints [3]. Table I lists the specific cryptographic primitives and their roles during this phase.

TABLE I. CRYPTOGRAPHIC PRIMITIVES USED IN THE PROPOSED PQC-AWARE NB-IOT SECURITY ARCHITECTURE AND THEIR FUNCTIONAL ROLES.

Primitive	Standard	Used in	Purpose	Rationale for Selection
CRYSTALS-Kyber	NIST FIPS 203 [12]	Control Plane (Onboarding)	Post-quantum key encapsulation	Compact ciphertexts among PQC KEMs; standardized; suitable for infrequent use
CRYSTALS-Dilithium	NIST FIPS 204 [10]	Control Plane (Authentication)	Device authentication	Strong security guarantees; smaller signatures than hash-based alternatives
ChaCha20-Poly1305	RFC 8439 / widely deployed	Data Plane	Authenticated encryption	High performance on constrained MCUs; constant-time; small overhead
HKDF	RFC 5869	Data Plane	Key derivation & ratcheting	Enables forward secrecy without public-key operations
Device Identifier	3GPP / vendor-defined	Control Plane	Device binding	Prevents impersonation during onboarding

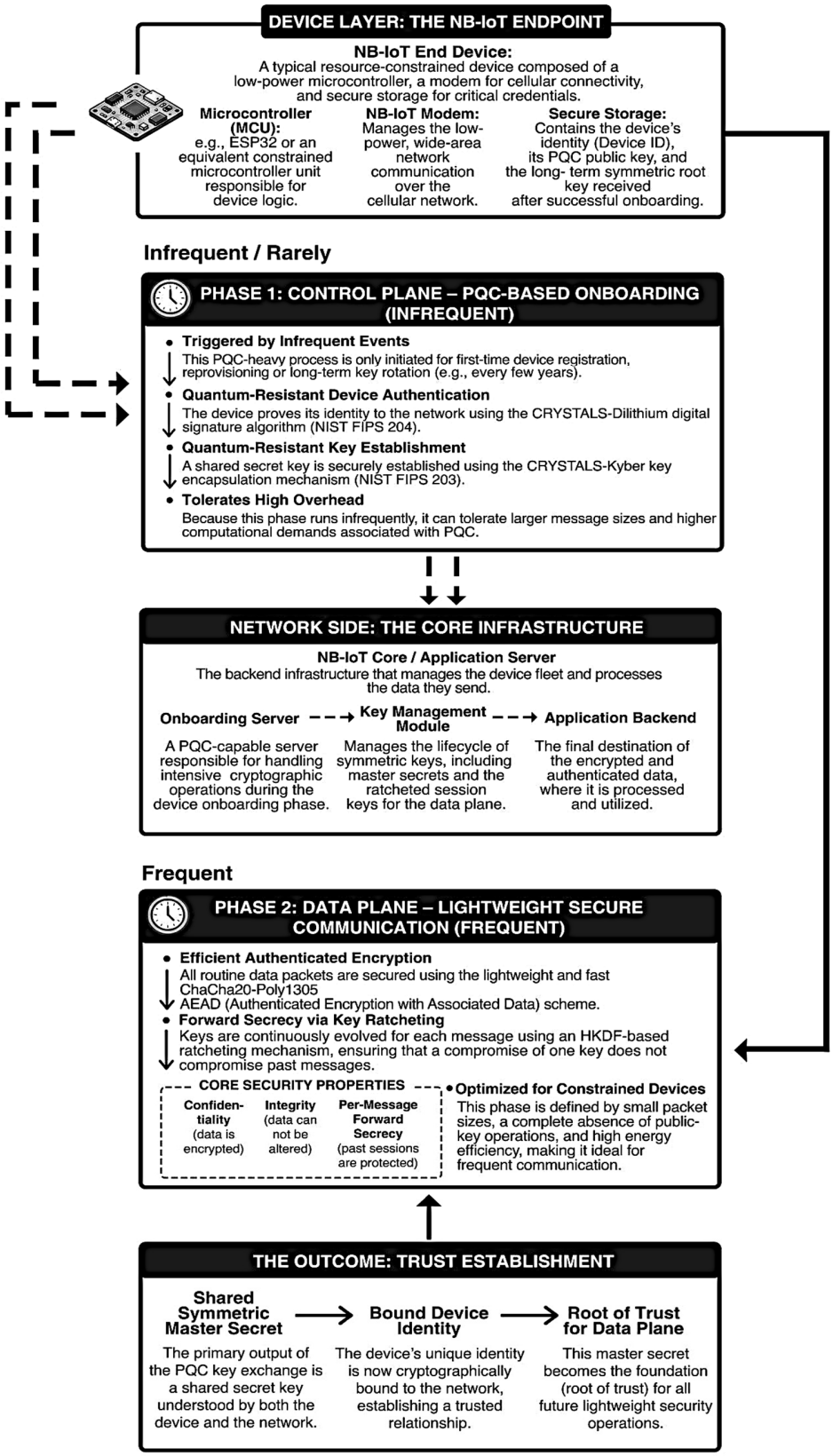

Fig. 1. PQC-aware secure communication architecture for NB-IoT. Post-quantum cryptographic primitives are confined to infrequent control-plane onboarding operations, while routine data-plane communication relies exclusively on lightweight symmetric authenticated encryption with key ratcheting.

C. Data-Plane Lightweight Secure Communication

Following successful onboarding, all routine communication is handled within the data plane. In contrast to the control plane, data-plane messages are transmitted frequently and must therefore incur minimal cryptographic overhead. Consistent with prior analyses of LPWAN security, the proposed architecture employs lightweight symmetric authenticated encryption to protect data-plane traffic [3]. As shown in Figure 1, data-plane keys are derived locally from the control-plane master secret and updated through key ratcheting mechanisms, providing forward secrecy without requiring additional over-the-air key exchanges. This design ensures confidentiality and integrity while preserving compatibility with NB-IoT payload size and energy constraints.

D. Key Management and Device Lifecycle Considerations

NB-IoT devices are often deployed with operational lifetimes exceeding ten years, making key management a central design concern. Post-quantum migration studies emphasize that frequent cryptographic reconfiguration is impractical in such environments and should be avoided whenever possible [1, 12]. The proposed architecture addresses this challenge by decoupling long-term trust establishment from routine data transmission. As summarized in Table I, post-quantum cryptographic mechanisms are invoked only during control-plane operations, while data-plane security relies on efficiently renewable symmetric keys. This approach supports conservative key management policies and minimizes operational disruption over the device lifecycle.

E. Design Rationale and Discussion

This selective deployment aligns with constrained-network analyses emphasizing incremental adoption and overhead management [1, 3, 12].

III. SECURITY ANALYSIS

This section analyzes the security properties of the proposed PQC-aware NB-IoT architecture under a well-defined threat model. The analysis focuses on both classical and quantum-capable adversaries and evaluates how the architecture achieves its stated security goals while respecting the constraints of constrained radio networks.

A. Threat Model

A powerful adversary with the following capabilities is considered, consistent with prior analyses of cellular and IoT security [9, 10]:

1. Network-level adversary: The adversary can eavesdrop on, inject, replay, delay, and drop NB-IoT messages over the wireless channel.
2. Active impersonation: The adversary may attempt to impersonate a legitimate NB-IoT device or network entity, including the use of rogue or fake base stations.
3. Device compromise: The adversary may compromise an NB-IoT end device at some point during its operational lifetime and obtain its current cryptographic state.
4. Long-term passive collection: The adversary may record encrypted traffic for extended periods with the intention of decrypting it in the future (harvest-now, decrypt-later).
5. Quantum-capable adversary: The adversary is assumed to have access to a cryptographically relevant quantum computer capable of breaking classical public-key schemes such as RSA and ECC, but not symmetric cryptography with adequate key sizes, nor standardized post-quantum primitives [1, 2].

Denial-of-Service (DoS) attacks are considered out of scope, as they are inherent to LPWAN environments and cannot be fully mitigated through cryptography alone.

B. Security Goals

Under this threat model, the proposed architecture aims to achieve the following security properties:

- G1: Quantum-resistant device authentication
- G2: Confidentiality and integrity of data-plane communication
- G3: Forward secrecy for routine data transmission
- G4: Resilience to long-term key compromise
- G5: Limited attack surface under device compromise

C. Control-Plane Security Guarantees

During onboarding, device authentication is performed using CRYSTALS-Dilithium, a lattice-based digital signature scheme standardized by NIST. Under standard hardness assumptions for module lattices, Dilithium remains secure against both classical and quantum adversaries. Consequently, an attacker cannot forge valid authentication messages without access to the device's private signing key. This mechanism directly mitigates impersonation attacks and rogue base-station scenarios identified in prior cellular security analyses [9, 10].

The establishment of a shared master secret relies on CRYSTALS-Kyber, standardized in NIST FIPS 203 [13]. Kyber provides indistinguishability under chosen-ciphertext attacks (IND-CCA) and remains secure against quantum adversaries under the Learning-With-Errors (LWE) assumption. Even if onboarding traffic is passively recorded, a future quantum adversary cannot retroactively derive the master secret. This property directly addresses harvest-now, decrypt-later threats for long-lived NB-IoT deployments [1].

Importantly, post-quantum cryptographic operations are confined to infrequent control-plane interactions. As shown in Figure 2 and Table II, the limited frequency of onboarding significantly reduces the exposure surface of PQC-related messages, while still providing a quantum-resistant root of trust. This design choice aligns with NIST guidance that certain post-quantum signatures are best suited for infrequent operations due to their message size [15].

D. Data-Plane Security Guarantees

All data-plane messages are protected using ChaCha20-Poly1305, providing Authenticated Encryption with Associated Data (AEAD). When used with fresh, unpredictable keys derived from the control-plane master secret, ChaCha20-Poly1305 provides strong confidentiality and integrity guarantees against both classical and quantum adversaries. As symmetric cryptography with sufficient key length is believed to remain secure in the post-quantum era, these guarantees are not weakened by quantum advances [2].

The proposed architecture achieves per-message forward secrecy through an HKDF-based key ratcheting mechanism. After each successfully authenticated message, fresh encryption keys are derived, and previous keys are irreversibly discarded. As a result, compromise of a device at time t does not enable decryption of messages transmitted before t. This property substantially limits the value of long-term passive traffic collection and reduces the impact of delayed compromise.

Authenticated encryption inherently prevents message modification and forgery. Replay attacks are mitigated through the use of monotonically evolving keys and implicit freshness guarantees provided by the ratcheting mechanism. An adversary replaying old ciphertexts cannot produce valid authentication tags under the current key state.

E. Device Compromise and Damage Containment

This study considered the case where an adversary compromises a device and obtains its current cryptographic state, including data-plane keys:

- Past communication remains protected due to forward secrecy.
- Future communication can be re-secured through re-onboarding or key rotation, which re-establishes a fresh post-quantum root of trust.
- Lateral movement to other devices is prevented, as each device maintains an independent cryptographic state.

This damage-containment property is particularly important in large-scale NB-IoT deployments, where physical access to individual devices cannot be ruled out.

F. Limitations and Residual Risks

The proposed architecture does not claim to eliminate all risks. Real-time revocation remains challenging in NB-IoT due to connectivity constraints; prolonged device compromise may expose future data until re-onboarding occurs, and denial-of-service attacks remain largely unmitigated. These limitations are inherent to LPWAN environments and are consistent with observations in prior cellular and IoT security research [3].

G. Summary of Security Properties

The architecture achieves quantum-resistant authentication and efficient data-plane security while respecting NB-IoT constraints.

IV. IMPLEMENTATION AND EXPERIMENTAL EVALUATION

This section evaluates the practical feasibility of the proposed PQC-aware NB-IoT security architecture. Rather than focusing on micro-benchmark cryptographic performance, the evaluation emphasizes communication overhead, transmission frequency, and long-term lifecycle impact, which prior studies have identified as the dominant cost factors in LPWAN and cellular IoT systems [3, 8].

A. Implementation Setup

A prototype implementation of the proposed architecture was developed on a representative NB-IoT platform. The implementation includes control-plane onboarding using lattice-based post-quantum primitives and data-plane protection using lightweight symmetric authenticated encryption. Post-quantum cryptographic operations follow NIST-standardized parameter sets [13, 14]. Symmetric cryptographic mechanisms are selected based on their widespread adoption and suitability for constrained environments [3]. The selected platform represents a widely deployed class of commercial NB-IoT devices rather than a performance-optimized prototype, allowing the evaluation to reflect realistic deployment conditions.

B. Communication Overhead Analysis

A key objective of the evaluation is to quantify the relationship between message size and transmission frequency, which fundamentally determines communication cost in NB-IoT systems. Prior work has demonstrated that RF transmission energy dominates overall system consumption, making frequent transmission of large cryptographic messages impractical [3].

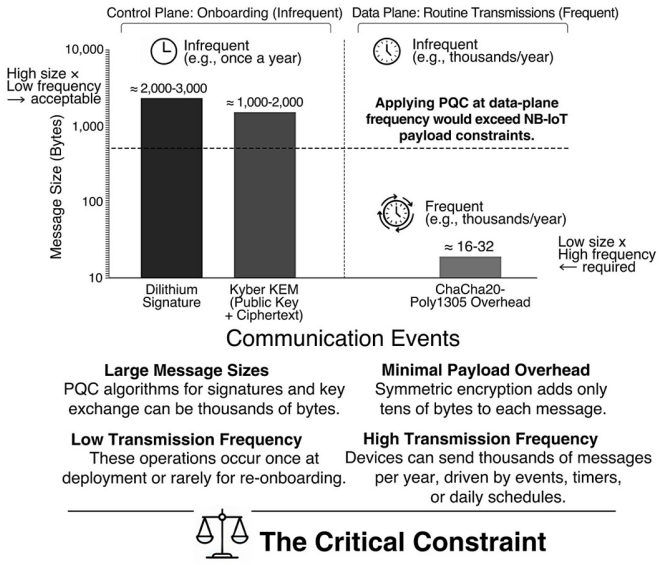

Fig. 2. Comparison of message size and transmission frequency between control-plane onboarding and data-plane communication in the proposed PQC-aware NB-IoT architecture. Large post-quantum cryptographic messages are confined to infrequent control-plane operations, while routine data transmission incurs minimal overhead.

Figure 2 illustrates a comparative analysis of communication overhead between control-plane onboarding and data-plane communication. Post-quantum cryptographic messages, including signatures and key encapsulation artifacts, exhibit sizes on the order of several kilobytes but are transmitted only during infrequent onboarding events. In contrast, data-plane messages incur minimal cryptographic overhead but are transmitted frequently throughout the device lifetime. This visualization highlights that the feasibility of post-quantum cryptography in NB-IoT systems depends not on absolute message size alone, but on the interaction between message size and transmission frequency.

C. Lifecycle Cost and Energy Impact

To assess long-term feasibility, the cumulative communication and energy cost of cryptographic operations is estimated over a typical ten-year NB-IoT device lifecycle. The analysis assumes conservative transmission patterns commonly observed in industrial and smart infrastructure deployments [3, 8]. As shown in Table II, post-quantum onboarding contributes a relatively high one-time cost but occurs only once or twice over the entire device lifetime. In contrast, data-plane communication dominates total transmission count but incurs negligible cryptographic overhead due to the use of lightweight symmetric mechanisms. These results demonstrate that confining post-quantum cryptography to infrequent control-plane operations yields a negligible contribution to total lifecycle cost. Energy impact is estimated using the transmission-dominant energy model commonly adopted in LPWAN analyses, where RF transmission cost dominates cryptographic computation cost [3].

D. Discussion of Experimental Findings

The evaluation confirms that the proposed PQC-aware architecture aligns with established observations regarding constrained wireless networks. Specifically, the results reinforce the conclusion that communication frequency, rather than cryptographic computation, is the primary determinant of scalability and energy efficiency in NB-IoT deployments [3, 8]. Furthermore, the findings are consistent with post-quantum migration guidance, which advocates minimizing disruptive changes and avoiding unnecessary cryptographic overhead in long-lived systems [1, 7, 12]. By amortizing post-quantum costs over extended lifecycles, the proposed architecture achieves a practical balance between quantum resistance and operational feasibility.

E. Summary of Evaluation Results

In summary, the implementation and evaluation demonstrate that post-quantum cryptographic mechanisms can be integrated into NB-IoT systems when applied selectively and with awareness of communication patterns. Figure 2 and Table II collectively show that the proposed architecture introduces minimal long-term overhead while preserving strong security properties. These results validate the architectural premise of the paper: post-quantum security in constrained IoT systems is feasible when guided by system-level design principles rather than uniform cryptographic substitution.

F. Code Availability and Reproducibility

Due to the use of commercial NB-IoT firmware and licensed cellular protocol stacks, the complete system implementation cannot be publicly released. However, the cryptographic protocol design, parameter settings, and experimental configuration details relevant to the proposed architecture can be provided by the author upon reasonable request to support independent reproduction at the architectural level.

V. DISCUSSION AND DEPLOYMENT CONSIDERATIONS

This section discusses practical considerations and broader implications of the proposed PQC-aware NB-IoT security architecture, focusing on realistic deployment environments and operational trade-offs.

A. Incremental Deployment and Backward Compatibility

One of the primary challenges in adopting post-quantum cryptography in cellular IoT systems is the need for incremental deployment. NB-IoT networks are typically operated by mobile network operators with heterogeneous device populations and long upgrade cycles. As emphasized in migration roadmaps and industry guidance, wholesale replacement of cryptographic mechanisms is neither feasible nor desirable [1, 11, 12]. The proposed architecture supports gradual deployment by confining PQC to the control plane. Devices and network components that support post-quantum onboarding can coexist with legacy devices that rely on classical mechanisms, reducing operational risk and enabling phased adoption aligned with operator policies.

TABLE II. ESTIMATED COMMUNICATION OVERHEAD AND ENERGY IMPACT OF CRYPTOGRAPHIC OPERATIONS OVER A 10-YEAR NB-IOT DEVICE LIFECYCLE.

Operation	Crypto-mechanism	Typical message size	Frequency (10 years)	Estimated energy impact	Remarks
Initial onboarding	Dilithium + Kyber	~3–5 KB	1	High (one-time)	Amortized over device lifetime
Re-onboarding /key rotation	Dilithium + Kyber	~3–5 KB	1	High (rare)	Optional, policy-driven
Routine data message	ChaCha20-Poly1305	+16–32 B	~87,600	Low	Compatible with NB-IoT payload limits
Key ratcheting	HKDF (local)	0 B	~87,600	Negligible	No communication overhead
Total PQC-related transmissions	**-**	**-**	**2 events**	**Negligible over 10 years**	**PQC confined to the control plane**

B. Trade-Offs in Post-Quantum Primitive Selection

The choice of post-quantum primitives reflects a balance between security, message size, and implementation maturity. Lattice-based schemes standardized by NIST provide a favorable trade-off for NB-IoT onboarding due to their relatively compact messages and efficient implementations [13, 14, 16]. Stateless hash-based signatures, while offering strong security assurances, incur significantly larger signature sizes and are therefore less suitable for constrained radio environments when used frequently [15]. This observation highlights the importance of context-aware algorithm selection. Future advances in PQC standardization or compression techniques may alter this trade-off and can be accommodated within the proposed architecture.

C. Key Management and Operational Policies

Key lifecycle management in NB-IoT deployments must account for long device lifetimes, limited connectivity, and operational constraints. The proposed architecture intentionally decouples long-term trust establishment from routine communication, enabling operators to schedule re-onboarding or key rotation on the order of years rather than months. Such policies align with recommendations for post-quantum migration in cellular networks, which advocate minimizing disruption while maintaining adequate security margins [3, 10-12].

D. Resilience and Failure Modes

Although the proposed design strengthens authentication and confidentiality, it does not eliminate all failure modes. Prolonged device compromise, loss of secure storage, or misconfiguration during onboarding can still undermine security. In addition, the architecture does not directly address DoS attacks, which are inherent to wireless environments and must be mitigated through network-level mechanisms. Importantly, by limiting the scope of PQC usage, the architecture reduces the risk that future vulnerabilities in specific post-quantum primitives would necessitate frequent, disruptive updates across the entire system.

E. Applicability Beyond NB-IoT

Although this work focuses on NB-IoT, the underlying design principles extend to other LPWAN and constrained-network technologies. The separation of control-plane and data-plane security, selective use of PQC, and lifecycle-aware key management apply to technologies such as LTE-M and emerging low-power cellular standards. However, the exact choice of cryptographic primitives and parameter sets may vary depending on network characteristics and regulatory requirements. Therefore, this architecture should be viewed as a design pattern, rather than a rigid protocol specification.

F. Limitations and Future Work

This work deliberately avoids proposing new cryptographic primitives or formal protocol verification. Although the security analysis demonstrates strong resistance to a broad class of threats, formal verification and large-scale field trials remain important directions for future research. Additionally, advances in PQC standardization, hardware acceleration, and protocol compression may enable broader use of post-quantum mechanisms in constrained environments. The proposed architecture is designed to accommodate such developments without fundamental redesign.

VI. CONCLUSION

This work demonstrates that the fundamental challenge of deploying post-quantum security in NB-IoT is not the availability of efficient cryptographic primitives, but the lack of system architectures that align cryptographic strength with communication patterns and device lifecycles. By framing post-quantum deployment as an architectural problem rather than an algorithmic one, the proposed PQC-aware design provides a practical and sustainable pathway toward quantum-resistant LPWAN systems. To address this challenge, this study proposed a PQC-aware secure communication architecture that explicitly separates control-plane onboarding from data-plane communication. By confining post-quantum cryptographic mechanisms to infrequent onboarding operations and relying on lightweight symmetric authenticated encryption for routine data transmission, the architecture achieves long-term quantum resistance without violating NB-IoT payload, reliability, or energy constraints.

The proposed design was implemented on a representative NB-IoT platform and evaluated experimentally. The results demonstrate that post-quantum onboarding can be realized reliably when amortized over long operational lifetimes, while routine data-plane communication remains efficient and robust. Security analysis under classical and quantum threat models confirms that the architecture provides strong authentication, confidentiality, forward secrecy, and damage containment, consistent with contemporary guidance on post-quantum migration. Rather than introducing new cryptographic primitives, this work emphasizes the importance of system-aware cryptographic integration. The architectural principles presented here offer a practical pathway for deploying quantum-resistant security in NB-IoT and other constrained networks, and complement ongoing standardization and migration efforts. As post-quantum cryptography continues to mature, such architecture-driven approaches will be essential to ensure that strong security remains deployable at scale.

DECLARATION OF COMPETING INTERESTS

The author declares that there are no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ACKNOWLEDGMENT

The author would like to thank Thai Nguyen University of Information and Communication Technology for the institutional support and infrastructure provided during this research.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request. Due to dependencies on commercial NB-IoT firmware and licensed cellular protocol stacks used in the experimental setup, certain implementation details are restricted to maintain compliance with licensing agreements.

REFERENCES

[1] U. Banerjee, A. Pathak, and A. P. Chandrakasan, "An Energy-Efficient Configurable Lattice Cryptography Processor for the Quantum-Secure Internet of Things," in *2019 IEEE International Solid- State Circuits Conference - (ISSCC)*, Feb. 2019, pp. 46–48, https://doi.org/10.1109/ISSCC.2019.8662528.

[2] S. Darzi, M. M. Rahman, I. Karim, R. Behnia, A. A. Yavuz, and E. Bertino, "Future-Proofing Authentication Against Insecure Bootstrapping for 5G Networks: Feasibility, Resiliency, and Accountability." arXiv, 2025, https://doi.org/10.48550/ARXIV.2510.23457.

[3] J. P. Mattsson, G. Selander, B. Smeets, and E. Thormarker, "Constrained radio networks, small ciphertexts, signatures, and non-interactive key exchange," in *Fourth PQC Standardization Conference (2022)*, 2022, vol. 10.

[4] L. Beckwith, D. T. Nguyen, and K. Gaj, "Hardware Accelerators for Digital Signature Algorithms Dilithium and FALCON," *IEEE Design & Test*, vol. 41, no. 5, pp. 27–35, Oct. 2024, https://doi.org/10.1109/MDAT.2023.3305156.

[5] D. Kim, J. Choi, S. Yoon, and S. C. Seo, "Optimized implementation of HQC on Cortex-M4," *ICT Express*, vol. 11, no. 5, pp. 939–944, Oct. 2025, https://doi.org/10.1016/j.icte.2025.07.001.

[6] E. D. Demir, B. Bilgin, and M. C. Onbasli, "Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms." arXiv, Mar. 31, 2025, https://doi.org/10.48550/arXiv.2503.12952.

[7] L. H. Mahdi and A. A. Abdullah, "Fortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21812–21821, Apr. 2025, https://doi.org/10.48084/etasr.10141.

[8] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, "Insecure connection bootstrapping in cellular networks: the root of all evil," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, Feb. 2019, https://doi.org/10.1145/3317549.3323402.

[9] "Stateless hash-based digital signature standard," National Institute of Standards and Technology, USA, NIST FIPS 205, Aug. 2024. https://doi.org/10.6028/NIST.FIPS.205.

[10] "Module-lattice-based digital signature standard," National Institute of Standards and Technology, USA, NIST FIPS 204, Aug. 2024. https://doi.org/10.6028/NIST.FIPS.204.

[11] A. Singla, R. Behnia, S. R. Hussain, A. Yavuz, and E. Bertino, "Look Before You Leap: Secure Connection Bootstrapping for 5G Networks to Defend Against Fake Base-Stations," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, Mar. 2021, pp. 501–515, https://doi.org/10.1145/3433210.3453082.

[12] "Module-lattice-based key-encapsulation mechanism standard," National Institute of Standards and Technology, USA, NIST FIPS 203, Aug. 2024. https://doi.org/10.6028/NIST.FIPS.203.

[13] "Announcing the Commercial National Security Algorithm Suite 2.0," National Security Agency (NSA), USA, PP-22-1338, Sept. 2022.

[14] "PQC Migration Roadmap," *Post Quantum Cryptography Coalition*. https://pqcc.org/post-quantum-cryptography-migration-roadmap/.

[15] A. J. Ross, B. Reaves, Y. Nasser, G. Cukierman, and R. P. Jover, "Fixing Insecure Cellular System Information Broadcasts For Good," in *Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses*, June 2024, pp. 693–708, https://doi.org/10.1145/3678890.3678924.

[16] "Technical Report on Quantum Secure 5G / beyond 5G Core using Post-Quantum Cryptography," Telecommunication Engineering Centre, India, TEC 910028:2025, 2025.

AUTHORS PROFILE

Do Thi Bac is a Senior Lecturer at Thai Nguyen University of Information and Communication Technology, Thai Nguyen, Vietnam. Her research areas include cryptography, communication and network security. She received her Ph.D. from Le Quy Don Technical University.