Redefining the Security of the Routing Protocol for Low-Power and Lossy Networks (RPL) with Post-Quantum Cryptography

Isaque Barbosa Martins, Matheus Pereira Lima, Anderson Paiva Cruz, Roger Immich, Ramon dos Reis Fontes
Metropole Digital Institute
Federal University of Rio Grande do Norte
Natal, Brazil
isaque.barbosa,matheus.pereira{@ufrn.edu.br},anderson,roger,ramon.fontes{@imd.ufrn.br}

***Abstract*—The widespread adoption of Internet of Things has raised critical concerns about the security of low-power networks, especially with the emergence of quantum computing. Routing Protocol for Low-Power and Lossy Networks (RPL), the standard routing protocol for such networks, lacks protection against quantum-enabled attacks. This paper proposes a hybrid cryptographic solution for RPL, combining AES-128 for symmetric encryption with CRYSTALS-Kyber768 for post-quantum key exchange. The implementation extends the RPL protocol while maintaining compliance with RFC 6550. Experimental validation in an IEEE 802.15.4 emulated environment shows that the proposed solution enhances security with minimal performance overhead. Results confirm the feasibility of deploying post-quantum cryptography in constrained devices, paving the way for secure and resilient IoT infrastructures.**

***Index Terms*—IoT, RPL, post-quantum**

I. Introduction

Currently, the Internet of Things (IoT) is transforming global connectivity by enabling direct communication between billions of smart devices. According to data from Statista, by the end of 2025, there will be approximately 20 billion IoT-connected devices worldwide, with projections indicating growth to around 40 billion by 2033 [1]. IoT encompasses communication between uniquely identified virtual objects that represent physical entities, such as sensors, which facilitate the collection of environmental and contextual data.

However, unlike traditional Internet-connected devices, a large portion of IoT devices have limited computational resources, which makes providing adequate security a significant challenge and demands special attention in the field of information security. From this perspective, previous studies have already identified vulnerabilities in various IoT systems and services, often stemming from the lack of appropriate security measures [2]–[4]. These vulnerabilities can be exploited by malicious actors, resulting in significant impacts on IoT systems.

With the advancement of quantum computing, IoT security faces a new and urgent threat. In the 1990s, Shor's quantum algorithm [5], [6] served as an early warning for information security, as it reduced the problem of factoring large prime numbers to polynomial complexity a problem that underpins RSA encryption, one of the most widely used algorithms in secure communication. Elliptic Curve Cryptography (ECC) is another widely used algorithm in information security, particularly within IoT. However, the U.S. National Security Agency (NSA) has also announced that both RSA and ECC are vulnerable to sufficiently large and stable quantum computers [7].

Therefore, the adoption of algorithms resistant to both quantum and classical attacks known as Post-Quantum Cryptography (PQC) has become increasingly important for securing IoT. Among them, CRYSTALS-Kyber [8] is one of three algorithms standardized by NIST [9]. Unlike RSA, it is based on hard lattice problems and was selected for its strong security and efficiency. Kyber also offers smaller key sizes and faster operations, which are crucial for constrained IoT devices.

In this article, we investigate how the CRYSTALS-Kyber post-quantum encryption scheme can efficiently protect resource-constrained IoT devices, enhancing communication security and reliability in low-power networks. The main contributions of this work are:

- Implementation and validation of AES-128 encryption mechanism to secure RPL control messages, ensuring confidentiality and efficiency in data traffic;
- Implementation and validation of RSA-1024 and CRYSTALS-Kyber-768 as asymmetric encryption solutions for the key exchange process in the RPL protocol. To the best of our knowledge, this represents the first documented integration of a NIST-standardized post-quantum cryptographic protocol with RPL to support secure key establishment;
- Execution of comprehensive testing to validate the cryptographic process, including a performance analysis of the integration of the algorithms in an emulated network environment;
- Sharing of all artifacts produced, including source code, test scenarios, and detailed documentation, to ensure the reproducibility of experiments and facilitate future research and validation efforts.

978-3-903176-75-1

The remainder of this paper is structured as follows. Section 2 provides the background concepts; Section 3 reviews related work in the field; Section 4 presents our proposal, while Section 5 evaluates our proposed solution; Finally, Section 6 concludes the paper and outlines future directions.

II. Background

The Routing Protocol for Low-Power and Lossy Networks (RPL) is a distance-vector protocol specifically designed for IoT scenarios, where devices are typically constrained in energy, memory, and processing power. Defined by RFC 6550, RPL builds routes in a Destination-Oriented Directed Acyclic Graph (DoDAG), which is rooted at a central node (usually the border router or sink). This structure allows efficient routing both upward (from leaf nodes to the root) and downward (from the root to leaf nodes), while adapting to frequent topology changes due to unreliable links or node mobility.

Figure 1 illustrates the formation of a DoDAG and the flow of RPL control messages DoDAG Information Solicitation (DIS), DoDAG Information Object (DIO), and Destination Advertisement Objects (DAO) in both RPL operating modes. The choice of operation mode (storing or non-storing) is crucial, as it defines how routing information is maintained and propagated within the network, directly affecting scalability, memory usage, and forwarding behavior. Nodes 1 and 2 are within radio range of the DoDAG root, while Node 3 is out of range and must connect via Nodes 1 or 2. When Node 3 sends a DIS message to Nodes 1 and 2, they reply with DIO messages. If Node 3 selects Node 1 as its preferred parent and decides to join the DoDAG, then:

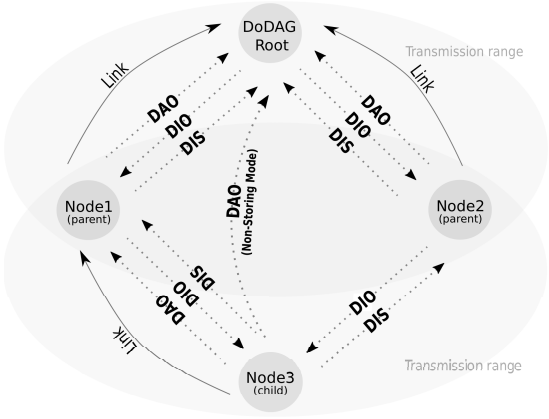


Fig. 1: Formation of a DoDAG.

- In the RPL non-storing mode of operation, it unicasts the DAO message directly to the root (as indicated by the dashed arrow), and other nodes ignore it.
- In the RPL storing mode of operation, the DAO is unicast to its selected parent (Node 1), which updates its routing table to include Node 3 as the next hop for that route.

To integrate the post-quantum cryptographic algorithm Crystals-Kyber into RPL within a DoDAG network, we extended the implementation of RPLD[1], adding support for symmetric encryption using AES-128 as specified by RFC 6550. Based on this foundation, we implemented key exchange using the Kyber Key Encapsulation Mechanism (KEM). This integration enables a robust cryptographic solution, aligned with modern network security requirements and resilient to emerging threats posed by advances in quantum computing.

[1]https://github.com/linux-wpan/rpld

III. Related Work

Security in IoT networks is a recurring concern and has been the subject of numerous discussions and studies over the years. These concerns have motivated the emergence of several proposals, including approaches focused on the application of post-quantum cryptography to ensure secure communications. For example, in [10], the authors proposed a method to enhance security in the Internet of Vehicles (IoV). Their solution uses post-quantum signatures based on a technique called systolic divisions, which optimizes division operations in cryptographic systems. The main goal is to employ digital signatures to ensure the authenticity and integrity of messages exchanged between IoV devices.

A post-quantum signature scheme based on the MQ (Multivariate Quadratic) cryptosystem was proposed in [11]. The MQ cryptosystem belongs to a family of public-key systems based on multivariate polynomials over finite fields and is suitable for protecting IoT devices against quantum computer attacks. The proposal was developed with a focus on efficiency and scalability, making it a viable solution for large-scale IoT networks.

In [12], the authors proposed, implemented, and evaluated an enhanced version of DTLS with post-quantum cryptography, capable of establishing secure communications even in the presence of quantum computers. They used a post-quantum NTRU-based solution (a public-key cryptographic system based on hard mathematical problems) to perform key exchange between entities. Ultimately, they demonstrated that it is feasible to integrate this enhanced DTLS version with post-quantum cryptography alongside the full IETF protocol stack in highly constrained environments.

Although several studies demonstrate growing concern with the security of IoT devices and their communications, few focus on the network layer, and in particular, the RPL protocol, which is specifically designed for routing in IoT environments. RPL is vulnerable to a variety of attacks, including selective forwarding, blackhole, sybil, wormhole, and sinkhole attacks [13]. These pose serious threats to the performance and reliability of IoT networks.

The widespread adoption and inherently accessible design of IoT devices introduce critical security challenges that demand the implementation of robust cryptographic tools to protect user privacy. To ensure the effective deployment of such tools, it is essential to develop a standardized and trustworthy infrastructure capable of providing security services, even in resource-constrained IoT environments. Until recently, Elliptic Curve Cryptography (ECC) has been the primary choice for secure cryptographic systems in websites, emails, online banking, and more. The adoption of ECC for security

was driven by several standardization bodies, including IEEE, ANSI, IETF, and NIST. Compared to RSA, ECC stands out as one of the most efficient cryptographic solutions against various real-world attacks.

However, as previously discussed, algorithms like RSA and ECC may become ineffective when exposed to attacks enabled by quantum computers [7]. Since then, significant efforts have been directed toward the development of Post-Quantum Cryptography (PQC). Quantum computers differ from classical machines in that they operate on atomic and subatomic systems rather than transistors, and they leverage properties of quantum mechanics. These properties include superposition, allowing the representation of multiple states simultaneously, and true parallelism, where computations can be executed in parallel without additional time or computational cost.

Although current quantum computers cannot yet operate with a sufficiently large and stable number of qubits for long durations, Google's most recent quantum processor has demonstrated results that if scaled could meet the operational requirements of fault-tolerant quantum algorithms [14]. This is a remarkable milestone that, combined with the known vulnerabilities of today's mainstream cryptographic algorithms, signals an imminent and very real threat to information systems connected to the Internet.

Therefore, this work aims to fill this gap by pioneering the application of a post-quantum cryptographic system in environments based on the RPL protocol. The implementation not only aims to strengthen communication security in IoT networks but also to encourage interest within the scientific and technological community in developing and enhancing quantum-resilient security solutions, particularly for constrained and critical communication scenarios.

However, most current IoT devices operate in low-power, high-loss networks, making traditional routing protocols unsuitable. Additionally, these devices face severe constraints in terms of memory, energy, and processing power, rendering them incapable of supporting such protocols. As a result, RPL has become the most widely adopted routing protocol for IoT networks, specifically optimized for devices with limited resources. Despite this, the current literature reveals limited focus on implementing post-quantum cryptography in resource-constrained IoT devices.

IV. Encryption of RPL Control Messages

The continuous evolution of quantum computing poses an imminent threat to the cryptographic foundations of existing Internet of Things (IoT) systems. As discussed in previous sections, routing protocols such as RPL, while optimized for constrained environments, remain susceptible to both classical and quantum-based attacks. To address these challenges, this section presents our proposed cryptographic enhancement for RPL, combining symmetric and asymmetric encryption mechanisms to protect control message exchanges in IoT networks.

Our approach builds upon two key cryptographic foundations: the use of AES-128 for symmetric encryption and the integration of CRYSTALS-Kyber768 for post-quantum secure key exchange. The goal is to create a hybrid and resilient security model that ensures both the confidentiality and authenticity of RPL control messages, without compromising the performance of low-power and lossy networks. The proposed implementation was designed to operate within the RPLD framework, leveraging its extensibility while adhering to the standards defined by RFC 6550.

In the following subsections, we detail the symmetric and asymmetric components of our proposal, explain the integration process within the RPL protocol, and discuss specific implementation choices aimed at preserving compatibility with resource-constrained devices. This design supports secure, future-proof routing in critical IoT scenarios, such as environmental monitoring, industrial automation, and smart infrastructure.

A. Symmetric Cryptography

According to RFC 6550, RPL message encryption must be performed using the AES-128 algorithm, which is widely adopted due to its efficiency and security in resource-constrained networks. This algorithm operates on 128-bit blocks, requiring that messages be properly padded to meet this requirement. This ensures the confidentiality of data exchanged between network nodes, protecting against attacks that could compromise the integrity and privacy of information. Additionally, implementing AES-128 within the RPL context enhances the security of critical operations in IoT networks, such as environmental monitoring and disaster detection.

The security-related fields in RPL are defined in compliance with RFC 6550. All RPL control messages are encapsulated within ICMPv6 packets, which include standard header fields such as Type, Code, and Checksum. These fields are present in every ICMPv6 control message but are not directly involved in the encryption process. Instead, Type and Code serve to identify the nature of the message, guiding the receiving node in how to interpret and process it correctly. Encrypted control message fields also adhere to RFC 6550 specifications. When AES-128 is applied, each message is padded as necessary to meet the required 128-bit block size (or its multiples), ensuring alignment with the symmetric encryption scheme in use.

To illustrate, consider a DIS message encapsulated within an ICMPv6 packet. The initial fields shared across all RPL messages are followed by encryption specific security parameters. Some of these are unique to the DIS message type, while the final segment of the packet contains padding bytes (typically zeros), ensuring the encrypted payload conforms to the RFC's structural and cryptographic requirements.

B. Asymmetric Cryptography

For asymmetric encryption, we used Crystals Kyber768, which encrypts the AES-128 symmetric key using a public key of 1184 bytes. This strategy is essential for strengthening security in IoT networks and other critical environments. It combines the robustness of post-quantum cryptography,

represented by Kyber, with the efficiency of AES-128 in securing control messages and key exchanges.

To implement Kyber, we used the algorithm's reference implementation, which provides public and private key generation, encapsulation of the shared secret derived from the public key, and decapsulation of the secret using the private key and the ciphertext produced during encapsulation. The implementation also allows the adjustment of the algorithm's security levels, which directly affect key sizes. These levels vary in both size and security, enabling flexibility depending on system requirements.

AES-128 is widely recognized for its efficiency and robustness in data encryption. However, the overall security of the system depends on how the symmetric keys are generated, distributed, and stored. Using Crystals Kyber to protect the symmetric key adds an extra layer of protection, making the system more resistant to attacks, especially against the rising threat of quantum computers, which could break traditional asymmetric cryptography like RSA and ECC.

The use of Kyber ensures resilience even in scenarios where the 800-byte public key is compromised. This is because the confidentiality of control messages remains protected by the robustness of AES-128, which continues to be a reliable and high-performance solution for symmetric encryption. This layered security model not only complicates direct attacks but also increases resistance to exploitation of vulnerabilities in resource-constrained IoT devices.

Furthermore, this approach aligns with modern security recommendations for critical networks, such as industrial systems and smart infrastructure, where the integrity and confidentiality of control messages are essential for safe and stable operation. The combination of Kyber and AES-128 offers a balance between long-term security and operational efficiency, making it ideal for energy and processing-limited devices. This hybrid approach ensures secure communications even in the face of future technological advancements such as quantum computing.

With this implementation, it was possible to carry out key exchange using event loops managed by the libev library, aiming to establish a TLS-like handshake. The process starts when a node wishing to join the network transmits its Kyber-generated public key. Upon receiving this packet, the root node uses Kyber to derive a shared secret from the public key and then generates a ciphertext. This ciphertext is sent back to the node that owns the public key, which then derives the same shared secret using its private key thus establishing a secure and authenticated communication channel between the parties.

V. Evaluation

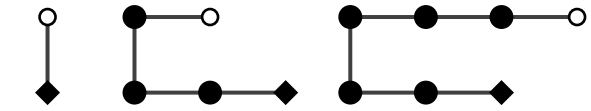
To evaluate the use of both symmetric and asymmetric cryptography in an IoT context, we extended the Mininet-WiFi [15] emulator to support IEEE 802.15.4 communications, particularly focusing on 6LoWPAN. We configured three topologies with different numbers of nodes, each running a modified version of RPLD[2].

[2]https://github.com/lowpan/rpld

To demonstrate the effectiveness of the proposed cryptographic integration, we verified the correct operation of the encryption process and evaluated its impact on network performance. For this purpose, we designed three distinct topologies: a direct connection between two nodes, a linear topology with three hops, and another with five hops. These configurations, illustrated in Figure 2, emerged naturally from RPL's topology formation process applied to small grid layouts containing 2, 5, and 7 nodes, respectively.

Each topology reflects an increasing path length between the source and root nodes, allowing us to assess the cryptographic and routing behavior across varying network depths. The white circle indicates the root node, black circles represent intermediate nodes (hops), and the black diamond marks the node used as a reference for the experiments.

To facilitate reproducibility and enable further experimentation, all configuration files and scripts used in the evaluation will be made publicly available upon the release of the final version of this paper.



(a) Direct (b) 3 hops (c) 5 hops

Fig. 2: RPL topologies with increasing hop counts.

A. Encryption/Decryption validation

To illustrate and validate the symmetric-key encryption, Listing 1 presents the fields of a fully encrypted DIO message, captured using the Wireshark tool. The field values appear obfuscated due to encryption, making them entirely different from the original sensor-generated data prior to applying the cryptographic mechanism.

It is worth noting that, for instance, the *flag* indicating the Mode of Operation (MOP) becomes unrecognizable to the RPL protocol after encryption. Nevertheless, since the participating sensors share the correct symmetric key, they are able to internally decrypt the entire message and accurately recover the original field values, ensuring secure and reliable communication.

Listing 1: Encrypted DIO fields

```
RPLInstanceID: 137
Version: 124
Rank: 3452
Flags: 0x7c, Zero, Mode of Operation (MOP): Unknown
Destination Advertisement Trigger Sequence Number: 245
Flags: 0x0d
Reserved: 23
DODAGID: 153c:be85:2b3f:8e80:fd3c:be8a:573f:8380:
```

B. Symmetric-key Impact

Table I presents the packet size variations resulting from the application of AES-128 encryption in RPL control messages across different topologies. In all scenarios, the DIO and DAO-ACK messages exhibit a uniform increase in size due to the

insertion of security-related header fields, as defined by RFC 6550. Specifically, the DIO message size increased from 100 to 121 bytes, while the DAO-ACK message grew from 80 to 108 bytes. The DAO message, however, experiences additional overhead that scales with the number of hops, as it includes padding bytes required to align the DODAGID transfers to the 128-bit block size used by AES. This behavior highlights the cumulative encryption cost in longer routing paths, which is especially relevant for evaluating the feasibility of secure communication in multi-hop IoT environments.

TABLE I: Packet sizes in the direct topology

DAO		
Network Topology	**No cryptography**	**AES**
Direct	100 bytes	127 bytes
3-hops DAO-ACK	160 bytes	182 bytes
5-hops DAO-ACK	200 bytes	220 bytes

C. Asymmetric-key Impact

Table II presents the sizes of ICMPv6 packets used during the key exchange process. The significant difference in packet size between RSA and Kyber has a direct impact on the time required to complete the key exchange between two nodes.

TABLE II: Key Exchange Packet Size

	RSA	**Kyber**
Symmetric-key	188 bytes	1148 bytes
Asymmetric-key	76 bytes	1244 bytes

Although the key exchange using Kyber takes nearly twice as long as RSA (0.3431 ms vs. 0.1889 ms), this increased delay represents a one-time cost incurred only during the initial key establishment phase. As such, its impact on overall system performance is minimal when compared to the continuous traffic exchanged during normal network operation. Still, in large-scale or time-sensitive IoT deployments, even small delays during node joins or high churn may affect routing convergence.

To mitigate this, Trickle Timer parameters in RPL can be tuned. Increasing redundancy suppression intervals or adapting transmission schedules can reduce control traffic during key exchange, easing congestion and accommodating the extra overhead of post-quantum algorithms like Kyber.

VI. Conclusion

In this work, we investigated and integrated the post-quantum cryptographic algorithm CRYSTALS-Kyber into the RPL protocol, focusing on enhancing the security of resource-constrained IoT networks. The proposed approach combines the use of CRYSTALS-Kyber for secure key exchange with AES-128 for symmetric encryption of control messages, providing a robust solution against emerging threats, including attacks from quantum computers. The results demonstrated that the combination of these algorithms successfully protected communications and indicated that although CRYSTALS-Kyber introduces a higher data overhead during the key exchange phase, the overall performance impact is mitigated by the use of AES-128 for symmetric encryption, resulting in greater efficiency for continuous traffic.

As future work, we intend to (i) incorporate additional authentication mechanisms, such as digital signatures or message authentication codes; (ii) compare different NIST-standardized post-quantum algorithms, such as CRYSTALS-Dilithium and SPHINCS+; (iii) study the impact of mobility and frequent topology changes on the cryptographic overhead and routing performance; and finally, we aim to (iv) integrate and evaluate our solution on real IoT hardware, such as ARM-based microcontrollers, to assess execution time, memory footprint, and energy consumption under realistic conditions, thereby validating the feasibility of post-quantum cryptography in operational environments.

Acknowledgment

This research was partially sponsored by CAPES grant Process #88887.005666/2024-00.

References

[1] statistica, "IoT connections worldwide 2022-2033 — Statista — statista.com." https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, 2024. [Accessed 29-12-2024].

[2] Z. Ling *et al.*, "Security vulnerabilities of internet of things: A case study of the smart plug system," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1899–1909, 2017.

[3] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2019.

[4] J. Deogirikar and A. Vidhate, "Security attacks in iot: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 32–37, IEEE, 2017.

[5] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.

[6] C. Bennett and P. Shor, "Quantum information theory," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2724–2742, 1998.

[7] U.S. National Security Agency, "Commercial national security algorithm suite and quantum computing faq." https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf, 2016. [Accessed 09-01-2025].

[8] J. Bos *et al.*, "Crystals-kyber: a cca-secure module-lattice-based kem," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 353–367, IEEE, 2018.

[9] G. M. D. Nist, "Module-lattice-based key-encapsulation mechanism standard," tech. rep., Gaithersburg, MD, 2024.

[10] H. Yi *et al.*, "Improving security of internet of vehicles based on post-quantum signatures with systolic divisions," *ACM Transactions on Internet Technology*, vol. 22, no. 4, pp. 1–15, 2022.

[11] S. Akleylek *et al.*, "Novel postquantum mq-based signature scheme for internet of things with parallel implementation," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6983–6994, 2020.

[12] J. Sepúlveda *et al.*, "Post-quantum enabled cyber physical systems," *IEEE Embedded Systems Letters*, vol. 11, no. 4, pp. 106–110, 2019.

[13] A. Jahangeer *et al.*, "A review on the security of iot networks: From network layer's perspective," *IEEE Access*, vol. 11, pp. 71073–71087, 2023.

[14] Google Quantum AI and Collaborators, "Quantum error correction below the surface code threshold," *Nature*, vol. Acelerated article preview, pp. 1476–4687, 2024.

[15] R. R. Fontes *et al.*, "Mininet-wifi: Emulating software-defined wireless networks," in *2015 11th International conference on network and service management (CNSM)*, pp. 384–389, IEEE, 2015.