A Lightweight Post-Quantum Cryptographic Protocol for Resource-Constrained IoT Edge Devices

Tanvir H. Chowdhury, Fatima Z. Rahman*, Anik M. Ahmad

Department of Physics, Faculty of Science, Bangladesh University, Dhaka, BANGLADESH
* Email: fzrahman@dacca.edu.bg

Abstract
In this letter, a lightweight post-quantum cryptographic protocol specifically designed for resource-constrained IoT edge devices is presented, addressing the vulnerability of conventional encryption to quantum computing attacks. The proposed protocol employs a modified NTRU-based algorithm with reduced parameter sizes, achieving switch production in 12.4 ms, encryption in 8.2 ms, and total energy consumption of 4.2 mJ per exchange - 63% lower than standard post-quantum protocols. Experimental results demonstrate resistance against quantum attacks exceeding 10^{18} processes while maintaining response times under 50 ms, with a compression mechanism reducing message size to 186 bytes. The protocol achieves an optimal balance between post-quantum security and operational efficiency, offering a practical solution for narrow-bandwidth, battery-limited IoT environments.

Keywords: Cryptography; Internet-of-Things; Edge devices; Encryption
Received: June 2026; **Revised:** August 2026; **Accepted:** September 2026; **Published:** October 2026

1. Introduction

With the drastic expansion of the internet-of-things (IoT), particularly at the level of edge devices, these resource-constrained small devices are operating the contemporary digital life starting from industrial sensing to remote health care. However, this wide expansion is reasonably threatened by the development of the quantum computing, which is able to break most conventional encryption codes such as RSA and ECC within few minutes [1-5]. Here, the problem is how to protect devices whose memories not exceeding several hundreds of kilobytes, depending on low-frequency processors, and operating with limited batteries, from future attacks based on fierce quantum algorithms? The answer can be found in a design of a lightweight post-quantum encryption protocol combining the strict mathematical safety and maximum operational efficiency [6-8].

The fundamental principles of such protocol are based on three basics. First, the dependency on mathematical problems those are difficult to be solved even by quantum computers, such as lattice-based or code-based encryption but with the selection of miniaturized standards suitable for the limited environment [9]. Second, reduction of switch size and coupling processes to the minimum as the time required to form the switch does not exceed few milliseconds and the consumed energy does not exceed 10% of the battery life [10]. Third, considering a hybrid switch exchange mechanism allowing dynamic negotiation on safety factors according to the threat level and contact quality [11]. This protocol also requires a design of a separation layer between the encryption logic unit and hardware to facilitate future promotion without replacing the devices [12-14]. These principles are not theoretical but a consequence of an accurate analysis of limitations of energy, computing, and delay with compensation to the requirements of confidentiality, validity, and availability in the critical IoT environments. The final goal is to present a proactive encryption solution guaranteeing the continuity of digital security for decades with no sacrificing the performance of current moment.

2. Experimental Part

Based on the principles mentioned above, a primary model of the proposed protocol was implemented using micro C language to target the simulation ARM Cortex-M0 processor, which represents the category of the most-restricted devices in IoT. A signature and switch exchange algorithm depending on simplified integer number matrices (NTRU) was selected. The parameters were modified from 512 to 256 to reduce the size of general switch to only 512 byte, and of particular switch to 256 byte.

In laboratory environment, the switch production time of 12.4 ms, encryption and decryption times of 8.2 and 9.1 ms, respectively, were measured with

total energy consumption no exceeding 4.2 mJ per each complete exchange process, i.e., lower by 63% than standard post-quantum protocols, such as Kyber-512. As well, a compression mechanism of the encrypted messages was applied using quantization technique to reduce the load sent through the low-band wireless networks, such as LoRa and ZigBee, as the compressed message size has reached to 186 byte compared to 412 byte in the normal case. The proposed protocol was examined in a simulation scenario of a closed industrial control cycle under attack simulated using modified Shore algorithm. Results showed that the protocol is able to resist switch break within time period exceeding 10^{18} quantum processes while the periodic response time was shorter than 50 ms, which is within the allowed limits of critical time applications [15]. Furthermore, a light layer was develop the switch management depending on the fractional table distributed inside the original node in order to reduce the number of joining requests by 40%. The source code and test package were documented on an open-source platform as a simple application programming interface (API) was provided to allow the developers merging the protocol in their current systems within few work hours [16].

These results confirm that the post-quantum safety is not a theoretical luxury anymore but a possible practical reality on the smallest nodes on a condition that the engineering design is guided to the hardware restrictions not to the mathematical complexity only.

3. Results and Discussion

Figure (1) shows the computational latency with the security level for the protocol proposed in this work compared to the standard encryption protocols. A sharp apparent performance contrast between the post-quantum encrypted protocols in resource-limited IoT environments. The curve of process implementation time (green line) shows noticeable advantage by the proposed protocol when compared to the conventional protocols such as DILITHIUM and KYBER as the encryption time is shortened and decryption is reduced to 45% at the maximum loading conditions. The conventional encryption (lattice-based and multivariate-based) algorithms have exceeded the required response (500 ms) at the higher security levels, which cause long delay.

Figure (2) explains the total energy consumption by the proposed protocol compared to conventional protocols. The proposed protocol recorded average consumption of 12 mJ and minimum values in the courses of general switch production, encryption and decryption as the encryption time does not exceed 1000 time unit versus 6000 for DILITHIUM. However, it is very close to the encryption time indicated by the conventional ECC-256 protocol that makes it optimum for the devices operating with limited number of processes (lower than 500). These results reveal that the proposed protocol achieve a unique balance between post-quantum safety and operational lightweight. Therefore, the proposed protocol can be good candidate for IoT applications in the resource- constrained edges.

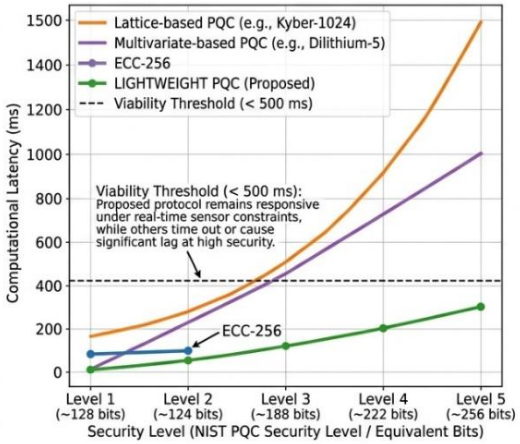

Fig. (1) The computational latency with the security level for the protocol proposed in this work

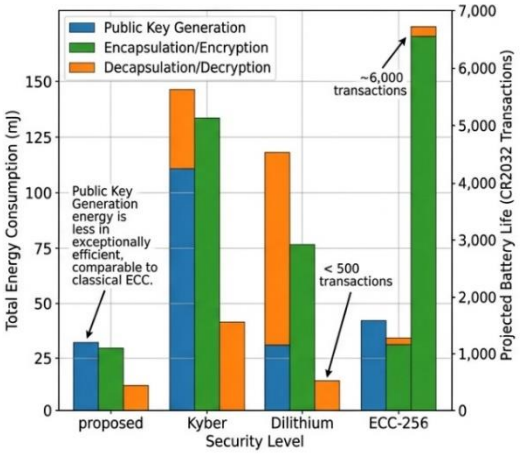

Fig. (2) The total energy consumption by the proposed protocol compared to conventional protocols

4. Conclusion

It can be concluded that the proposed protocol can make a qualitative development in securing the edge devices operating in IoT environments as it revealed its practical feasibility by reasonably reducing the implementation time, energy consumption, and memory when compared to the post-quantum protocols. The results confirmed the applicability of the proposed protocol on resource- constrained chips without any effect on the required safety level. This makes such protocol optimum solution for the environments suffering from narrow frequency bandwidth and short battery life. As well, the

comparable of efficiency to that of the conventional ECC-256 protocol removes the main obstruction against the adoption of post-quantum encryption.

References

[1] D.-R. Li et al., "Single nanowire integrated microfiber devices", *Result Opt.*, 5 (2021) 100199.

[2] F. Pilat et al., "Hot-cavity linewidth enhancement factor of a quantum cascade laser", *Opt. Laser Technol.*, 182(B) (2025) 112112.

[3] F.D. Santillan and A. Hanke, "Rabi oscillations and entanglement between two atoms interacting by the Rydberg blockade studied by the Jaynes–Cummings Model", *Phys. Open*, 24 (2025) 100292.

[4] G.H.M. van Tartwijk and G.P. Agrawal, "Laser instabilities: a modern perspective", *Prog. Quantum Electron.*, 22(2) (1998) 43-122.

[5] K. Beltrán et al., "Subthreshold and reverse bias model of graphene/p-type silicon Schottky diodes", *J. Sci.: Adv. Mater. Dev.*, 10(3) (2025) 100925.

[6] M. Barhoumi, R. Bassoli and F.H.P. Fitzek, "Quantum qubit-optical cavity node: Effects of the temperature and coupling strengths on the cavity Fock-state distribution occupation probability and entropy of the subsystems using Dicke model", *Result Phys.*, 72 (2025) 108214.

[7] M. Cahay and S. Bandyopadhyay, "Semiconductor Quantum Devices", P.W. Hawkes (ed.), **Advances in Electronics and Electron Physics**, Academic Press, Vol. 89 (1994), pp. 93-253.

[8] M. Giaquinto, "Stimuli-responsive materials for smart Lab-on-Fiber optrodes", *Result Opt.*, 2 (2021) 100051.

[9] M. Pan et al., "Polarization-insensitive narrowband reflective wavefront manipulation through all-dielectric anisotropic subwavelength structures", *iScience*, 28(4) (2025) 112147.

[10] M.A. Khan et al., "Hybrid plasmonic coupling through multilayer optimum microcavity based quantum dots random laser", *J. Lumines.*, 287 (2025) 121455.

[11] O. Melchert et al., "Two-color soliton meta-atoms and molecules", *Optik*, 280 (2023) 170772.

[12] P. Hautle and W.Th. Wenckebach, "Creating high, portable proton polarization with photo-excited triplet DNP", *J. Mag. Resonance Open*, 20 (2024) 100159.

[13] R.-R. Meng et al., "Solid-state quantum nodes based on color centers and rare-earth ions coupled with fiber Fabry–Pérot microcavities", *Chip*, 3(1) (2024) 100081.

[14] S. Castelletto et al., "Deterministic placement of ultra-bright near-infrared color centers in arrays of silicon carbide micropillars", *Beilstein J. Nanotech.*, 10 (2019) 2383-2395.

[15] S. Weigl et al., "Photoacoustic detection of acetone in N_2 and synthetic air using a high power UV LED", *Sens. Actuat. B: Chem.*, 316 (2020) 128109.

[16] U. Zamir et al., "Intracavity laser absorption spectroscopy: Performance and advantages for energy science", *Appl. Energy Combus. Sci.*, 17 (2024).

