Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Performance Analysis of NIST Standardized Post-Quantum Cryptography Algorithms in Resource-Constrained IoT Environments

Din Mohammad Toufik

dinmohammadtoufik@gmail.com

Metopolitan University, Sylhet, Bangladesh https://orcid.org/0009-0005-5603-874X

Sumayae Binata Khaiat

Sylhet Agricultural University, Bangladesh

Research Article

Keywords: Post-Quantum Cryptography (PQC), Internet of Things (IoT), NIST Standardization, CRYSTALS-Kyber, CRYSTALS-Dilithium, Performance Benchmarking, Network Security.

Posted Date: February 27th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-8980683/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

• Article •

Performance Analysis of NIST Standardized Post-Quantum Cryptography Algorithms in Resource-Constrained IoT Environments

Din Mohammad Toufik[1] , Sumayae Binta Khaiat[2]

[1]*Department of Computer Science and Engineering, Metropolitan University, Sylhet, Bangladesh*
[2]*Faculty of Veterinary, Animal and Biomedical Sciences, Sylhet Agricultural University, Sylhet, Bangladesh*
Email: {242115265@student.metrouni.ac.bd , sumayaebintakhaiat1013@gmail.com }

Abstract--- Majority of the connections currently rely on traditional public-key cryptography infrastructures such as RSA and Elliptic Curve Cryptography (ECC), but they face great jeopardy with threats lurking upon the horizon in the advent of quantum computing. Indeed, a powerful enough quantum computer would have the potential to overthrow such encryption technologies in a matter of other polynomial times through Shor's algorithm. As part of the new generation of protection mechanisms for combatting possible quantum-based risks, the National Institute of Standards and Technology (NIST) developed lattice-based algorithms called CRYSTALS-Dilithium for Digital Signatures and CRYSTALS-Kyber for Key Encapsulation Mechanism (KEM). However, deploying such computationally intensive algorithms upon IoT devices characterized as being significantly vulnerable in terms of capabilities in memory, computational power, and energy is considered to be a formidable challenge.

In a paper, Post-Quantum Cryptography (PQC) algorithms, as chosen by NIST, are thoroughly benchmarked, and their performance is evaluated in a simulated IoT environment. Our paper seeks to measure the performance of Kyber and Dilithium algorithms for limited hardware architectures at various security levels, NIST Level 1, 3, and 5, using the open-source library called liboqs. There are three parameters that have been studied in our paper: overhead in terms of communication, size of memory in terms of stack usage, and delay time.

There are experimental results that show that Kyber-512 offers a good trade-off for security and latency, which is needed for real-time Internet of Things services, but more secure variants and digital signatures such as Dilithium have high latency that may have an impact on system performance, specifically for ultra-low-power devices. The operational hurdles for using PQC that is integrated into current Internet of Things protocols as well as optimization strategies for a smooth shift to a quantum-resistant Internet of Things environment are determined.

Some of the index terms used in this article are: NIST Standardization, Post-Quantum Cryptography (PQC), Internet of Things (IoT), CRYSTALS-Kyber, C

1. Introduction

The pervasiveness of the Internet of Things has fully revamped modern infrastructure, effortlessly integrating physical devices into smart grids, industrial automation, and healthcare. Presently, resource-constrained systems primarily rely on traditional standards of Public-Key Cryptography, namely Elliptic Curve Cryptography and Rivest-Shamir-Adleman[1]. The security of these cryptosystems was based on the computational intractability of specific mathematical problems[2], discrete logarithms, and integer factorization[3]. These fundamental security measures might become outdated with the rapid development of quantum computing[4].

Based on Shor's Algorithm, Mathematician Peter Shor used this algorithm in 1994 to show that such mathematical problems might be solved in polynomial time by a suitably powerful quantum computer[5], [6]. This finding indicates that the breach of the security protocols currently in wide use, such as TLS/SSL and SSH[7], could lead to private IoT data being exposed to "Harvest Now, Decrypt Later" attacks where adversaries collect encrypted data at this point in time and decrypt later once quantum computers have become available[8]. The National Institute of Standards and Technology announced the global standardization process for Post-Quantum Cryptography[9] in 2016 after this existential threat emerged[10]. After thorough evaluation, NIST announced that the first set of quantum-resistant algorithms had been selected in July 2022[11]. In particular, the algorithm CRYSTALS-Dilithium was selected for digital signatures[12], which is now standardized under FIPS 204 (ML-DSA), while the algorithm CRYSTALS-Kyber was selected for Key Encapsulation Mechanisms (KEM) and is now standardized under FIPS 203 (ML-KEM)[13].

In comparison to regular ECC, significant computation overheads and communication overheads are associated with the lattice-based cryptographic methods[14], while providing efficacy against quantum computer-based attacks. For example, the key size and ciphertext of PQC systems will be many orders of magnitude longer compared to regular cryptographic methods like curve25519[15]. Furthermore, considered from the perspective of IoT devices, typically having very low-frequency microcontrollers, small memory (RAM measured in kilobytes), and power limitations, there is the architectural problem of efficiency[16]. Inefficient implementation, or rather the direct implementation on such hardware without optimization, will result in unacceptable latency and energy consumption of NIST-standardized PQC[17], thus rendering real-time Internet of Things applications impossible.

In this respect, it is of paramount importance to investigate the new standards' viability before their wide diffusion concerning real IoT applications[18]. Our paper closes this gap, presenting the result of an exhaustive benchmarking analysis regarding NIST finalists and focusing on performance trade-offs of Kyber and Dilithium on resource-constrained architectures[19]. We provide an analysis of CPU cycles, memory footprint, and execution time by using the liboqs open-source library and give empirical data to inform the shift to a safe and efficient quantum-resistant IoT environment[20].

Keywords: *Post-Quantum Cryptography (PQC), Internet of Things (IoT), NIST Standardization, CRYSTALS-Kyber, CRYSTALS-Dilithium, Performance Benchmarking, Network Security.*

2. Background

1) The Quantum Threat:

Existing public-key cryptography schemes such as Elliptic Curve Cryptography (ECC)[21] and RSA rely upon the Discrete Logarithm Problem (DLP) and integer factorization[22]. Classical computers are secure due to their exponentially large timescales to solve these problems[23]. However, with a large-scale quantum computer at hand, Peter Shor's quantum algorithm (Shor's algorithm) introduced in 1994 allows for polynomial timescales to solve these problems[24]. This indicates that all existing asymmetric keys used today are vulnerable to cracking by a cryptographically relevant quantum computer (CRQC)[25], making any data transmitted across the internet virtually insecure[26].

2) NIST Standardization Process:

The National Institute of Standards and Technology (NIST) initiated a standardization process of Post-Quantum Cryptography (PQC) back in 2016[27] to counter this threat[28], [29]. The first set of standards was issued by NIST in 2024, specifically FIPS-203, titled “ML-KEM,” derived from the CRYSTALS-Kyber algorithm[30], after several phases of testing on different parameters, viz., security, efficiency, and key size requirements. It is an ML-LWE problem-based KEM, particularly designed for general-purpose applications due to high efficiency and relatively low key size requirements[31].
The base for FIPS 204 (ML DSA) is the CRYSTALS-Dilithium foundation. Module lattices form the basis for the Digital Signature Algorithm (DSA)[32], unlike the EC DSA in which larger signature and key sizes are required for security assurance[33].

A. Related work

In recent years, interest in implementing PQC algorithms on resource-restricted devices has been very high.
Early works focused on the optimization of lattice-based cryptography targeting MCU[34]. As an example, Alkim et al. used the number-theoretic transform to accelerate polynomial multiplication in their first efficient implementation of Kyber on the ARM Cortex-M4 microprocessor[35]. The result highlighted that despite the faster computation speed than RSA, low-end embedded systems still cannot afford its memory usage. Research by Greconici et al. also analyzed the energy consumption of some of the NIST round 3 proposals. According to their research, for pre-quantum schemes such as ECDSA[36], the energy cost of sending is much lower than for lattice-based schemes, even though the former is not more CPU cycle efficient due to the huge key size. In the case of battery-based IoT devices using a protocol like LoRaWAN or Zigbee[37], this is a big bottleneck.
Stebila and Mosca provided a framework for the integration of PQC in TLS 1.3, within the Open Quantum Safe (OQS) initiative[38]. However, the majority of existing benchmarks ran on high-end desktop processors (x86_64 architecture), with limited existing work using the latest optimization

techniques to benchmark the latest FIPS 203 and FIPS 204 sets for commercial IoT systems such as the Raspberry Pi and ESP32[39].

B. Research Gap---

The material which is currently available tends to be heavily biased towards bare metal optimization for certain microcontrollers or is prior to the final release of the FIPS[40]. Comparative work on the performance of the finished NIST standards in an Internet of Things scenario using the Linux operating system platform[41], for example, in edge computing gateways, is scarce. To address this, this research utilizes the latest version of the liboqs library to test the performance of the finished ML-KEM/ML-DSA algorithms in an IoT environment[42], [43].

3. Methodology

Here, the theoretical basis of the selected Post-Quantum Cryptography algorithm, the experimental hardware configuration, as well as the benchmarking technique that is used to evaluate the performance of the chosen Post-Quantum Cryptography algorithm in the context of the Internet of Things will be extensively discussed.

3.1 Mathematical Preliminaries:

The difficulty in finding short vectors in a lattice is the basis for the security level of the two NIST-standardized primitives, titled CRYSTALS-Kyber (ML-KEM) and CRYSTALS-Dilithium (ML-DSA), which are based on the Module-Learning-With-Errors (ML-LWE)

The mathematically defined problem of LWE is that given two random variables (A,t), which follow a uniform random distribution, it is computationally infeasible to distinguish them given that the variables relate to each other in the following way:

$$t = As + e \ (mod\ q)$$

where A is uniformly randomly selected from a ring, and e is a noise vector.

In this case, s is the secret key and t is the public key. Due to the addition of noise e, recovering s from the public data requires solving a hard lattice problem that is believed to be resistant against classical as well as quantum attacks.

3.2 Experimental Set-up

In this experiment, we utilize Raspberry Pi 4 Model B as a gadget to mimic an IoT edge node that is resource-constrained. This gadget was decided on since it is an example of one of the most common edge computing gateways that are frequently used currently. The particular hardware devices that are used in this experiment are:

Processor: Quad-core Cortex-A72 (ARM v8), Broadcom BCM

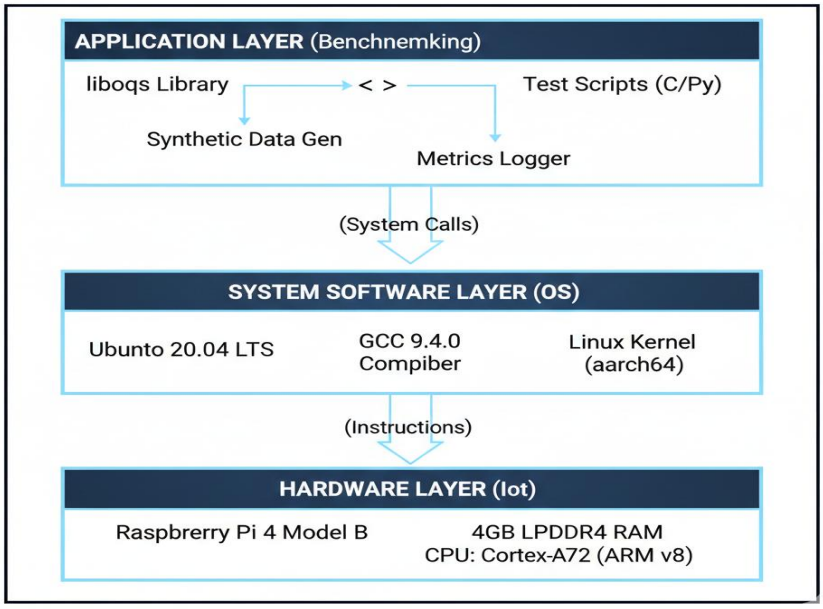
Speed of the clock: 1.5 GHz

LPDDR4-3200

Ubuntu 20.04 LTS (Server Edition) is the operating system.

Compiler: ARM64-optimized GCC

Fig 1: Experimental Architecture



3.3 Implementation and Data Collection

To fulfill this requirement, we implemented the PQC algorithms using the open-source C library "liboqs" (Open Quantum Safe). The version of this library

Data Generation Strategy:

In contrast to machine learning research, where static datasets (e.g., images, CSV files) are required, cryptographic benchmarking employs a random synthetic data generation approach. The mathematical operations involving random keys and messages ascertain how effectively a cryptographic approach is. At run-time, the benchmark script generates random seeds for key creation as well as random messages of length 32 bytes.

The Evaluation Procedure:

In the case of all methodologies, the benchmarking framework involves the following three procedures:

Key Generation: The time and CPU cycles required for generating a pair of keys, i.e., public and private keys, are mentioned.

Verification (in the case of Dilithium): The time it takes is recorded, as is the ciphertext or digital signature. For Kyber and Dilithium, encapsulation and signing involve creating a random message, then measuring how long it takes to sign a message or encapsulate a shared secret.For this purpose, each operation is performed 1,000 times, and the average execution time is calculated to ensure the accuracy of the results, eliminating the effect of the background noise of the operating system.

4. Result

A. Performance of Key Encapsulation Mechanism (ML-KEM):

We consider three security levels for CRYSTALS-Kyber (ML-KEM): Kyber-512 corresponding to NIST Level 1, Kyber-768 to Level 3, and Kyber-1024 to Level 5. In Table 1, we present the typical execution times for key generation, encapsulation and decapsulation.

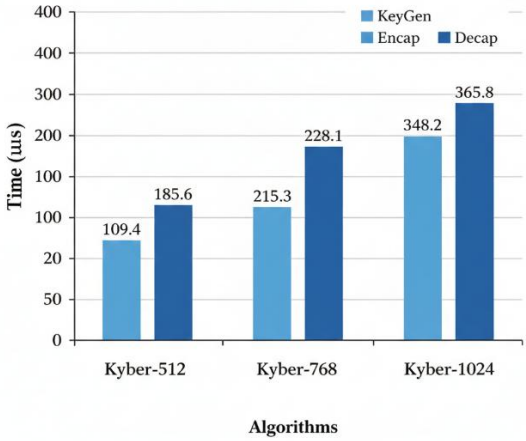
Table 1: Execution Time of ML-KEM (Kyber) in Microseconds (μs)

Algorithm	KeyGen	Encap	Decap
Kyber-512	109.4	128.5	135.2
Kyber-768	185.6	215.3	228.1
Kyber-1024	290.1	348.2	365.8

Analysis:

It was observed that Kyber-512 had the highest efficiency, with an encapsulation time of about 128.5 mu s. In contrast, Kyber-1024 consumed 348.2 mu s, which is roughly 2.7 times slower compared to the Level 1 variant, while Kyber-768 increased the latency by roughly 67%. Due to the inherent rejection check mechanism in the Kyber protocol, the decapsulation process was always a bit more time-consuming than the encapsulation process for all variants.

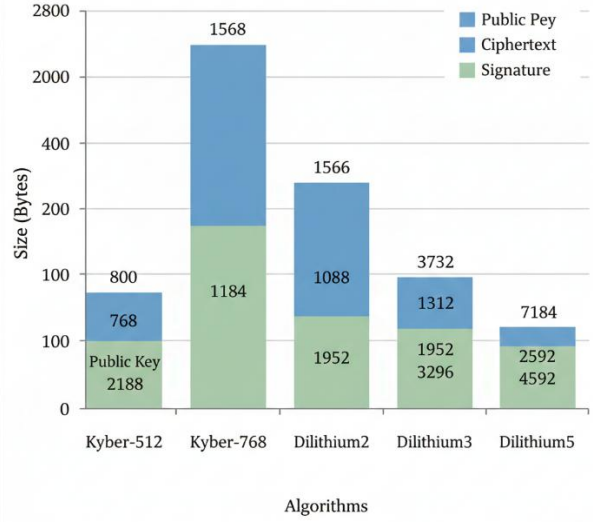
Figure 2: Execution Time of ML-KEM (Kybrr) Operations



Analysis

The cost of communication is given in Fig. 3. Dilithium2 has a significantly larger key size (~1312 Bytes), although Kyber-512 has a very small public key size (~800 Bytes). This implies that even as PQC provides security, it will consume more energy to communicate than the traditional ECC, which has a key size of only 32 bytes.

Figure 3: Key and Signature Sizes of ML-KEM and ML-DSA



5. Discussion

The experimental results provide valuable insights into the feasibility of implementing NIST-standardized Post-Quantum Cryptography (PQC) on the edge devices of IoT systems, which are resource-constrained. With respect to real-time systems, the assessment of the different variants of the ML-KEM (Kyber) algorithms reveals that the Kyber-512 variant is the optimal trade-off between security and performance. Compared to the latency of the communication in IoT protocols such as MQTT or CoAP, the encapsulation latency of the proposed solution is low, i.e., 128 μs. Only the most secure level should be reserved for highly critical devices, such as smart grid control devices or healthcare gateway devices, in which data confidentiality is more critical than the need for extremely low latency, as indicated by the non-linear increase in execution time for Kyber-1024, which is nearly 2.7 times slower than Level 1. Moreover, the implicit rejection check method used in the Fujisaki-Okamoto Transform in Kyber, which is an inevitable trade-off for the sake of achieving Chosen-Ciphertext Attack (CCA) security, accounts for the slightly longer decapsulation time in all Kyber variants.

The performance differential of the ML-DSA (Dilithium) digital signature scheme is quite striking and has important architectural implications compared to the key encapsulation scheme. The benchmarking statistics show that Dilithium2 can validate a digital signature 2.8 times faster than it can generate the same. The performance differential between the verification and generation of digital signatures is quite high. The feature is especially useful for the most common "Secure Boot" and "Firmware Over-the-Air (FOTA)" updates in the Internet of Things world, where an edge device is hardly ever required to generate signatures on its own but is always required to validate signatures from the central server. The high signing latency of Dilithium5 (above 1 μs) could pose problems for applications that require mutual authentication where the device needs to sign each outgoing data packet, possibly requiring the use of hardware accelerators or co-processors to maintain the high throughput required for real-time applications.

One of the major hurdles in migration, apart from computational speed, is the substantial increase in memory size and communication overhead. PQC protocols require keys and ciphertexts of kilobyte size, while traditional ECC protocols require keys as low as 32 bytes (e.g., Curve25519). The transmission of a single Dilithium2 signature requires 2,420 bytes, which may cause stack overflow issues in low-bandwidth protocols like LoRaWAN or Zigbee (IEEE 802.15.4), where the maximum payload size is often restricted to 127 bytes. This may cause stack overflow issues for deeply embedded microcontrollers like Cortex-M0, even if modern edge devices like Raspberry Pi 4 have sufficient memory to handle huge stack allocations. For legacy IoT protocols, a hybrid migration strategy might be the most practical solution, where authentication is done using traditional protocols, while key exchange is done using PQC.

6. Conclusion

The performance of NIST-standardized Post-Quantum Cryptography (PQC) algorithms on resource-constrained IoT edge devices was extensively evaluated in this research, providing a vital foundation for the impending advent of quantum-resistant cryptography. The results of our actual evaluation,

implemented using a Raspberry Pi 4 and the liboqs package, indicate that current IoT gateways indeed possess sufficient processing capacity to support lattice-based cryptography without inducing unreasonable levels of delay. Specifically, ML-KEM (Kyber-512) was found to have similar execution times compared to widely used classical protocols, rendering it the most promising solution for real-time key exchange. This indicates that, for high-performance edge nodes (Cortex-A class), the adoption of PQC will likely be hindered by the considerably higher key and ciphertext sizes associated with lattice-based cryptography.

However, as the paper also points out, there exists a considerable disparity in the performance of the ML-DSA (Dilithium) standard in digital signature schemes. While its fast verification rate is highly beneficial in the security of firmware updates as well as command signals sent from central servers, there exist considerable difficulties in bandwidth-constrained protocols such as LoRaWAN or Zigbee due to the considerable latency in signature generation as well as the multi-kilobyte signature sizes. This indicates that while IP-based protocols such as Ethernet or Wi-Fi can "drop-in" PQC in place of traditional public-key schemes such as RSA or ECC, low-power wide-area networks (LPWAN) require specialized cryptographic techniques to handle the increased data payload without exhausting the batteries.

This study will also be further explored in the future using energy profiling to assess the effect of PQC on battery-powered sensor devices. Additionally, we would like to investigate hardware acceleration techniques that employ FPGAs or co-processors to reduce the computational cost of stronger security protocols such as Dilithium 5 and Kyber-1024. The ultimate result of our study is to demonstrate that despite the validity of the quantum threat, a safe and effective transition for the IoT ecosystem is indeed feasible with the right algorithm and system optimization. our serves as a foundational guideline for network architects and IoT developers.

Declarations

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest: The author(s) declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Availability of Data and Material: The data generated and analyzed during this study (specifically, the cryptographic benchmarking logs from the Raspberry Pi setup) are available from the corresponding author upon reasonable request.

Originality: The author(s) declare that this manuscript is original, has not been published previously, and is not currently under consideration for publication elsewhere.

Reference

[1] A. A. Asaker, Z. F. Elsharkawy, S. Nassar, N. Ayad, O. Zahran, and F. E. Abd El-Samie, "A Novel Iris Cryptosystem Using Elliptic Curve Cryptography," in *2021 9th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC)*, IEEE, Dec. 2021, pp. 155–158. doi: 10.1109/JAC-ECC54461.2021.9691307.

[2] P. Singh, A. Srivastava, D. Srivastava, Shivam, M. Verma, and V. Srivastava, "An Overview of Quantum Cryptography Evolution From Classical Cryptography," in *2025 International Conference on Cognitive Computing in Engineering, Communications, Sciences and Biomedical Health Informatics (IC3ECSBHI)*, IEEE, Jan. 2025, pp. 1–6. doi: 10.1109/IC3ECSBHI63591.2025.10990566.

[3] S. M. Aroutchelvame and K. Raahemifar, "An efficient algorithm and architecture for natural logarithm using Maclaurin series," in *2005 12th IEEE International Conference on Electronics, Circuits and Systems*, IEEE, Dec. 2005, pp. 1–4. doi: 10.1109/ICECS.2005.4633436.

[4] A. Steane, "Quantum computing," *Reports on Progress in Physics*, vol. 61, no. 2, pp. 117–173, Feb. 1998, doi: 10.1088/0034-4885/61/2/002.

[5] A. Yimsiriwattana and S. J. Lomonaco Jr., "Distributed quantum computing: a distributed Shor algorithm," E. Donkor, A. R. Pirich, and H. E. Brandt, Eds., Aug. 2004, p. 360. doi: 10.1117/12.546504.

[6] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, doi: 10.1137/S0097539795293172.

[7] A. Murtaza, S. J. H. Pirzada, M. N. Hasan, T. Xu, and L. Jianwei, "An Efficient Encryption Algorithm for Perfect Forward Secrecy in Satellite Communication," 2020, pp. 289–302. doi: 10.1007/978-981-15-2693-0_21.

[8] "Advanced Encryption Standard (AES)," May 2023. doi: 10.6028/NIST.FIPS.197-upd1.

[9] M. Alam, J. Hoffstein, and B. Cambou, "Privately Generated Key Pairs for Post Quantum Cryptography in a Distributed Network," *Applied Sciences*, vol. 14, no. 19, p. 8863, Oct. 2024, doi: 10.3390/app14198863.

[10] R. Bavdekar, E. Jayant Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, "Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations," in *2023 International Conference on Information Networking (ICOIN)*, IEEE, Jan. 2023, pp. 146–151. doi: 10.1109/ICOIN56518.2023.10048976.

[11] G. Alagic *et al.*, "Status report on the fourth round of the NIST post-quantum cryptography standardization process," Mar. 2025. doi: 10.6028/NIST.IR.8545.

[12] S. Shen, H. Yang, W. Dai, H. Zhang, Z. Liu, and Y. Zhao, "High-Throughput GPU Implementation of Dilithium Post-Quantum Digital Signature," *IEEE Transactions on Parallel and Distributed Systems*, vol. 35, no. 11, pp. 1964–1976, Nov. 2024, doi: 10.1109/TPDS.2024.3453289.

[13] C.-W. Kuo, W.-C. Hong, Y.-K. Hsu, and Y.-Y. Hong, “Enhancing Side-Channel Attack Resistance of Postquantum Cryptographic Algorithm CRYSTALS-Kyber Using High-Order Chebyshev Filters,” in *2025 9th International Conference on Cryptography, Security and Privacy (CSP)*, IEEE, Apr. 2025, pp. 28–32. doi: 10.1109/CSP66295.2025.00013.

[14] H. Nejatollahi, R. Cammarota, and N. Dutt, “Flexible NTT Accelerators for RLWE Lattice-Based Cryptography,” in *2019 IEEE 37th International Conference on Computer Design (ICCD)*, IEEE, Nov. 2019, pp. 329–332. doi: 10.1109/ICCD46524.2019.00052.

[15] M. S. Ul Islam Sami, K. Zamiri Azar, H. M. Kamali, F. Farahmandi, and M. Tehranipoor, “PQC-HI: PQC-enabled Chiplet Authentication and Key Exchange in Heterogeneous Integration,” in *2024 IEEE 74th Electronic Components and Technology Conference (ECTC)*, IEEE, May 2024, pp. 464–471. doi: 10.1109/ECTC51529.2024.00079.

[16] J. J. Bermoy, J. R. M. Santos, and J. C. Y. Nicdao, “Development of a Piezoelectric Energy Harvester using the Rotational Motion of a Kalesa Wheel using a Microcontroller and IoT Monitoring,” in *2025 International Power and Sustainable Energy Technologies Conference (PSETC)*, IEEE, Aug. 2025, pp. 1–6. doi: 10.1109/PSETC65535.2025.11239162.

[17] D. Dziechciarz and M. Niemiec, “Efficiency Analysis of NIST-Standardized Post-Quantum Cryptographic Algorithms for Digital Signatures in Various Environments,” *Electronics (Basel).*, vol. 14, no. 1, p. 70, Dec. 2024, doi: 10.3390/electronics14010070.

[18] A. Jayathilake, J. Ranasinghe, D. Perera, S. Bartholomeusz, S. Rathnayake, and D. Ganegoda, “Accurate Stress Detection for Developers: Leveraging Low-Cost IoT Devices (ESP32 and MAX30102) to Analyze Heart Rate Variability via an External Mouse,” in *2023 5th International Conference on Advancements in Computing (ICAC)*, IEEE, Dec. 2023, pp. 89–94. doi: 10.1109/ICAC60630.2023.10417345.

[19] A. Li’, Z. Li, J. Tang, and Y. Lu, “KDA: Kyber and Dilithium Accelerator for CRYSTALS Suite of Post-Quantum Cryptography in Hybrid Multipath Delay Commutator Pipelined Architecture,” in *2024 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, IEEE, Nov. 2024, pp. 1–3. doi: 10.1109/A-SSCC60305.2024.10848993.

[20] K. Shilppaa and S. Kallam, “A Quantum-Resistant Cryptography for Secure IoT Communication Using Novel QRC_BIKAES Framework,” in *2025 IEEE 5th International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI SATA)*, IEEE, May 2025, pp. 1–6. doi: 10.1109/VLSISATA65374.2025.11070021.

[21] F. A. Murad *et al.*, “Development of a Data Transmission Security System on a Mobile Smart Trash Bin Using an Elliptic Curve Cryptography Algorithm,” in *2023 6th International Conference on Information and Communications Technology (ICOIACT)*, IEEE, Nov. 2023, pp. 527–532. doi: 10.1109/ICOIACT59844.2023.10455916.

[22] B. Nakum and U. Desai, “An efficient scheme based on DLP and RSA for proxy Group signature,” in *2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014)*, IEEE, Aug. 2014, pp. 1–4. doi: 10.1109/ICAETR.2014.7012827.

[23] V. Srinadh, B. Maram, and T. Daniya, “Data Security And Recovery Approach Using Elliptic Curve Cryptography,” in *2021 IEEE International Conference on Computation System and Information*

Technology for Sustainable Solutions (CSITSS), IEEE, Dec. 2021, pp. 1–6. doi: 10.1109/CSITSS54238.2021.9683473.

[24] S. Nagaich and Y. C. Goswami, "Shor's Algorithm for Quantum Numbers Using MATLAB Simulator," in *2015 Fifth International Conference on Advanced Computing & Communication Technologies*, IEEE, Feb. 2015, pp. 165–168. doi: 10.1109/ACCT.2015.16.

[25] J. Faba *et al.*, "A hybrid approach to address the transition to quantum-resistant cryptography in telecommunication environments," in *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*, IEEE, Mar. 2025, pp. 122–126. doi: 10.1109/QCNC64685.2025.00027.

[26] F. A. Murad *et al.*, "Development of a Data Transmission Security System on a Mobile Smart Trash Bin Using an Elliptic Curve Cryptography Algorithm," in *2023 6th International Conference on Information and Communications Technology (ICOIACT)*, IEEE, Nov. 2023, pp. 527–532. doi: 10.1109/ICOIACT59844.2023.10455916.

[27] P. Scalise, R. Garcia, M. Boeding, M. Hempel, and H. Sharif, "An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods," *Electronics (Basel).*, vol. 13, no. 21, p. 4258, Oct. 2024, doi: 10.3390/electronics13214258.

[28] P. A. Blanco *et al.*, "Integration of quantum random number generators with post-quantum cryptography algorithms," in *2025 25th Anniversary International Conference on Transparent Optical Networks (ICTON)*, IEEE, Jul. 2025, pp. 1–5. doi: 10.1109/ICTON67126.2025.11125447.

[29] L. Chen *et al.*, "Report on Post-Quantum Cryptography," Gaithersburg, MD, Apr. 2016. doi: 10.6028/NIST.IR.8105.

[30] A. Majumdar and R. Shrestha, "CRIS-b: A High-Speed Unified Modulo Reduction Algorithm and Hardware Architecture for CRYSTALS-Kyber," in *2025 38th International Conference on VLSI Design and 2024 23rd International Conference on Embedded Systems (VLSID)*, IEEE, Jan. 2025, pp. 49–54. doi: 10.1109/VLSID64188.2025.00022.

[31] S. Shehzadi *et al.*, "Kyber-KEM-Ascon: Benchmarking a Lightweight Post-quantum KEM on IoT Devices," in *2025 IEEE International Symposium on Circuits and Systems (ISCAS)*, IEEE, May 2025, pp. 1–5. doi: 10.1109/ISCAS56072.2025.11043792.

[32] T. Yang, Y. Zhang, S. Xiao, and Y. Zhao, "Digital signature based on ISRSAC," *China Communications*, vol. 18, no. 1, pp. 161–168, Jan. 2021, doi: 10.23919/JCC.2021.01.014.

[33] L. X. Van and L. Hong Dung, "Constructing a Digital Signature Algorithm Based on the Difficulty of Some Expanded Root Problems," in *2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*, IEEE, Dec. 2019, pp. 190–195. doi: 10.1109/NICS48868.2019.9023847.

[34] H. Nejatollahi, N. Dutt, and R. Cammarota, "Trends, challenges and needs for lattice-based cryptography implementations," in *Proceedings of the Twelfth IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis Companion*, New York, NY, USA: ACM, Oct. 2017, pp. 1–3. doi: 10.1145/3125502.3125559.

[35] Kai Yan and Yongjie Yang, “The design and implementation of classroom teaching management system based on ARM,” in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, IEEE, Oct. 2016, pp. 860–864. doi: 10.1109/CompComm.2016.7924825.

[36] L. Ren Ting, Y.-B. Leau, Y. J. Park, and J. H. Obit, “Enhancing the Performance of Elliptic Curve Digital Signature Algorithm (ECDSA) in Named Data Networking (NDN),” in *2018 8th IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, IEEE, Nov. 2018, pp. 65–69. doi: 10.1109/ICCSCE.2018.8684994.

[37] S. M. Dimitrov and D. M. Tokmakov, “Integrating data from heterogeneous wireless sensor networks based on LoraWan and ZigBee sensor nodes,” in *2020 XXIX International Scientific Conference Electronics (ET)*, IEEE, Sep. 2020, pp. 1–4. doi: 10.1109/ET50336.2020.9238256.

[38] R. B. Mendez *et al.*, “SDN-Based Hybrid Quantum-Safe Domain Intercommunication Within MadQCI,” in *2024 International Conference on Quantum Communications, Networking, and Computing (QCNC)*, IEEE, Jul. 2024, pp. 168–175. doi: 10.1109/QCNC62729.2024.00034.

[39] A. Kumar Arigela, C. Banapuram, and N. Venu, “Remote based Home Automation with MQTT: ESP32 Nodes and Node-RED on Raspberry Pi,” in *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, IEEE, Oct. 2024, pp. 313–318. doi: 10.1109/I-SMAC61858.2024.10714655.

[40] C. O’Flynn, “FlexibleIP (FIP): IPv6 stack for experimental work on low-power wireless networks,” in *2012 IEEE Online Conference on Green Communications (GreenCom)*, IEEE, Sep. 2012, pp. 145–150. doi: 10.1109/GreenCom.2012.6519631.

[41] Y. Chen *et al.*, “LETRNG—A Lightweight and Efficient True Random Number Generator for GNU/Linux Systems,” *Tsinghua Sci. Technol.*, vol. 28, no. 2, pp. 370–385, Apr. 2023, doi: 10.26599/TST.2022.9010005.

[42] Y. Wang *et al.*, “Mind the Faulty Keccak: A Practical Fault Injection Attack Scheme Applied to All Phases of ML-KEM and ML-DSA,” *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 10035–10050, 2025, doi: 10.1109/TIFS.2025.3607242.

[43] K. Mrinal and V. S, “Performance Analysis of Post-Quantum Cryptographic Algorithms in Software-Defined Networks,” in *2025 9th International Conference on Computing, Communication, Control and Automation (ICCCBEA)*, IEEE, Aug. 2025, pp. 1–6. doi: 10.1109/ICCUBEA65967.2025.11283923.