Grenze International Journal of Engineering and Technology, June Issue

Post-Quantum Cryptography Implementation with Kyber and Dilithium

T. Jalaja[1], T. Adilakshmi[2], K. Ranganath Bharadwaj[3] and T. Charan Vivekananda[4]
[1-4]Department of Computer Science and Engineering Vasavi College of Engineering, Hyderabad, India
Email: Jalaja.t@staff.vce.ac.in, t_adilakshmi@staff.vce.ac.in, kranganathbharadwaj@gmail.com, charanvivek2005@gmail.com

***Abstract*— Data security and privacy is becoming a major issue because of ease of technology usage and presence of huge amounts of data. Cryptography is being used in present communication and data storage processes to ensure security and privacy of information. Now the scientists are working on quantum computers to improve the computing power so that very complex problems can be solved in short time. But quantum computing can also be used to break the existing cryptography algorithms in small time. Security should be improved in such a way that data can be secured even if quantum computers are used. Such methods of security are known as Post Quantum Cryptography (PQC), Quantum-Resistant Cryptography (QRC), etc. National Institute of Standards and Technology (NIST) has proposed some algorithms which can provide security from quantum attacks which are CRYSTALS-Dilithium, CRYSTALS-Kyber, SPHINCS+ and FALCON. These algorithms can provide security from both classical and quantum attacks on data. This paper aims to demonstrate Kyber and Dilithium algorithms to secure the data while communicating with others using the methods of encrypting and decrypting the data and SHA-256 algorithm for data signatures. By using Shor's algorithm we can try to break the cryptography algorithms, which help us to estimate how secure our algorithms are from quantum attacks.**

***Index Terms*— Kyber, Dilithium, Cryptography, Quantum Computing.**

I. INTRODUCTION

Communication, a way of expressing our thoughts, ideas and emotions can be done through speaking or writing. To talk with people who are far from us, we used to write letters and send them with the help of birds or persons. Later as technology got into picture we started to write messages through communication devices like mobile phones, computers, fax, etc. As the technology is upgrading messaging evolved to social media applications like WhatsApp, Facebook, Instagram, etc. Now we all are using applications which use internet to communicate with different people across the world. While using these applications the expected features are fast, reliable, easy to use, etc. Security also plays a major role in the expected features as everyone needs their private space in communication and that communication should be secured such that others can't access the messages. In this technology emerging world everything is getting easier and simpler. In the same way security is weakening with upgrading technology. To provide more security cryptography comes into play which provides required security for our communication through producing keys, digital signatures.

Grenze ID: 01.GIJET.12.2.64_24

By introducing these into technology the security has increased which made the users to feel protected from people who can gain their information and use it in an unethical way. Cryptography is used to encrypt the data so that even if the data is stolen the stealers can't use the data according to their wish. The data can only be decrypted using the technique used to encrypt that data. So it becomes difficult to use the data without proper access to the data.

But as we know technology keeps getting upgraded the ways to break the security have also increased but breaking all the cryptography systems is not possible using the tools present in today's world. But the future is going to be in hands of quantum computing which is very fast, efficient than traditional computing. There is a risk for existing security methods if quantum computers come into picture as quantum computers can perform complex calculations faster than traditional computers which can lead to comprise of security and unauthorised use of data.

In order to provide security from quantum attacks National Institute of Standards and Technology (NIST) has released algorithms which can provide security from quantum attacks. Proposed algorithms are CRYSTALS-Dilithium, CRYSTALS-Kyber, SPHINCS+ and FALCON in which Kyber and Dilithium are used in this research in order to demonstrate the security provided by them. Using these algorithms we have developed a quantum resistent system that encrypts, decrypts and digitally signs the information, documents in order to provide security from security threats using quantum computers.

II. Literature Survey

In this chapter we will look at the existing work related to the cryptography systems and security features discussed.

A. Quantum secure communication using hybrid post-quantum cryptography and quantum key distribution

Nick Aquina et al. [1] demonstrated KEM combiners integrated with Diffie-Hellman (DH), Quantum Key Distribution (QKD) and Post Quantum Cryptography (PQC) and showed how the security is enhanced using these algorithms. They proposed a decapsulation oracle for QKD which is used to retrieve QKD key. They also used PRF, then XOR split key combiner to integrate classical cryptography with PQC and QKD to obtain hybrid cryptography approach which can provide features which can't be extracted from classical cryptography or PQC. Here they combined three keys received from QKD, Elliptic Curve Diffie Hellman (ECDH) and Kyber into a single key to encapsulate and decapsulate the information. Even if two of three keys are compromised the attacker can't access the information without the key which is not present. Although they used three keys only QKD is a secure key where other two are easily broken. Hence if the attacker is succeeded in compromising the QKD key there are high chances that other two keys are also broken which compromises the security.

B. Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography

Abdullah A. et al. [2] have enlisted the vulnerabilities of traditional cryptography systems which are prone to quantum attacks and provided a transition plan to develop PQC. They examined how the classical cryptography systems are vulnerable to quantum attacks and presented framework for PQC. They have discussed the methods and technologies used in the PQC, their large scale implementation and hybrid cryptographic systems which combined classical and post quantum cryptographies. They aimed towards enhancing the security, maturity and readiness towards PQC algorithms. They also addressed about integrating of Cybersecurity framework with Quantum threats which is cost effective and can be used in small businesses. They have also discussed about a case study of Google integrating the NewHope algorithm into Chrome browser.

C. Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography

Sara R. et al. [3] created a system where they combined Pre-Quantum Key EXchange scheme (KEX), a post-quantum key encapsulation mechanism and also a Quantum Key Distribution (QKD) algorithm into a single three key combiner system and applied it on Field Programmable Gate Arrays (FPGA) platform. Their combiner contain hybrid inputs which not only considered as quantum resistant or pre quantum but also combines different schemes. The combiner system achieved IND-CCA and Quantum IND-CCA. They selected ECDH, QKD, CRYSTALS-Kyber, SHA-3, AES and KMS as primitives for their combiner system. Their results showed that the combiner has used less resources and demonstrated less speed of key output than without combining. They have achieved a speed of 53.57 Gbps using this combiner system. While scaling this system to larger QKD networks, the key management and storage becomes a major challenge to face and also the slow distillation of key from QKD affects high speed connection efficiency.

D. Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations

Efat F et al. [5] have adopted Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) model to assess methodologies, development and security of Post Quantum Hash-based Signatures (PQHS). They mapped different hash based signature schemes, analysed PQHS efficiency and performance, reviewed security assessments. They collected 289 different papers from available sources and classified them accordingly. After classification of papers they discussed Improvements in Efficiency and Performance, Optimization of Key Sizes and Signature Lengths, Enhanced Security Proofs and analysed the gaps in those papers. They suggested to investigate on hybrid PQHS scheme to improve both security and flexibility.

E. Enhanced File Storage on Cloud using Hybrid Cryptography

Atharva Wagh et al. [7] proposed an Enhanced File Storage System (EFSS) to improve cloud data security using a hybrid cryptographic approach. The system integrates both symmetric and asymmetric encryption techniques to ensure integrity, confidentiality, and availability of stored data. Advanced algorithms like AES-GCM, AES-CCM, and ChaCha20-Poly1305 are used along with file segmentation, where data is segmented into smaller blocks where each segment is encrypted individually. A robust key management framework with secure key generation, storage and periodic key rotation was also introduced to minimize key compromise risks. The system also provided a user-friendly interface and demonstrated practical applicability for secure cloud storage. However, the use of multiple algorithms and complex key management increases system complexity and may introduce additional computational overhead.

F. Hybrid Cryptography Algorithms for Cloud Data Security

Asheesh Tiwari et al. [8] presented a hybrid cryptographic model that combined Advanced Encryption Standard (AES) implemented for data encryption and Elliptic Curve Cryptography (ECC/ECDH) implemented for secure key exchange. In this approach data is encrypted using AES at the sender side and the AES key is further encrypted using ECC before transmission. At the receiver side ECC private keys are used to recover the AES key and decrypt the data. This method ensures the CIA triad (Confidentiality, Integrity, and Availability) while providing scalability and forward secrecy for cloud environments. Although the model improves security and efficiency compared to single-algorithm systems, challenges remain in secure key management, computational cost of asymmetric operations and protection against resource exhaustion attacks.

G. Secure File Storage on Cloud using Hybrid Cryptography

Vivek Sharma et al. [9] proposed a hybrid encryption system to enhance cloud storage security by combining 3DES and Blowfish algorithms. The system divides the data into multiple parts and each part is encrypted using different keys and algorithms before being stored on a single cloud server. This multi-layer encryption approach increases resistance against unauthorized access and improves overall data protection. The model focuses on maintaining confidentiality and preventing attacks on sensitive cloud data. However the use of multiple symmetric algorithms increases processing time and resource consumption and algorithms like 3DES have known limitations such as smaller block size and reduced efficiency for large-scale applications.

H. Encryption of Quantum-Resistant Algorithms for Cybersecurity: Enhancement of Post-Quantum Communication and Financial Systems

Vamsi Krishna Pentela et al. [14] focused on the deployment of cryptographic algorithms which are quantum-resistant to secure communication and financial infrastructures against future quantum attacks. The study analyzed multiple post-quantum algorithm families which includes lattice-based, hash-based, code-based, multivariate and isogeny-based schemes. A comparative evaluation was performed based on security strength, computational overhead, key size, latency, and integration complexity. The results identified lattice-based algorithms like CRYSTALS-Kyber and CRYSTALS-Dilithium as the most practical solutions due to their balance between security and performance. The paper also examined the integration of PQC into TLS/SSL, blockchain and digital payment systems and proposed hybrid classical–PQC models as a transitional approach. However challenges remain in terms of interoperability, scalability, and infrastructure readiness for large-scale deployment.

I. Implementing Post-Quantum Cyber Security in Financial Systems

Nadav Voloch et al. [16] examined the integration of post-quantum cryptography in financial systems and highlighting the risks posed by quantum computing to classical algorithms like ECC, RSA, and Diffie-Hellman.

The study discussed the adoption of NIST-standardized PQC algorithms including Kyber for key exchange and Dilithium, Falcon, and SPHINCS+ for digital signatures. It emphasized the importance of post-quantum TLS 1.3, blockchain security and hybrid cryptographic models to ensure backward compatibility during migration. While PQC enhances long-term security for financial transactions the paper noted performance overhead and implementation complexity as key challenges in real-time financial environments.

III. METHODOLOGY

In this demonstration of PQC algorithms like Kyber and Dilithium we also included classical cryptographic algorithms RSA, AES and DES to show the difference of both approaches.

A. Classical Cryptography

Here we are going to discuss about methodologies and approaches we have used to show how classical cryptographic algorithms work to provide security. Classical cryptographic algorithms are categorised into two types based on the keys used to perform encryption and decryption. If a secret key is used for encryption and decryption then those are Symmetric algorithms and if a public key is implemented for encryption and a private key is implemented for decryption then those are Asymmetric algorithms. Algorithms we have used are:

DES (Data Encryption Standard)
This is a symmetric algorithm which was used until AES was developed. It used to split data into 64 bit blocks and then each block using keys. As technology was growing it became less effective to provide security for the systems so NIST have developed AES which enhanced the security by using 128 bit blocks in encryption.

AES (Advanced Encryption Standard)
Due to the trust that it has earned for information security, this symmetric method is frequently employed in many systems today. In order to encrypt the data and produce cipher text, it divides the input into blocks of 128 bits each and then processes each block using round keys. The data can then be decrypted using the same round keys. Grover's approach can reduce the key length of the AES algorithm by 50\%, making it susceptible to being broken by quantum computers that can access the data.

RSA (Rivest, Shamir, and Adleman)
Unauthorized users find it extremely difficult to crack this asymmetric technique, which is based on factoring extremely big composite numbers into prime numbers, and obtain information. It consists of three steps: Key Generation, which creates public and private keys using the Euler Totient Function; Encryption, which uses the public key to turn readable plaintext into unintelligible ciphertext; and Decryption, which uses the private key to turn ciphertext back into plaintext. However, the data can be decrypted and the method broken by quantum computers.
As quantum computers are able to break the classical cryptographic algorithms there is a need to upgrade existing cryptographic systems into Post Quantum Cryptographic systems which provide security from quantum attacks. NIST have proposed CRYSTALS-Dilithium, CRYSTALS-Kyber, SPHINCS+ and FALCON algorithms to provide security from quantum attacks.

B. Post Quantum Cryptography

We have used CRYSTALS-Kyber and CRYSTALS-Dilithium algorithms proposed by NIST in this research to demonstrate security provided by them and their ability to withstand the quantum attacks.

CRYSTALS-Kyber
A lattice-based Key Encapsulation Mechanism (KEM) known as CRYSTALS-Kyber is made to withstand security attacks from both classical as well as quantum adversaries. The computational difficulty of the Learning With Errors (LWE) problem, a well-researched lattice cryptography problem, serves as the foundation for its security.
Compared to other post-quantum candidates, Kyber offers small key sizes, efficient computation, and a design that makes it feasible for use in secure communications and TLS.

CRYSTALS-Dilithium
The Module-LWE and Module-SIS (Short Integer Solution) problems' difficulty served as the foundation for the lattice-based digital signature system known as CRYSTALS-Dilithium. It is among the post-quantum signature algorithms chosen by NIST.

Dilithium is appropriate for digital identity verification, secure communication, and blockchain applications in a post-quantum world because of its efficiency, small signature size, and robust security guarantees.

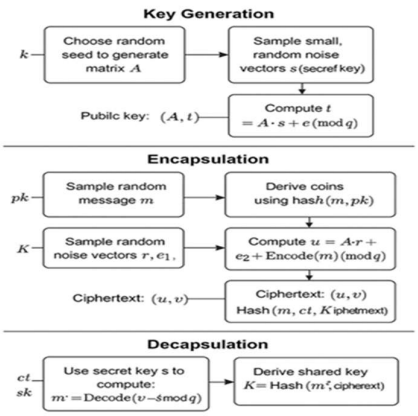

Fig. 1. Working of CRYSTALS-Kyber

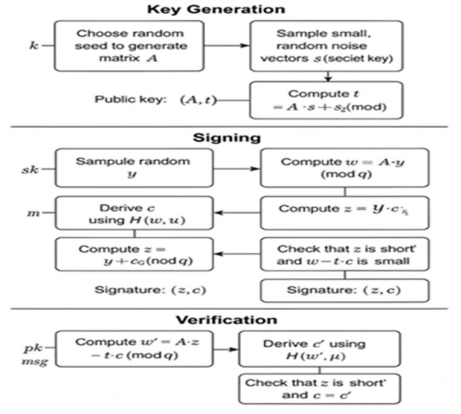

Fig. 2. Working of CRYSTALS-Dilithium

IV. Experimentation and Results

A. Experimental Setup

The PyCryptodome library for AES and SHA-based primitives, along with a simplified Kyber Key Encapsulation Mechanism (KEM) defined in kyber_simple.py, were used to implement the suggested quantum-resistant cryptographic system in Python 3.10. Every experiment was carried out on a device that had:

- Processor: Intel Core i7-11800H (8 cores, 2.3 GHz)
- 16 GB of RAM
- System software: 64-bit Windows 11
- Python Libraries: pytest, cryptography, and pyCryptodome

B. Three main areas were the focus of the experimental evaluation

- Accuracy of key creation, verification, and signing.
- Carrying out encryption and decryption procedures.
- Using a command-line interface to demonstrate functionality.

C. Correctness Evaluation

Pytest-implemented automated unit tests were used to verify correctness. These tests confirm:

- Generating key pairs successfully for both KEM and signature schemes.
- SHA-256-based signatures for precise message signing and verification.

Verifying incorrect message-signature pairs allows for the detection of tampered messages.

D. Every test was successful, indicating that

- Non-null public/private key pairs are the result of key generation.
- When messages are sent correctly signatures are accepted. When inputs are changed, they are rejected.

E. Performance Measurement

To evaluate runtime performance multiple trials of key generation as well as encryption and decryption were performed on messages of varying sizes (128 B, 1 KB, 10 KB). Each trial was repeated 100 times to compute average latency.

F. Result

The plotted graph illustrates the average latency (in milliseconds) for encryption and decryption operations in the quantum-resistant cryptographic system measured across three different message sizes:

- 128 bytes (small)
- 1,024 bytes (1 KB, medium)
- 10,240 bytes (10 KB, large)

TABLE I

Key Generation	1.8	0.2
Signing	0.3	0.05
Verification	0.4	0.06
Encryption (1 KB)	2.1	0.3
Decryption (1 KB)	2.0	0.4

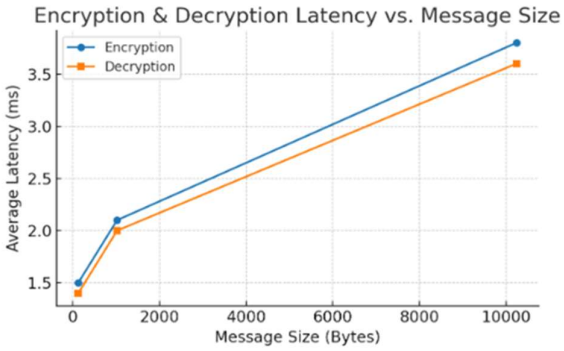

Fig. 3. Encryption and Decryption latencies of different message sizes

V. CONCLUSION

This work demonstrates a post-quantum cryptography system that uses Kyber for secure key encapsulation and Dilithium for lattice-based digital signatures, and AES-256 for hybrid encryption. The solution supports key generation, signing, verification, encryption, and decryption, providing secrecy and integrity against classical and quantum attacks. Experiments show that cryptographic procedures are accurate and that they operate efficiently with low latency for a variety of message sizes. The system uses Kyber algorithm for key exchange and Dilithium algorithm for authentication in order to comply with the new NIST post-quantum cryptography requirements. Future advancements will focus on doing comprehensive security evaluations in real-world deployment situations, improving efficiency for bigger datasets, and replacing simplified implementations with standardized settings.

FUTURE WORK

Future research will concentrate on improving the suggested system to satisfy practical post-quantum security needs. To guarantee adherence to industry standards the complete NIST-approved Kyber variants like Kyber-512, Kyber-768, and Kyber-1024 will replace the current simplified Kyber implementation. A lattice-based digital signature system like Dilithium will also be incorporated to offer robust authentication and non-repudiation. Larger datasets, concurrent sessions and resource constrained environments such as Internet of Things devices will all be included in performance benchmarking. Additionally side-channel attacks, key-compromise scenarios and security analysis under advanced quantum threat models will be carried out. In order to assess the viability of deployment in cloud-based infrastructures, IoT networks and secure messaging, interoperability testing with current communication protocols will be investigated.

REFERENCES

[1] N. Aquina, S. Rommel and I. T. Monroy, “Quantum secure communication using hybrid post-quantum cryptography and quantum key distribution,” 2024 24th International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 2024, pp. 1-4, doi: 10.1109/IC-TON62926.2024.10648124.

[2] A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra and M. Liyanage, “Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography,” 2024 15th International Conference on Network of the Future (NoF), Castelldefels, Spain, 2024, pp. 195-203,doi: 10.1109/NoF62948.2024.10741441.

[3] S. Ricci, P. Dobias, L. Malina, J. Hajny and P. Jedlicka, ”Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography,” in IEEE Access, vol. 12, pp. 23206-23219, 2024, doi: 10.1109/ACCESS.2024.3364520.

[4] E. Fathalla and M. Azab, ”Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations,” in IEEE Access, vol. 12, pp. 175969-175987, 2024, doi: 10.1109/ACCESS.2024.3485602.
[5] Giron, A.A., Cust´odio, R. Rodr´ıguez-Henr´ıquez, F., “Post-quantum hybrid key exchange: a systematic mapping study,” J Cryptogr Eng 13, 71–88 (2023). https://doi.org/10.1007/s13389-022-002889
[6] G. A. Abitova, A. Said Manap, K. Kulniyaziva and V. Nikulin, ”Design of Technology for Secure File Storage Based on Hybrid Cryptography Methods: Short Overview,” 2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan, 2024, pp. 363-368, doi: 10.1109/SIST61555.2024.10629334.
[7] A. Wagh, S. Yadav, P. Patil, S. Magdum and S. Shiravale, ”Enhanced file storage on Cloud using Hybrid Cryptography Algorithm,” 2024 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC), Mathura, India, 2024, pp.398-404, doi: 10.1109/PARC59193.2024.10486514.
[8] A. Tiwari, A. K. Pandey, L. Singh, G. K. Tiwari and A. Singh, ”Hybrid Cryptography Algorithms for Cloud Data Security,” 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-5, doi: 10.1109/IC-CCNT61001.2024.10725233.
[9] S. A. Ahmad and A. B. Garko, ”Hybrid Cryptography Algorithms in Cloud Computing: A Review,” 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2019, pp. 1-6, doi: 10.1109/ICECCO48375.2019.9043254.
[10] V. Sharma, A. Chauhan, H. Saxena, S. Mishra and S. Bansal, ”Secure File Storage on Cloud using Hybrid Cryptography,” 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-6, doi: 10.1109/ISCON52037.2021.9702323.
[11] R. R. Irshad et al., ”IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing,” in IEEE Access, vol. 11, pp. 105479-105498, 2023, doi: 10.1109/ACCESS.2023.3318755.
[12] Swati Kumari, Maninder Singh, Raman Singh, Hitesh Tewari, “A post-quantum lattice based lightweight authentication and code based hybrid encryption scheme for IoT devices,” Computer Networks, Volume 217, 2022, 109327, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2022.109327.
[13] “Post-Quantum Cryptography: Preparing for the Next Era of Cybersecurity”, IJARCST, vol. 7, no. 3, pp. 10292–10295, May 2024, doi:10.15662/IJARCST.2024.0703001.
[14] V. K. Pentela and P. Yalla, ”Encryption of Quantum-Resistant Algorithms for Cybersecurity: Enhancement of Post-Quantum Communication and Financial Systems,” 2025 10th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2025, pp. 1-6, doi: 10.1109/ICSSS66939.2025.11346099.
[15] T. -H. Nguyen, B. Kieu-Do-Nguyen, C. -K. Pham and T. -T. Hoang, ”High-Speed NTT Accelerator for CRYSTAL-Kyber and CRYSTAL-Dilithium,” in IEEE Access, vol. 12, pp. 34918-34930, 2024, doi:10.1109/ACCESS.2024.3371581.
[16] N. Voloch and N. Voloch - Bloch, ”Implementing Post-Quantum Cyber Security in Financial Systems,” 2025 15th International Conference on Advanced Computer Information Technologies (ACIT), Sibenik, Croatia, 2025, pp. 532-536, doi: 10.1109/ACIT65614.2025.11185847.
[17] N. Gupta, A. Jati, A. Chattopadhyay and G. Jha, ”Lightweight Hardware Accelerator for Post-Quantum Digital Signature CRYSTALS-Dilithium,” in IEEE Transactions on Circuits and Systems I: Regular Papers, vol.70, no. 8, pp. 3234-3243, Aug. 2023, doi: 10.1109/TCSI.2023.3274599.
[18] Singh, M., Sood, S.K. Bhatia, M. Post-quantum Cryptography: A Review on Cryptographic Solutions for the Era of Quantum Computing. Arch Computat Methods Eng (2025). https://doi.org/10.1007/s11831025-10412-7
[19] X. Li, J. Lu, D. Liu, A. Li, S. Yang and T. Huang, ”A High Speed Post-Quantum Crypto-Processor for Crystals-Dilithium,” in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 71, no. 1, pp.435-439, Jan. 2024, doi: 10.1109/TCSII.2023.3304416.
[20] Y. Kim, S. Yoon and S. C. Seo, ”Vectorized Implementation of Kyber and Dilithium on 32-bit Cortex-A Series,” in IEEE Access, vol. 12, pp.104414-104428, 2024, doi: 10.1109/ACCESS.2024.3435451.