Analysis of Post Quantum Cryptography Algorithms concerning their applicability to IoT devices

Hasham Sarwar
Bahria University Islamabad, Pakistan
hsarwar0337@gmail.com
Anjum Ashraaf
Bahria University Islamabad, Pakistan
anjumashraaf786@gmail.com

***Abstract*—The increasing ubiquity of Internet of Things (IoT) devices has necessitated robust security measures, especially with the impending threat of quantum computing to conventional cryptographic protocols. In this study, we address the imperative of selecting an optimized post-quantum cryptographic algorithm tailored for implementation on resource-constrained IoT devices while ensuring compliance with stringent security standards. This research employs a comprehensive evaluation framework that considers the unique constraints of IoT devices, including limited computational capabilities and memory resources. Furthermore, our assessment accounts for the diverse security requirements stipulated by prevailing standards to guarantee resilience against both classical and quantum threats. Through a systematic analysis of various post-quantum cryptographic algorithms, encompassing factors such as computational efficiency and resistance to quantum attacks, this study identifies a select set of algorithms that exhibit promising suitability for IoT device deployment. The evaluation considers renowned standards, including NIST's Post-Quantum Cryptography Standardization initiative to align with industry best practices and interoperability. The findings presented in this study offer guidance to IoT device manufacturers, system architects, and security practitioners in making informed decisions regarding the adoption of post-quantum cryptographic algorithms. The selected algorithms not only demonstrate adeptness in mitigating quantum threats but also address resource constraints inherent in IoT environments, ensuring a secure foundation for the rapidly expanding ecosystem of interconnected devices.**

***Index Terms*—Post Quantum, PQ cryptography for IoT, Iot Constrainted PQC Algorithm**

I. Introduction

POST - quantum cryptography remains a basic wilderness in getting the undeniably interconnected scene of IoT gadgets. The IoT environment, portrayed by its huge swath of interconnected gadgets and frameworks, has upset ventures, homes, and urban communities, yet it additionally brings to the front phenomenal security challenges. As these gadgets trade delicate data, the need to shield this information against arising dangers, especially quantum registering, has become basic. Quantum computing, with its capability to break customary cryptographic calculations through its sheer computational power, represents a huge danger to the security infrastructure on which present-day IoT frameworks depend. The vulnerability of these frameworks requires a proactive methodology — one that expects and mitigates likely breaks through the reception of post-quantum cryptographic calculations. The center challenge lies not simply in that frame of mind of post-quantum algorithms but in distinguishing ones that are upgraded for implementation on asset-completed IoT gadgets. These gadgets frequently have restricted computational abilities, memory, and power assets contrasted with conventional registering frameworks. In this manner, any cryptographic arrangement carried out inside the IoT system should find some kind of harmony between security powerfulness and asset productivity [1]. Tending to this test requires a thorough assessment system that takes into account the assorted elements affecting the reasonableness of post-quantum cryptographic calculations for IoT sending. One significant viewpoint is the computational proficiency of algorithms like NtruEncrypt [1], taking into account the requirements of IoT gadgets. Calculations that request negligible computational power while offering powerful protection from both regular and quantum dangers become crucial in this specific circumstance. Memory impression addresses another urgent thought. IoT gadgets, frequently outfitted with restricted memory, require cryptographic calculations that are light on memory utilization. Adjusting this prerequisite without settling for less on the security stance of the algorithm turns into a characterizing model in the determination cycle. Additionally, any picked calculation requirements to line up with existing security guidelines to guarantee interoperability, consistency, and future sealing. Principles set by associations like NIST (Public Foundation of Norms and Innovation) offer pivotal benchmarks for cryptographic conventions, guaranteeing they meet the tough security prerequisites while advancing similarity across different IoT executions. The scene of post-quantum crypto-realistic calculations is tremendous, with various competitors competing for consideration. A few unmistakable competitors incorporate lattice-based, hash-based, code-based, and multivariate-based cryptographic plans, each with its one-of-a-kind qualities and shortcomings concerning IoT sending. Thinking about these calculations in contrast to foreordained models and principles becomes essential in the choice cycle [2]. Notwithstanding the cryptographic strength, factors like simplicity of execution, versatility to IoT- explicit correspondence conventions, and obstruction against side-channel assaults are additionally vital in the dynamic favorable to the process. These elements guarantee that the picked calculation not only satisfies the security guidelines yet in addition coordinates crease lessly

inside the IoT biological system, defending against potential weaknesses. The result of this assessment is essential, as it guides IoT gadget makers, framework engineers, and security experts in coming to informed conclusions about the choice and execution of post-quantum cryptographic calculations. The chosen calculations need to not just endure the dangers presented by quantum computing yet in addition adjust to the asset requirements intrinsic in the IoT environment. Certainly! In the domain of post-quantum cryptography, a few groups of 4 cryptographic techniques have arisen as possible up-and-comers for getting IoT gadgets against quantum dangers. These include hash-based, code-based, multivariate-based, and lattice-based cryptographic plans, each with its interesting ascribes, what's more, reasonableness for execution on asset obliged IoT gadgets.

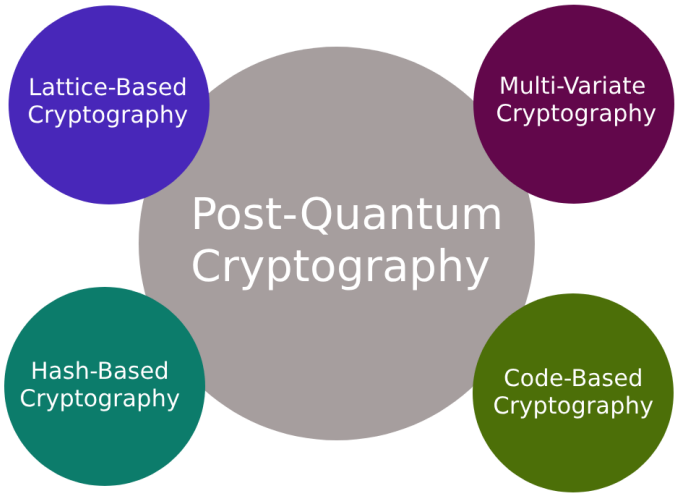

Fig. 1: Types of PQC

1) Hash-Based Cryptography: Hash-based cryptographic calculations, for example, the Merkle tree-based structures like XMSS (Broadened Merkle Mark Plan), offer flexibility against quantum assaults. These plans depend on the collision safe properties of hash capabilities. XMSS, for example, gives a stateful mark plot that can be proficiently executed on asset obliged gadgets. Its security comes from the one-wayness of cryptographic hash capabilities, guaranteeing obstruction against quantum enemies [3].

2) Code-Based Cryptography: Code-based cryptographic calculations, prominently the McEliece cryptosystem, influence the trouble of unraveling mistake amending codes to give security. In spite of its huge security edges against quantum foes, the McEliece cryptosystem generally shows bigger key sizes, which could present difficulties with regards to IoT gadgets with obliged assets. Notwithstanding, endeavors are continuous to enhance its execution for IoT conditions by diminishing its computational above [4].

3) Multivariate-Based Cryptography: UOV (Unbalanced Oil and Vinegar) schemes which is bassically a Multivariate-based cryptographic schemes and it depend on the intricacy of addressing frameworks of multivariate polynomial conditions. UOV offers minimal marks and generally more modest key sizes, making it a likely possibility for IoT organizations. In any case, it requires cautious boundary choice to adjust security and proficiency in asset compelled conditions [5].

4) Lattice-Based Cryptography: Lattice-based cryptography has acquired huge consideration because of its robustness against quantum assaults and its flexibility in offering different cryptographic natives. Plans like NTRUEncrypt and NTRUSign in light of lattice issues areas of strength for give and have shown promising flexibility to asset compelled IoT gadgets. They offer more modest key sizes and productive executions, making them practical choices for getting IoT biological systems [6].

A. Quantum Threats

Quantum algorithms like Shor's and Grover's algorithm, represents a considerable threat to existing cryptographic frameworks, especially those utilized in asset obliged IoT (Web of Things) gadgets. Shor's calculation, for example, has the ability to proficiently factor huge numbers, compromising generally utilized cryptographic algorithm like RSA and ECC (Elliptic Bend Cryptography). All the while, Grover's calculation speeds up the method involved with looking through unsorted information bases, possibly compromising symmetric key cryptography.

The limited computational power of IoT gadgets fuel the danger, as quantum PC progressed they could take advantage of weaknesses in current Crypto-System. This increase the requirement to adapt post-quantum cryptographic algorithm. guaranteeing the security and protection of IoT environments despite advancing computational capacities [7].

1) Grovers Algorithm: The goal is to look in an unstructured dataset, where there could be no prior information about the pursuit space. Traditional calculation routinely require O(n) errands to find the ideal dataset in a vector space with N parts. On the other hand, Grover's estimation on a very basic level further develops efficiency by diminishing the fundamental errands to simply $O(\sqrt{n})$, presenting a quadratic speedup in the chase cycle [20]. The states are prepared in superposition of qubit states, where the prophet i.e., a lot of unitary directors mark the game plan state in superposition, things being what they are. Further improvement is done to extend the probability of the market state. The checking of the game plan is a singular step movement in QC, while improvement requires Grover's cycles. There emphasess achieve extended probability of market state. Here, the quantum parallelism achieves the wonderful advance as it plays out the all-on monster force attack in a single step not by any stretch of the imagination like the dated cycle procedure, where the savage power is executed in an iterative circle for instance step-by- step.

2) Shor's Algorithm: Shor's algorithm is famous for having the potential to break the currently widely used encryption (e.g., RSA), and it was the invention of Shor's algorithm that ignited the widespread interest in quantum computing in the late 1990s. The quantum computing part of Shor's algorithm is only for period finding. It is then combined with a classical algorithm to perform integer factorization in order to break the classical encryption [21]. The implementation

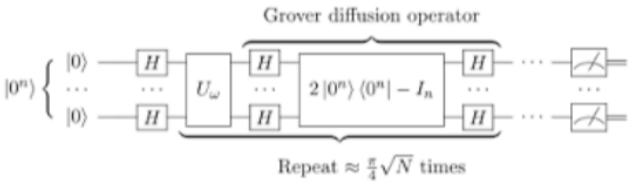

Fig. 2: Grovers Algorithm

of Shor's algorithm allows the parallel implementation of function, . This process requires classical computers steps for each computation of. Whereas, the quantum superposition results in implementation of combinations of modular function in a single step by using the control and target qubit approach to implement unitary operator of the function described above. Here, due to modular function a periodicity in the states is observed, this periodicity is extracted by applying the quantum Fourier transform on the whole qubit register. Again, here measuring the state would have not given enough information. Further, classical evaluation methods like Chinese remainder theorem are used for estimation of coprime numbers that form the key of RSA. The basic functions of all these algorithms

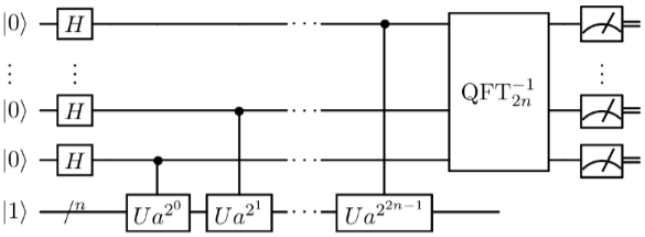

Fig. 3: Quantum Parallelism

can be reduced in three simple steps,

- Apply superposition to all the qubits in one register.
- Have another register initialized as needed.
- Apply a controlled-unitary operation on the second register with control at the first register of qubits.

Here, controls can be on multiple and different qubit registers, which results in different state of second register for each respective control state. Here, the actual parallelism is applied. Further, different amplification or Fourier transform can be applied as per need. Here, measurement is not the solution.

II. Related Studies

The internet of Things (IoT) plays expected an essential part in the headway of correspondence innovation and in our day to day lives. Satrya et al. in [8] tended to security lacunae in the geography and design of IoT energy observing frameworks utilizing post-quantum cryptographic strategies. They proposed custom fitted executions of the Rivest-Shamir-Adleman (RSA), N-th degree Shortened Polynomial Ring Units (NTRU), and a set-up of cryptographic natives in view of Module Learning With Adjusting (Saber) as post-quantum cryptographic competitor calculations for IoT gadgets. These expect to get distributer supporter start to finish correspondence in energy framework observing. Moreover, they offer a near examination of these custom fitted executions on low-asset gadgets, for example, the Raspberry Pi, during information transmission utilizing the Message Lining Telemetry Transport (MQTT) convention. Results show that the modified execution of NTRU beats both SABER and RSA regarding computer processor and memory utilization, while Light SABER arises as the leader while considering encryption and unscrambling delays.

Jain et al. in [9] examined cryptography calculations and conventions of IoT with various classifications. Coordinated PQC of Public Foundation of Principles and Innovation (NIST) third level finalists on Raspberry Pi 4 (RPI4) board with Linux working framework. The presentation of Post-Quantum Cryptography plans for IoT has been assessed. At last, a Post-Quantum Cryptography conspire has been recommended for the Web of Things in light of the presentation examination.

T. M. Fernández-Caramés in [10] gave a study on post-quantum IoT frameworks (IoT frameworks safeguarded from the at present realized quantum registering assaults): the primary post-quantum cryptosystems and drives were explored, the most important IoT structures and difficulties were examined, and the normal future patterns were demonstrated.

S. Sarıbaş et al. in [11] picked three key epitome systems and two computerized signature calculations with various boundary sets from the cycle three entries. They estimated their TLS 1.3 handshake execution utilizing two asset obliged gadgets and contrasted it with that of old style encryption and advanced signature plans. Try results showed that post-quantum calculations accompany an additional message above while their handshake defer values are promising.

J. Señor et al. in [1]measures the exhibition of one of the finalists of the normalization cycle called NTRU and carried out it in a custom remote sensor hub intended for applications in the outrageous edge of the IoT. The cryptosystem is executed and assessed inside the cycles of the Contiki-NG working framework. Moreover, extra examinations are performed to check in the event that ordinarily coordinated equipment peripherals for cryptography inside present day microcontrollers can be utilized to accomplish better execution with NTRU, at the single hub level as well as at the organization level, where the NTRU key exemplification component is tried in a genuine correspondence process. The outcomes got from these tests show that NTRU is reasonable for current microcontrollers focusing on remote sensor networks plan, while old gadgets present in well known stages probably won't manage the cost of the expense of its execution.

Asif et al. in [12] gave an exhaustive study to academic local area with complete data on rudimentary numerical realities, as well as to address continuous execution, equipment engineering, open issues, assault vectors, and the importance for the IoT organizations. The study includes comes about because of existing traditional calculations and understanding into the post quantum hash based cryptography.

O. M. Guillen et al. in [13] introduced an examination of NTRUEncrypt's benefits over other cryptosystems for use in such gadgets. They depict four unique NTRUEncrypt executions on an ARM Cortex M0-based microcontroller,

think about their outcomes, and show that NTRUEncrypt is appropriate for use in battery-worked gadgets. They present execution and memory impression figures for various security boundaries, as well as energy utilization in an asset compelled microcontroller to reinforcement these cases.

Seyhan et al. in [14] analyzed crucial attributes and layered design of IoT conditions. Essential security necessities and arrangement innovations for IoT design were recollected. A few significant open issues in the writing for IoT gadget security are reviewed. From these open issues, the post-quantum security of IoT gadgets with restricted assets is engaged. The fundamental reason for their paper is to further develop the obliged asset order and give a perspective for post-quantum IoT security. In this specific circumstance, a touchy characterization is proposed by further developing the restricted asset grouping of IETF. The cryptosystem proficiency definition is made for the examination of asset obliged gadget security. Utilizing the proposed arrangement and effectiveness definition, the use of grid based cryptosystems in asset obliged IoT gadget security is dissected.

S. Ebrahimi et al. in [15] Propose InvRBLWE, an advanced variation for double learning with blunders over the ring (Ring-LWE) plot that is shown to be secure against quantum assaults and is exceptionally effective for equipment executions. They propose two designs for InvRBLWE: 1) a high velocity engineering focusing tense and strong IoT gadgets and 2) a ultralightweight design, which can be carried out on asset obliged hubs in IoT. They give trial results to two adaptations of the InvRBLWE plot giving 84 and 190 pieces of exemplary security. Their execution results on field programmable door exhibit overwhelm the best of the work of art and post-quantum past executions. In addition, two distinct application explicit coordinated circuit (ASIC) executions show improvement with regards to speed, region, power, or potentially energy.

K. Mayes et al. in [16] introduced examination from a down to earth execution of the Kyber768 CPAPKE public key encryption part on a MULTOS IoT Trust-Anchor chip. The examination thought about memory and speed necessities, and improvements, and looked at the NTT change variant of Kyber, introduced in Cycle 1 of the NIST rivalry, with the Kroenecker multiplier method that takes advantage of an equipment crypto-coprocessor. The work started with a nonexclusive multi-round multiplier approach, which was then superior utilizing an original change of the info information, permitting an implicit particular duplicate capability to be utilized, essentially speeding up an increase round, and multiplying the useable size of the equipment multiplier.

R. Ristov et al. in [17] investigated public key encryption (PKE) with post quantum cryptography (PQC) calculation Kyber, in spite of it being typically utilized as key-exemplification system (KEM). The proposed approach has been assessed tentatively. The led explore scrambles the information on one situation on the IoT gadget itself and in the other situation the information is encoded on a haze hub.

Alessandra et al. in [18] proposed a Keccak gas pedal to accelerate SHA3 calculations for the Gems Kyber calculation on the RISCV-based progressed microcontroller PULPissimo. Contrasted with the plain SW execution on RISC-V, our outcomes show a speedup element of up to 2.79 to the detriment of a 12.4 percent assets above. Public Organization of Guidelines and Innovation (NIST) reported SHA-3 as the new norm for better security. SHA-3 is additionally taken advantage of in the vast majority of the ongoing post-quantum cryptographic (PQC) conventions.

A. Khalid in [19] studies the common sense of organization of Cross section based Calculations (LBC) plans. In this unique circumstance, the cutting edge LBC executions on the obliged gadgets (counting low-power FPGAs and implanted chip), driving as far as low-power impression, little region, minimized data transfer capacity necessities and elite execution is reasonably assessed and seat stamped. The work closes by distinguishing a set-up of some most loved LBC plans as far as different IoT basic execution seat marks.

III. Our Contribution

In our investigation, we dig into the assessment of post-quantum calculations concerning their speed and adherence to the NIST security standard. Collecting assorted discoveries from different sources, we unite this data into a complete paper to recognize the most effective calculations for IoT gadgets, accentuating both speed and security con- sider- ations. Our methodology includes investigating the presentation furthermore, energy utilization effects of current post-quantum key trade components, especially those partaking in the NIST normalization process. We select calculations helpful to programming executions and continue to quantify their im-settlement on asset obliged IoT gadgets. The summit of our work offers rules for choosing ideal cryptosystems for IoT gadgets, taking into account the predetermined requirements. Our commitments are illustrated as follows:

- Showing the joining of post-quantum cryptosys- tems into IoT gadgets in their current structure.
- Consolidating round 3 calculations in the NIST contest for post-quantum encryption norms into predominant IoT programming and equipment.
- Measuring the effect of different post-quantum encryption calculations on gadget asset utilization.
- Giving useful rules to choosing a cryptosys- tem custom-made to the imperatives forced on IoT gadgets

IV. Methods

In this SLR we present different but important cryptosystems participating in the NIST standardization process, we also consider the resource-constrained IoT. we primarily focus on highlighting their key aspect along with the time needed to generate key pairs, encryption, and decryption on Raspberry Pi 4. In our final phase, we try to identify and provide justification for different aspects and reasons behind the selection of these algorithms by using a systematic process of data collection, exploration, and interpretation Our objective is to conduct a comprehensive analysis of diverse results extracted from various papers. we specifically chose those papers that perform their experiment on Raspberry Pi for our specific purpose which is to extract the most suitable post-quantum algorithm

for key sharing and digital signatures within the considered context.

Our picked area of assessment rotates around post-quantum cryptosystems of definite round in the NIST normalization process. This determination is propelled by the expectation of these cryptosystems being integrated into industry organizations and coordinated into libraries that asset obliged gadgets will use for web correspondence.

As of the ongoing composition, the NIST normalization process is progressing through its third stage, highlighting fifteen up-and-comers. Among these, seven have been assigned as finalists, while eight are being considered as possible other options. This unique scene prompts our examination concerning their flexibility, taking into account the advancing idea of the determination cycle. Table I shows the finalists for NIST normalization. As per the writing, the cryptosystems generally reasonable to asset obliged gadgets are those cross section based [22].

Public-Key Encryption/KEM	**Digital Signatures**
Classic McEliece	CRYSTALS-DILITHIUM
CRYSTALS-KYBER	FALCON
NTRU	Rainbow
Saber	

TABLE I: Post-Quantum Cryptosystems Parameters

Table II below shows the algorithms and their parameters associated with them. The table also highlights the security level of each algorithm as per NIST security standards.

Algorithm	**Public-Key Size**	**Private-Key Size**	**Ciphertext Size**	**Security Level**
SABER (LightSaber)	672	992	1312	1
CRYSTAL-KYBER	1632	800	736	1
NTRU	699	935	699	1
NTRU Prime	897	1125	1025	2
FrodoKEM	9616	19888	9720	1

TABLE II: Post-Quantum Cryptosystems Parameters

Table (III) provides a comparative analysis of clock cycle efficiencies for key generation, encryption, and decryption in the Kyber and LightSaber cryptographic algorithms. Meanwhile, the table (IV) offers additional insights into specific variants such as Kyber512 and Saber-KEM, detailing their respective performances in key generation, encapsulation, and decapsulation operations.

The Table V presents an exhibition examination of post-quantum cryptographic calculations, explicitly Dilithium2 and Falcon512, with regards to key age, encapsulation, and decapsulation tasks. Clock cycle efficiencies are accounted for each cryptographic variation, giving experiences into their computational prerequisites for secure tasks with regards to the Web of Things.

Algorithm	Key Gen	Encrypt	Decrypt
Kyber	649678	884848	985258
Lightsaber	1051530	1538646	1861934

TABLE III: Analysis of the Kyber and LightSaber [1]

Crypto System	Variant	Key Generation	Encapsulation	Decapsulation
Kyber	Kyber512	237267	252163.8	252939.6
Saber	Saber-KEM	358270.2	357384.6	356729.4

TABLE IV: Analysis of Post-Quantum Cryptography for Internet of Things [9]

Table VI presents execution measurements for the Kyber512 post-quantum secure calculation in the TLS convention, explicitly zeroing in on key age, encapsulation, and decapsulation processes. The outcomes exhibit the calculation's effectiveness in cryptographic tasks.

Table VII gives a relative investigation of post-quantum cryptosystems for Web of-Things (IoT) applications, exhibiting key age, encapsulation, and decapsulation times for Kyber512 and LightSaber calculations. The outcomes highlight the presentation varieties between these cryptographic frameworks with regards to IoT security.

Table VIII frameworks the presentation measurements for various Kyber key boundaries, introducing the time taken for key pair age, encryption, and decryption process. Quite, the table features the productivity of Kyber512 and Kyber512_aes in different cryptographic tasks, estimated in milliseconds.

Table IX gives execution measurements to various key boundaries, including the time expected for key pair age, encryption, and decoding processes. Prominently, it grandstands the proficiency of EES1087EP2, APR2011_439_fast, and APR2011_743_fast in different cryptographic activities, estimated in milliseconds.

Table X presents execution measurements for various key boundaries, including key pair age, encryption, and decoding processes estimated in a large number of cycles (k Cycle). Furthermore, it gives data on the measures of private keys, public keys, plaintexts, and ciphertexts in bytes. The outcomes offer bits of knowledge into the computational necessities and information sizes related with key tasks for the predetermined key boundaries.

Table XI gives key boundary execution measurements to the Hawk cryptographic framework, highlighting key age, marking, and confirmation processes estimated in a great many cycles (k Cycle). Moreover, it remembers the size of the produced computerized signature for bytes. These measurements offer experiences into the computational expenses and mark sizes related with Falcon_512 key activities.

Table XII presents key parameter performance metrics for the Sha256withRSA cryptographic system, including key generation, signing, and verification processes measured in thousands of cycles (k Cycle). The table also indicates the

Crypto System	Variant	Key Gen	Encapsulation	Decapsulation
Dilithium	Dilithium2	483283.8	2034835.2	485231.4
Falcon	Falcon-512	87717058.2	23680247.4	269701.2

TABLE V: Analysis of Post-Quantum Cryptography for Internet of Things [9]

Crypto System	Key Gen	Encapsulation	Decapsulation
Kyber512	21240000	20340000	20340000

TABLE VI: Evaluating the performance of post-quantum secure algorithms in the TLS protocol [11]

size of the generated digital signature in bytes. These metrics provide insights into the computational costs and signature sizes associated with Sha256withRSA key operations.

Table XIII sums up key execution measurements for Dilithium cryptographic frameworks, exhibiting key age, marking, and confirmation processes estimated in 1000 cycles. Also, it gives the size of the produced computerized signature in bytes. The introduced measurements offer a brief outline of computational expenses and mark sizes related with Dilithium key tasks.

V. Conclusion

After a broad assessment of various post-quantum cryptographic computations, with a particular highlight on network based parts, our assessment contemplated that Kyber 512 stands separated as the best choice, basically in light of its striking pace in key age, encryption, and decryption. It meets the NIST security level 1 rules, going with it a lively decision, especially earnest despite the undeniable peril introduced by quantum computers to Web correspondences.

For resource obliged contraptions, similar to those normal in the Trap of Things (IoT), Kyber 512 grandstands immaterial time complexities, conveying it significantly sensible and secure. Regardless, if time complexity is certainly not a fundamental concern, the NTRU variety APR2011 439 fast beats others to the extent that speed while staying aware of NIST security Level 2 rules.

These conclusions start from a social event of results from various examinations inside this space, expressly drove on Raspberry Pi 4 hardware, setting the legitimacy and meaning of our disclosures.

Our survey, zeroed in on the lattice based post-quantum instruments from the US Public Association of Standards standardization process, highlighted finding plans sensible for devices with confined computational resources. Strikingly, we picked varieties with lower security levels that really save a satisfactory level of safety for standard use, restricting the computational load on these devices.

In our assessment, the trade off generally turns around the agreement among security and time viability, unequivocally among Kyber512 and the NTRU Variety APR2011 439 fast. Kyber512 displays prevalent speed, restricting time necessities, however the NTRU variety boasts the main level security among the idea about estimations.

Kyber512's fortitude lies in its adequacy and speed, ensuring expedient cryptographic exercises. Of course, the NTRU Variety APR2011 439 speedy prevails with regards to giving raised wellbeing endeavors, offering generous security for delicate data.

Crypto System	Key Generation (ms)	Encapsulation	Decapsulation
Kyber512	50434455	22324454	21784556
LightSaber	5445674	28624566	27360444

TABLE VII: A Comparative Study of Post-Quantum Cryptosystems for Internet-of-Things Applications [8]"

Kyber Key Parameters	KeyPair (ms)	Encryption (ms)	Decryption (ms)
kyber512	464400	206400	240800
kyber512_aes	567600	206400	137600

TABLE VIII: Kyber Performance Metrics

Key Parameter	KeyPair (ms)	Encryption (ms)	Decryption (ms)
EES1087EP2	3130434	223633	223600
APR2011_439_fast	2233455	120414	51756
APR2011_743_fast	1376045	154800	86756

TABLE IX: Key Parameter Performance Metrics

Key Params	KeyPair (k Cycle)	Encrypt (k Cycle)	Decrypt (k Cycle)	Private Key (Bytes)	Public Key (Bytes)	Plain Text (Bytes)	Cipher (Bytes)
1024	688110	619211	378432	634	162	26	128
2048	3870110	223622	739621	1217	294	26	256

TABLE X: Key Parameter Performance Metrics

Key Params	Key Gen (k Cycle)	Sign (k Cycle)	Verify (k Cycle)	Sign size (Bytes)
falcon_512	28232300	2523200	221100	658

TABLE XI: Falcon Key Parameter Performance Metrics

Key Params	Key Gen (k Cycle)	Sign (k Cycle)	Verify (k Cycle)	Sign size (Bytes)
Sha256RSA	3123400	112800	17200	256

TABLE XII: Key Parameter Performance Metrics for Sha256withRSA

Key Params	Key Gen (1000 Cycle)	Sign (1000 Cycle)	Verify (1000 Cycle)	Sign size (Bytes)
dilithium2	1225400	1423400	751230	2420
dilithium2_aes	1667800	2445600	378400	2420

TABLE XIII: Dilithium Key Parameter Performance Metrics

The choice between these estimations requires a canny idea of the specific necessities: whether improving for faster taking care of times or zeroing in on most outrageous security for the mixed data.

REFERENCES

[1] J. Señor, J. Portilla and G. Mujica, "Analysis of the NTRU Post-Quantum Cryptographic Scheme in Constrained IoT Edge Devices," in IEEE Internet of Things Journal, vol. 9, no. 19, pp. 18778-18790, 1 Oct.1, 2022, doi: 10.1109/JIOT.2022.3162254.

[2] Kumar, Adarsh and Ottaviani, Carlo and Gill, Sukhpal Singh and Buyya, Rajkumar. (2021). Securing the future internet of things with post-quantum cryptography. Security and Privacy. 5. 10.1002/spy2.200.

[3] B. Ravinder Reddy, T. Adilakshmi, "Merkle Tree-based Access Structure for Sensitive Attributes in Patient-Centric Data," International Journal of Engineering Trends and Technology, vol. 70, no. 6, pp. 106-113, 2022. Crossref, https://doi.org/10.14445/22315381/IJETT-V70I6P213

[4] Biswas, Bhaskar & Sendrier, Nicolas. (2008). McEliece Cryptosystem Implementation: Theory and Practice. 47-62. 10.1007/978-3-540-88403-3_4.

[5] Kipnis, A., Patarin, J., Goubin, L. (1999). Unbalanced Oil and Vinegar Signature Schemes. In: Stern, J. (eds) Advances in Cryptology — EUROCRYPT '99. EUROCRYPT 1999. Lecture Notes in Computer Science, vol 1592. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48910-X_15

[6] Pradhan, Pawan & Rakshit, Sayan & Datta, Sujoy. (2019). Lattice Based Cryptography : Its Applications, Areas of Interest & Future Scope. 988-993. 10.1109/ICCMC.2019.8819706.

[7] Althobaiti, Ohood & Dohler, Mischa. (2021). Quantum-Resistant Cryptography for the Internet of Things Based on Location-Based Lattices. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3115087.

[8] Satrya, Gandeva Bayu, Yosafat Marselino Agus, and Adel Ben Mnaouer. 2023. "A Comparative Study of Post-Quantum Cryptographic Algorithm Implementations for Secure and Efficient Energy Systems Monitoring" Electronics 12, no. 18: 3824. https://doi.org/10.3390/electronics12183824

[9] S. P C, K. Jain and P. Krishnan, "Analysis of Post-Quantum Cryptography for Internet of Things," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2022, pp. 387-394, doi: 10.1109/ICICCS53718.2022.9787987.

[10] T. M. Fernández-Caramés, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6457-6480, July 2020, doi: 10.1109/JIOT.2019.2958788.

[11] S. Sarıbaş and S. Tonyalı, "Performance Evaluation of TLS 1.3 Handshake on Resource-Constrained Devices Using NIST's Third Round Post-Quantum Key Encapsulation Mechanisms and Digital Signatures," 2022 7th International Conference on Computer Science and Engineering (UBMK), Diyarbakir, Turkey, 2022, pp. 294-299, doi: 10.1109/UBMK55850.2022.9919545.

[12] Asif, Rameez. 2021. "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms" IoT 2, no. 1: 71-91. https://doi.org/10.3390/iot2010005

[13] O. M. Guillen, T. Pöppelmann, J. M. Bermudo Mera, E. F. Bongenaar, G. Sigl and J. Sepulveda, "Towards post-quantum security for IoT endpoints with NTRU," Design, Automation and Test in Europe Conference and Exhibition (DATE), 2017, Lausanne, Switzerland, 2017, pp. 698-703, doi: 10.23919/DATE.2017.7927079.

[14] Seyhan, K., Nguyen, T.N., Akleylek, S. et al. Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey. Cluster Comput 25, 1729–1748 (2022). https://doi.org/10.1007/s10586-021-03380-7

[15] S. Ebrahimi, S. Bayat-Sarmadi and H. Mosanaei-Boorani, "Post-Quantum Cryptoprocessors Optimized for Edge and Resource-Constrained Devices in IoT," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5500-5507, June 2019, doi: 10.1109/JIOT.2019.2903082.

[16] K. Mayes, "Performance Evaluation and Optimisation for Kyber on the MULTOS IoT Trust-Anchor," 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 2020, pp. 1-8, doi: 10.1109/SmartIoT49966.2020.00010.

[17] R. Ristov and S. Koceski, "Quantum Resilient Public Key Cryptography in Internet of Things," 2023 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2023, pp. 1-4, doi: 10.1109/MECO58584.2023.10154994.

[18] Alessandra Dolmeta, Mattia Mirigaldi, Maurizio Martina, and Guido Masera. 2023. Implementation and integration of Keccak accelerator on RISC-V for CRYSTALS-Kyber. In Proceedings of the 20th ACM International Conference on Computing Frontiers (CF '23). Association for Computing Machinery, New York, NY, USA, 381–382. https://doi.org/10.1145/3587135.3591432

[19] A. Khalid, S. McCarthy, M. O'Neill and W. Liu, "Lattice-based Cryptography for IoT in A Quantum World: Are We Ready?," 2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI), Otranto, Italy, 2019, pp. 194-199, doi: 10.1109/IWASI.2019.8791343.

[20] Habibi, Mohammad Reza, Saeed Golestan, Ali Soltanmanesh, Josep M. Guerrero, and Juan C. Vasquez. 2022. "Power and Energy Applications Based on Quantum Computing: The Possible Potentials of Grover's Algorithm" Electronics 11, no. 18: 2919. https://doi.org/10.3390/electronics11182919

[21] Wong, H.Y. (2024). Shor's Algorithm. In: Introduction to Quantum Computing. Springer, Cham. https://doi.org/10.1007/978-3-031-36985-8-29

[22] Post-Quantum Cryptography. 2021. Available online: https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization