2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI) | 979-8-3503-9523-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICMCSI61536.2024.00027

A Survey on NIST 3rd Round Post Quantum Digital Signature Algorithms

1st Rasha Shajahan
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham
Amritapuri-campus, India
rashajahan2684@gmail.com

2nd Dr. Kurunandan Jain
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham
Amritapuri-campus, India
kurunandanj@am.amrita.edu,

3rd Dr. Prabhakar Krishnan
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham
Amritapuri-campus, India
kprabhakar@am.amrita.edu,

***Abstract*—Currently, digital signature techniques used in public key infrastructure are based on challenges such as discrete logarithms and integer factorization. The introduction of quantum computers poses significant risks to these algorithms, since they may be able to solve the aforementioned problems faster than existing computers. Hostile assaults and security flaws might put the entire Internet's security infrastructure in danger. In the era of quantum computing, protecting digital networking requires adopting a quantum-resistant perspective. One area of cryptography that aims to address the looming security problems that quantum computing is bringing about is post-quantum cryptography (PQC). Its goal is to reduce the risks associated with the current encryption and digital signature technologies. To ensure information security in the era of quantum computing, the NIST is actively involved in standardizing and collaborating on these initiatives. Our survey conducts a study to assess the readiness of post-quantum digital signatures to ensure data security during storage and transport. It also provides an extensive analysis of performance metrics for the 3rd NIST candidates of PQC digital signature algorithms, including key sizes and execution times.**

***Keywords*—Digital Signature, Post-Quantum Cryptography, Post-Quantum Digital Signature**

I. Introduction

For over forty years, traditional cryptographic techniques have been fundamental in ensuring secure communications. These techniques primarily focus on converting plaintext into ciphertext and vice versa for decoding. They fall into two categories: symmetric and asymmetric algorithms, each with unique qualities. Symmetric algorithms, using the same key for both encryption and decryption, are efficient and can process data faster. They bolster their security in a post-quantum environment by employing XOR operations and hash algorithms to mask data analysis. In contrast, asymmetric algorithms rely on robust mathematical functions, notably the complexity of prime factorization, to support their security. However, this dependence on challenging mathematical problems, such as prime factorization, increases processing overhead, slowing down power and modulus computations. The emergence of quantum computers has significantly complicated the field of cryptography. Traditional asymmetric cryptography techniqueslike RSA and Diffie-Hellman, heavily reliant on these mathematical challenges, face severe threats from quantum computing. Quantum computers achieve unparalleled speeds and efficiency by leveraging quantum physics concepts. Particularly concerning are quantum algorithms like Shor's, developed by Peter Shor in 1996 [5], which efficiently factor large numbers,posing a significant risk to classical cryptographic systems such as RSA. Additionally, Grover's Algorithm, capable of accelerating attacks with square root complexity, exacerbates these security challenges. It's crucial to note that all existing asymmetric methods, including RSA, ECC, DH, and DSA, are vulnerable to quantum assaults because they rely on centuries- old mathematical difficulties. This revised version aims to enhance readability and clarity while maintaining the original content's technical aspects.

The escalating threat posed by advancements in quantum computing has spurred a growing interest in Post-Quantum Cryptography (PQC). Utilizing discrete logarithms and integer factorization, PQC aims to safeguard data in scenarios where traditional number-theoretic public-key encryption might fall short. To devise robust cryptosystems capable of resisting attacks from both conventional and potentially quantum computers, PQC explores diverse cryptographic paradigms, suchas lattice-based, multivariate, hash-based, isogeny-based, and code-based cryptography [6].

The transition from classical cryptography to Post-Quantum Cryptography (PQC) presents challenges, notably compatibility issues arising from fundamental algorithmic differences. PQC algorithms, often more computationally intensive, may strain systems with limited processing capabilities. This shift necessitates simultaneous support for both traditional and PQC algorithms, demanding meticulous planning to ensure seam- less interoperability. Managing larger keys in PQC becomes intricate, especially in storage-constrained environments. The migration process incurs costs for software and hardware up- dates, training personnel, and potential disruptions to existing systems. In response to these challenges, our survey evaluates the readiness of post-quantum digital signatures to ensure data security during storage and transmission. It offers a detailed analysis of performance metrics for the third NIST candidates of PQC digital signature algorithms, encompassing key sizes and execution times.

979-8-3503-9523-5/24/$31.00 ©2024 IEEE
DOI 10.1109/ICMCSI61536.2024.00027

II. Digital Signature

Digital signatures, serving as cryptographic methods, effectively emulate traditional handwritten signatures and physical seals used on documents, offering a reliable means to authenticate and preserve the integrity of digital content. The procedure entails creating two different keys; which consist of a private key for exclusive ownership and a matching public key for open sharing. There are two primary stages to this process: verification and signature. During the signing phase, the sender leverages their private key to perform a complex mathematical operation on the data slated for signing. As a result of this process, the original data is added with a distinct digital signature, creating a signed message. During the verification procedure, the public key provided by the sender is used to validate the digital signature's legitimacy. The verification process hinges on identifying a match between the digital signature and the original data, with such alignment confirming the signature's validity, while any discrepancies or signs of data tampering led to a failed verification. This outlines the fundamental process of digital signatures. However, upon closer examination of the digital signature process, it can be categorized into two schemes [2]: an identity scheme and a signature scheme. Both identity and signature schemes primarily serve the purpose of allowing individuals to demonstrate their identity or, in some way, authenticate a message.

Two essential components of an ID-scheme (Identity Scheme) are an interactive protocol and a key-generation method. The algorithm that generates keys is in charge of creating a key pair, which consists of a verification key for User 2 and a signature key for User 1. Equipped with their respective keys, User1 and User2 can engage in a secure interaction through an interactive protocol. The sender acts as the prover, and the receiver acts as the verifier. Consequently, the interactive protocol begins with User 1 (the sender) initiating the process by selecting a random value and transmitting it to User 2 (the receiver). In response, User 2 selects a random challenge and sends it back to User 1. It's important to note that these values are both independent and random. Upon receiving the challenge, User1 employs her signature key and the two random values to execute a specific computation. This computation allows User 1 to demonstrate to User 2 that she possesses the signature key without revealing it. User 2 finalizes the interaction by utilizing his verification key, random values, and User 1's response to assess whether he is convinced that User1 genuinely holds the signature key. User 2's decision, whether to accept or reject User 1's claim, determines the success of identification protocol. This decision signifies the validation of identity establishment or message signing. Within the signature scheme, User 1 employs her signature key and the signature algorithm to sign the message, resulting in the generation of a digital signature. Subsequently, User1 transmits this digital signature to User 2 for verification. Equipped with the verification key obtained from the key generator, User2 utilizes the verification algorithm to ascertain the message's authenticity. Based on the outcome of the verification process, User2 determines the acceptance or rejection of the message, thereby ensuring its reliability and confirming the legitimacy of its source.

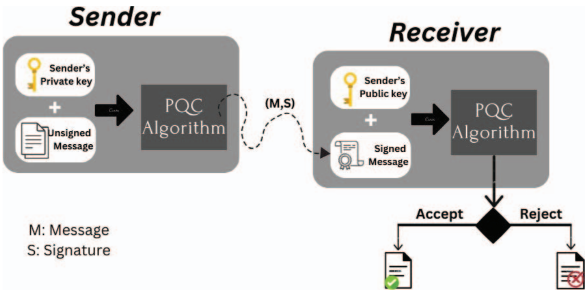

Fig. 1. Digital Signature Process

Digital signatures deliver an array of notable advantages, including authentication, guaranteeing data integrity, enabling non-repudiation, and fortifying security against unauthorized data access or unauthorized modifications. They are extensively applied in securing email communications, facilitating secure financial transactions, validating the legality of con- tracts, and verifying the authenticity of software, among various other applications. In the contemporary digital landscape, digital signatures play an indispensable role in fostering secure and trustworthy digital communication.

III. Vulnerabilities in Current Cryptographic Algorithms

Vulnerabilities in current cryptographic algorithms are a significant and growing concern in our increasingly digitized world. However, it's not just quantum threats that current cryptographic systems contend with. There are also vulnerabilities stemming from implementation flaws, side-channel attacks, and evolving attack techniques in the classical computing realm. Attackers with enough skill could use these flaws to jeopardize the confidentiality of communications and encrypted data. In this section, we will address some of the vulnerabilities encountered in current cryptographic systems.

A. *Shor's Algorithm*

Discrete logarithm calculation and big composite number factoring are two computationally difficult problems for conventional computers. In 1994, mathematician Peter Shor published Shor's technique, a quantum technique that changed the game. This algorithm capitalizes on a fundamental feature of quantum computing called "quantum parallelism," enabling simultaneous operations on multiple inputs. Additionally, its proficiency in finding periods (using Quantum Fourier Transform) efficiently addresses a longstanding challenge faced by classical algorithms when dealing with large numbers [5]. Notably, Shor's Algorithm poses a substantial threat to widely adopted cryptographic systems like RSA and ECC.

B. Grover's Algorithm

In 1996, Lov Grover presented Grover's Algorithm, whose main goal was to make searching unsorted lists or databases more effective than it was with traditional methods. It is not as dangerous as Shor's Algorithm for current encryption techniques, but it is still important for quantum computing. Grover's Algorithm, like Shor's Algorithm, takes advantage of quantum parallelism and provides a quadratic speedup over traditional search methods. With this efficiency, one can search through N items in about N steps, which is a significant improvement over conventional approaches [5]. In addition to its database search application, Grover's Algorithm finds utility in optimizing brute-force attacks on symmetric encryption keys, halving the search space. It's essential to note that while Grover's Algorithm doesn't directly break encryption systems, it has the potential to weaken them by reducing the effective key length.

C. Side-Channel Attack

Side-channel attacks are a substantial risk to conventional cryptography because they take advantage of vulnerabilities in how cryptographic algorithms are physically implemented. These vulnerabilities result in unintended information leaks, which traditional cryptographic methods are not constructed to withstand. By covertly observing physical attributes, like power usage, and electromagnetic radiation, during cryptographic processes, side-channel attacks [7] are executed. By doing this, data security is compromised since attackers can learn the secret keys used for encryption. These attacks are difficult to identify since they use a variety of tactics and are carried out in secret. If they are successful, it could harm cryptographic systems' security and result in data-leaks, or illegal access. To counteract side-channel attacks, countermeasures have been developed, which include designing more secure hardware and software. However, implementing these countermeasures can raise the complexity and cost of cryptographic systems.

D. Simon's Algorithm

Simon's algorithm is a quantum algorithm with a quantum advantage over traditional computing, developed by Daniel Simon in 1994. His technique is well recognized for its lightning-fast speed at which these particular issues may be solved; it achieves this with only $O(n)$ queries to the black-box function, a significant improvement over more conventional approaches. Most importantly, it's critical to realize that the primary goal of Simon's technique is not to compromise traditional encryption systems, which are the primary targets of quantum flaws. Systems that use discrete logarithms or factorization are examples of these.

To defend Post-Quantum Cryptography (PQC) against side-channel attacks and algorithms such as Grover's and Simon's, among others, strategies such as quantum-resistant algorithms, hybrid systems, large key sizes, and parameters, Quantum Key Distribution (QKD) for secure key exchange, secure communication protocols, side-channel attack countermeasures, and constant-time implementations should be used.

IV. Post Quantum Cryptography

The National Institute of Standards and Technology (NIST) has standardized two hash function-based stateful digital signature methods, XMSS (eXtended Merkle Signature Scheme) and LMS (Leighton-Micali Signature), for use in the first phase of PQC. It was temporarily standardized. Also, these schemes were larger and required constant updating of the secret key, making them unsuitable for applications like IoT, where efficiency, scalability, and simplicity are crucial. The organization sought to identify the most suitable long-term standardized algorithm.

Quantum-resistant cryptography, or post-quantum cryptography (PQC), is a subfield of cryptography. PQC is primarily focused on preserving cryptographic security even in the event of potential attacks using quantum computers. Its principal goal is to replace current encryption techniques with algorithms built to withstand quantum computer attacks. PQC is a broad field that includes a variety of mathematical underpinnings and cryptographic techniques, such as multivariate polynomial cryptography, hash-based cryptography, lattice-based cryptography, etc.

A. Lattice-based Cryptography

Lattice-based cryptography is an encryption technique that relies on mathematical constructs known as lattices [2]. Although lattices find applications across different domains, their introduction to cryptography and their essential role can be attributed to the work of Ajtai. His work introduced lattice-based cryptographic systems that pose challenging mathematical problems.

A lattice is a mathematical construct formed by an infinite grid of points in n-dimensional space, creating a regular pattern that extends indefinitely. It can be likened to a collection of points, each characterized by coordinates within the multidimensional space. In the context of cryptography, lattices are typically grids with two or more dimensions. Lattice-based cryptography derives its security from the complexity of specific computational challenges linked to the lattice structures,a few of which are detailed below.

- The Shortest vector problem (SVP): Identify the shortest non-zero vector within a given lattice, which is difficult due to the potential existence of multiple vectors with the same minimal norm.
- The Closest vector problem (CVP): Identify the nearest lattice point to the target vector.
- The Short integer solution (SIS): Identify the non-zero vector that satisfies a system of linear equations within the lattice.
- The Learning with Errors (LWE): The goal is to deduce the unidentified coefficients utilizing a set of equations that might include noise or errors.

The two main components of lattice-based encryption are public keys and secret keys. The lattice structure provides the public key, which is freely distributed, whilst the secret key is only known to the intended recipient and is closely related to the lattice's capacity to solve mathematical puzzles. The strength of lattice-based cryptography lies in its resistance to quantum errors. The inherent complexity of solving mathematical problems based on lattices poses a significant challenge forquantum computers, making it improbable to gain a substantialadvantage in compromising the security provided by lattice- based cryptography. This characteristic positions lattice-based cryptography as a resilient and practical choice for ensuring secure communication in the post-quantum computing era.

B. Hash-based Cryptography

Hash-based cryptography relies on mathematical algorithms called hash functions, which transform input data or messages into fixed-length strings, often in hexadecimal format. These hash functions are optimized for speedy computation and ensure that identical inputs consistently yield the same hash value, offering determinism. In practical terms, this cryptographic approach is commonly employed in digital signatures, where a sender generates a message hash, encrypts it with their private key, and appends it to the message. Recipients, using the sender's public key, can then verify the message with the already-signed message, confirming the message's authenticity and integrity. Beyond these applications, hash-based cryptography is pivotal in various cryptographic protocols, such as HMAC (Hash-based Message Authentication Code), hash chains, and Merkle trees [8]. These protocols playa central role in establishing secure communications and form the foundation of technologies like blockchain.

The two key characteristics of hash functions are pre-image resistance, which makes it computationally challenging to reverse a hash result to expose the original input, and collision resistance, which makes it difficult to identify two separate inputs that give the same hash value. When combined, these features increase the security and dependability of hash-based cryptographic applications.

C. Multivariate polynomial Cryptography

The complex mathematical characteristics of multivariate polynomials are used for security in multivariate polynomial cryptography, a subset of public-key cryptography. Inthis cryptographic approach, the public key adopts the formof a multivariate polynomial function, while the private key remains confidential, holding the decryption authority. This method displays significant robustness against quantum threats, positioning it as a promising choice for PQC in safeguarding digital communication amidst the era of quantum computing. However, it is crucial to acknowledge the computational demands and intricate key management linked to multivariate polynomials. The system's security depends onits ability to solve polynomial equations, which is still difficultfor even the fastest computers.

V. NIST PQC STANDARDIZATION

The NIST PQC Standardization aims to establish standardized cryptographic methods resilient to quantum computing vulnerabilities. It covers a wide range of cryptographic techniques, including secure hash functions, asymmetric key encryption, digital signatures, and key exchange. The study has progressed through several phases, such as requesting algorithm submissions, holding public reviews, and going through demanding evaluation cycles. The study has re- received cryptographic algorithm proposals from worldwide researchers and organizations and actively promotes participation and feedback from the cryptographic community, industry, academia, and the general public to enhance its standardizationendeavors.

NIST received 82 submissions in total as a reaction to the public call for PQC standardization recommendations. Only 69 of these submissions fulfilled minimal requirements. In December 2017, the PQC standardization effort commenced its first phase, during which 26 candidate algorithms were chosen for additional assessment [9]. The secondround of the study started in January 2019 and, as the number of candidate algorithms dropped, 15 algorithms were ultimately chosen to go to the third round. Out of these fifteen algorithms, eightare classified as alternate candidates, and the other seven are finalist candidates. Among the fifteen candidate algorithms, three digital signature techniques and four public-key encryption/KEM processes are among the finalist options. In a similarvein, the eight alternate potential algorithms consist of three digital signature systems and five public-key encryption/KEM processes. NIST has selected a number of these candidates, some of which are noteworthy: four of the third-round candidates (CRYSTALS–KYBER, CRYSTALS–Dilithium, FAL-CON, and SPHINCS+) have been selected for standardization, and four more (BIKE, Classic McEliece, HQC, and SIKE) have been advanced to a fourth round for more thoroughreview and consideration.

A. NIST Security Levels

NIST acknowledges the challenges in assessing post-quantum cryptography systems' security throughout the standardization process, considering the potential for quantum algorithm advancements and the challenges in predicting the performance of quantum computers in the future. NIST suggests a classification scheme that complies with established NIST criteria in terms of computational resources and is basedon the security levels of reference primitives. The suggested categories are key search on a 128-bit block cipher and collision search on a 384-bit hash function. Circuit size is the unit of measurement for quantum attacks, and submitter is urged to classify their initial findings conservatively. Higher- category parameter sets automatically meet lower-categorystandards. NIST advises concentrating on categories 1, 2, and/or 3 for adequate security and utilizing at least one higher-security parameter set.

TABLE 1 provides estimates of computational resources required for quantum and classical attacks on cryptographic

TABLE I
COMPUTATIONAL RESOURCE ESTIMATIONS FOR SECURITY-LEVEL ATTACKS ON CRYPTOGRAPHIC ALGORITHMS USING CLASSICAL AND QUANTUM TECHNIQUES

NIST Security Levels	**Classical Gate Counts**	**Quantum Gate Counts (Circuit Size)**
1	AES 128	2^{170}/MAXDEPTH quantum gates or 2^{143} classical gates
2	SHA3-256	2^{146} classical gates
3	AES192	2^{233}/MAXDEPTH quantum gates or 2^{207} classical gates
4	SHA3-384	2^{210} classical gates
5	AES256	2^{298}/MAXDEPTH quantum gates or 2^{272} classical gates

TABLE II
THIRD-ROUND CANDIDATES FOR POST-QUANTUM DIGITAL SIGNATURES SELECTED BY NIST

	3rd round NIST status	**4th phase NIST Status**	**Security Level**	**Scheme**
Dilithium	Finalist	Standardized	1, 2, 3	Lattice-based
Falcon	Finalist	Standardized	1, 5	Lattice-based
Rainbow	Finalist	Not selected	1, 3, 5	Multivariate
GeMSS	Alternative	Not selected	1, 3, 5	Multivariate
Picnic	Alternative	Not selected	1,3,5	Hash-based
SPHINCS+	Alternative	Standardized	1,3,5	Hash-based

algorithms, specifically AES (Advanced-Encryption Standard) and SHA-3 (Secure-Hash-Algorithm 3). Estimates are given in terms of gate counts, where the quantum gate counts are presented as a function of a parameter called MAXDEPTH, representing a limit on the circuit depth for quantum attacks. The classical gate counts represent the estimated computational resources needed for classical attacks. The security categories based on these estimates offer a higher level of quantum security than a basic analysis might suggest.

VI. 3RD ROUND POST-QUANTUM DIGITAL SIGNATURE ALGORITHMS

The Third Round of Post Quantum Digital Signature Candidates will be examined in this section as part of the NIST effort to standardize PQC (Post-Quantum Cryptography). Table II provides a thorough summary of a few chosen cryptographic algorithms together with their current Third Round standings. Dilithium, Falcon, and Rainbow are the front-runners; GeMSS, Picnic, and SPHINCS+ are backup choices. NIST's main goal is to standardize digital signature methods so that they can withstand adaptively selected message attacks and be existentially unforgeable (also known as EUF-CMA security). Each algorithm's cryptographic schemes which include hash-based, multivariate, and lattice-based cryptography—as well as the corresponding security levels are displayed in TABLE II. Interestingly, a higher security level that the algorithm provides is correlated with a higher security level.

A. CRYSTALS-Dilithium

Building on the concepts of Short Integer Solution (SIS) and Learning with Errors (LWE) issues, Dilithium is a notable lattice-based digital signature system. Dilithium, which is optimized for different NIST security levels 1, 2, and 3, is one of the main components of the NIST Post-Quantum Cryptography (PQC) competition submission for the Cryptography Suite for Algebraic Lattices (CRYSTALS). The system enhances traditional cryptographic methods by adopting Fiat- Shamir with aborts, focusing on optimizing public key size and employing advanced techniques in public key generation. Its key generation involves sampling a secret key from a specific distribution and then deriving the corresponding public key. The public key is generated based on the secret key and is used for signature verification. Dilithium introduces innovative functions like Expand-A, CRH, and ExpandMask, effectively reducing key and signature sizes compared to other systems, albeit still larger than traditional systems like RSA and ECC. Its notable security measures make it resilient against potential side-channel attacks, aligning with the efficiency standards of advanced lattice-based signature schemes. Despite computational costs, Dilithium showcases, efficiency improvements, addressing the theoretical threat of quantum computers.

Furthermore, Dilithium's meticulous design extends to robust security measures, particularly guarding against potential side-channel attacks and ensuring the utmost protection of sensitive data. The system excels in aligning with the efficiency standards of current advanced lattice-based signature schemes, showcasing standout characteristics in terms of robust security, especially concerning Strong Unforgeability under Chosen Message Attacks (SUF-CMA). While its reduction may not be categorized as tight, Dilithium stands out as a compelling choice in the realm of PQC. Moreover, [17] emphasizes how a tiny hardware accelerator for the CRYSTALS-Dilithium digital signature technique was implemented, showing how flexible the system is to fit into the smallest Zynq FPGA with the least amount of resources used. the fewest resources that are feasible.

.

B. Falcon

"Fast Fourier Lattice-based Compact signatures Over NTRU lattices," or FALCON for short, is a PQC digital signature algorithm designed around NTRU principles. Its core objective is to minimize public key and signature sizes, facilitating the transition to post-quantum cryptographic approaches. Working inside the GPV (Gentry-Peikert-Vaikuntanathan) framework, FALCON uses a Fast Fourier trapdoor sampler that is based on earlier work by Ducas and Prest, together with NTRU lattices. By solving the difficult Short Integer Solution problem (SIS) across NTRU lattices, the algorithm provides a high level of security (SUF-CMA) in both the Random Oracle Model and the Quantum Random Oracle Model. FALCON comes in three different flavors, each with its own specs and features. The key creation entails taking a sample of a secret key and producing the matching public key. After that, the public key is employed to confirm the signature. Falcon is renowned for emphasizing smaller keys without sacrificing security. Notably, FALCON's key and signature generation processes

TABLE III
Security Parameters of CRYSTALS-Dilithium

Parameters	Description
Parameter q	Modulus used in the construction of the lattice
Parameter d	Weight of the secret key
Parameter c	Weight of the error term
Parameter $\gamma 1$	Derived from prime modulus q [(q-1)/16]
Parameter $\gamma 2$	Half the value of $\gamma 1$
Parameter (k, l)	Number of modules for polynomial coefficients
Parameter η	Bit length of the nonces
Parameter β	Bit length of the secret key
Parameter ω	Maximum number of ring elements in the secret key
Signature size	Length of the signature key
Public key size	Length of public key
Private key size	Length of the private key

TABLE IV
Parameter set of CRYSTALS-Dilithium [4]

Security Levels	–	1	2	3
Parameter q	8380417	8380417	8380417	8380417
Parameter d	14	14	14	14
Parameter c	60	60	60	60
Parameter $\gamma 1$	523776	523776	523776	523776
Parameter $\gamma 2$	261888	261888	261888	261888
Parameter (k, l)	(3,2)	(4,3)	(5,4)	(6,5)
Parameter η	7	6	5	3
Parameter β	375	325	275	175
Parameter ω	64	80	96	120
Signature size (bytes)	1387	2044	2701	3366
Public key size (bytes)	896	1184	1472	1760
Private key size (bytes)	2081	2733	3348	3916

are nondeterministic, providing probabilistic outcomes, while the signature verification process is deterministic, adhering to fixed validation rules.

The cryptographic parts of FALCON perform as follows: their minimum clock period is 32.434 ns, and their maximum frequency is about 30 MHz [4]. While having a similar area overhead for signature verification, FALCON-1024 and FALCON-512 show different delays. Because of its decreased latency, FALCON-512 is recommended for speedier implementations. While loop pipelining results in a longer clock period than the baseline and loop-unrolled architectures, it improves latency by approximately 22% without adding extra memory or area expenses.

C. Rainbow

Rainbow stands as a robust digital signature scheme classified under the multivariate polynomial umbrella, distinguished for its capacity to fend off potential quantum threats. What sets Rainbow apart is its multi-layer structure, incorporating multiple strata of multivariate polynomial equations, rendering it notably resilient against an array of cryptographic attacks. Beyond its security attributes, Rainbow also strikes an essential balance between security and computational efficiency. This equilibrium translates into a practical means of generating and verifying digital signatures, offering a viable solution for real- world applications.

The Unbalanced Oil and Vinegar (UOV) scheme [14] serves as the foundation for Rainbow, a signature system that enhances security by constructing a tiered Oil and Vinegar structure. It is available in three versions (compressed, cyclic, and classic) for different security levels and achieves EUF-CMA security with specific modifications. The key generation involves choosing random coefficients for multivariate polynomials, constructing an equation system, and solving it. The shift to Post-Quantum Cryptography (PQC) is not without its difficulties, such as the unpredictability of quantum computing paths and the difficulties associated with technology adoption. According to the security levels of reference primitives, NIST suggests a classification scheme that gives priority to categories 1, 2, and/or 3 for adequate security.

D. GeMSS

Multivariate Quadratic Public-Key Cryptosystem (MPKC) provides a quantum-resistant solution for digital signatures; one example is the HFEv-class studied in [3].In GeMSS, the key generation process involves creating a tree structure. While the private key is constructed using the tree's structure, the public key is produced using the hash values of the nodes in the tree. The MPKC's Great Multivariate Signature Scheme (GeMSS), which actively participates in the NIST PQC Standardisation process, is built on the HFEv-class.HFEv-, which is based on Patarin's HFE system, extends the central map F by substituting modifiers such as Vinegar (v) and Minus (-) for monomials to improve security and trapdoor efficiency. Based on HFEv-, the robust quantum-resistant digital signature system known as GeMSS has garnered significant research support for more than twenty years. The inversion of the fundamental polynomial equation still creates a computational barrier even with the increased security and performance. Unlike the QUARTZ system, these issues are successfully handled. In a quantum setting, GeMSS functions well, despite certain drawbacks including huge key sizes and slow key pair and signature creation.

TABLE V
Security Parameters of Falcon

Parameters	Description
Parameter n	Dimension of polynomial ring
Parameter ϕ	Defines the characteristics of the problem space
Parameter q	Prime number
Parameter β^2	Control the distribution of errors
Signature size	Length of the signature key
Public key size	Length of public key

TABLE VI
Parameter set of Falcon [4]

FALCON Variants	FALCON-512	FALCON-768	FALCON-1024
NIST security-level	1	2-3	4-5
Parameter n	512	768	1024
Parameter ϕ	$x^n + 1$	$x^n - x^{n/2} + 1$	$x^n + 1$
Parameter q	12289	18433	12289
Parameter β^2	43533782	100464491	87067565
Signature size (bytes)	657.38	993.91	1273.31
Public key size (bytes)	897	1441	1793

TABLE VII
SECURITY PARAMETERS OF RAINBOW

Parameters	Description
Parameter F	Finite field.
Parameter (v1, o1, o2)	Constant integer values
Signature size	Signature key length
Public key size	Length of public key
Private key size	Length of private key

TABLE VIII
PARAMETER SET OF RAINBOW

Rainbow Variants	Ia_Classic	IIIc_Classic	Vc_Classic
Security Levels	1	3	5
Parameter F	GF(16)	GF(256)	GF(256)
Parameter v	32	68	92
Parameter o1	32	36	48
Parameter o2	32	36	48
Signature size (bytes)	64	156	204
Public key size (kB)	149	710	1705.5
Private key size (kB)	93	511.4	1227.1

TABLE IX
PARAMETER SET OF GEMSS

GeMSS Variants	GeMSS-128	GeMSS-192	GeMSS-256
Key-pair Generation (ms)	42	166	424
Signing time (ms)	260	694	1090
Verification time (μs)	41	117	336
Public key size (bytes)	417408	1304192	3603792
Private key size (bytes)	14208	39440	82056
Signature size (bytes)	48	88	104

E. Picnic

Picnic, designed as a post-quantum digital signature system, stands out for its innovative use of zero-knowledge proof of system employing structured reference strings (SRS). This mathematical construct contributes to reducing the signature size and enhancing operational efficiency, making Picnic well-suited for diverse practical applications, particularly in environments with limited computational resources. The system excels in delivering robust security without imposing excessive computational burdens, offering a promising solution for the challenges posed by post-quantum computing.

Post-quantum, Unforgeable, and Indistinguishable Signatures with Classically Efficient Proofs, or "Picnic," distinguishes itself as a third-round candidate. Its ability to combine security and conventional processing performance allows itto flourish in a post-quantum world. Picnic provides non-interactive proofs of knowledge with zero knowledge by utilizing symmetric key primitives and the MPC in the head paradigm. To generate a secret key in Picnic, one just creates one at random and uses it to get the public key. The public key is computed using the hash functions and the secret key. The main element of the signature technique is the secret key that is linked to a block cipher and is used to encrypt a public plaintext block into a public ciphertext block, which eventually becomes the public key. Picnic's versatility stems from its ability to let users select internal blocks and parameters. However, this flexibility also makes it difficult to make the best decisions possible because it affects several variables that vary depending on the implementation, such as the code size, security level, time taken to create and verify signatures, and size of the signatures and keys. The research [4] delves into the subtleties of the Picnic FPGA component's performance and offers an understanding of its operational characteristics. These components run at a maximum frequency of 120 MHz with a clock period of 8.36 ns, and they feature hierarchically specified area overhead and execution latency. It's interesting to note that key generation, along with signature generation and verification, turns out to be the most efficient process. An overview of Picnic's performance features may be obtained by considering the substantial impact optimization techniques such as loop unrolling and loop pipelining have on latency and area overhead.

F. SPHINCS+

Cryptographic signature systems SPHINCS [15] and SPHINCS+ [15] are made for post-quantum computing security. Hash-based SPHINCS+, which offers strong security, including EUF-CMA, was entered into the NIST competition. Its cautious methodology, however, leads to higher signature sizes and slower cryptographic processes. SPHINCS+ key creation isbased on tree topologies and hash functions. The public keyis obtained using the hash values of the nodes in a tree, and the private key is generated randomly. Importantly, it remains resilient against collision attacks on the hash function, whichis a crucial element in its security. The resource requirements and execution times of SPHINCS+ components vary in terms of performance which can be analyzed from Table XIII [4].

Security is based on the notion that the tweakable hash functions' pseudorandom function (PRF) can be regarded as a random oracle, and it is based on, the use of standard function families. The highest security level, level 5, increases latency but consumes the most resources. The choice of security level should be based on specific performance and security requirements, with levels 1 and 3 being more suitable for speed.

VII. DISCUSSION

The NIST standardization process's third phase has identified six candidates for Post-Quantum Cryptography (PQC) digital signatures, categorized into Lattice-based, Multi- variate Polynomial-based, and Hash-based groups. Notably, Dilithium, within the Lattice-based category, stands out as the most secure option, with its resilience tied to the dimensionality of each lattice. This distinctive feature enhances security and distinguishes it from other cryptographic algorithms, emphasizing its robustness in the evolving land- scape of post-quantum security. A comprehensive comparison of PQC algorithms reveals notable trade-offs and strengths. In the realm of lattice-based Digital Signature Algorithms, CRYSTALS-Dilithium excels in security, surpassing Falcon in key size reduction. Falcon, characterized by larger public and signature keys, demonstrates superior signing and verification speed. Dilithium 2 exhibits swift handshake performance,

TABLE X
Parameter Set for Picnic

Picnic Variants	picnic-L1-FS	picnic-L1-UR	picnic2-L1-FS	picnic-L3-FS	picnic-L3-UR	picnic2-L3-FS	picnic-L5-FS	picnic-L5-UR	picnic2-L5-FS
Security levels	1	1	1	3	3	3	5	5	5
Parameter S	128	128	128	192	192	192	256	256	256
Parameter n	128	128	128	192	192	192	256	256	256
Parameter s	10	10	10	10	10	10	10	10	10
Parameter r	20	20	20	30	30	30	38	38	38
Parameter H	256	256	256	384	384	384	512	512	512
Parameter T	219	219	343	329	329	570	438	438	803
Parameter u	-	-	27	-	-	39	-	-	50
Signature size (bytes)	34032	53961	13802	76772	121845	29750	132856	209506	54732
Public key size (bytes)	32	32	32	48	48	48	64	64	64
Private key size (bytes)	16	16	16	24	24	24	32	32	32

TABLE XI
Security Parameters of Picnic

Parameters	Description
Parameter S	Number of bytes in the secret key
Parameter n	Dimension of the problem
Parameter s	Constant parameter value
Parameter r	Number of rounds in the scheme
Parameter H	Output size of hash function
Parameter T	Number of tree levels
Parameter u	Security level variation parameter
Signature size	Length of the signature key
Public key size	Length of public key
Private key size	Length of private key

TABLE XII
Security Parameters of SPHINCS+

Parameters	Description
Parameter n	Size of the hash function output
Parameter h	Height of the hypertree structure
Parameter d	Number of layers in the hypertree
Parameter log t	Number of iterations in the WOTS+ (Winternitz One-Time Signature scheme)
Parameter k	Number of subtrees in the hypertree
Parameter w	Number of Winternitz parameter sets in the WOTS+ scheme
Signature key size	Length of the signature key
Public key size	Length of the public key
Private key size	Length of the private key

TABLE XIII
Parameter set for SPHINCS+

SPHINCS+ Variants	SPHINCS+-128f	SPHINCS+-128s	SPHINCS+-192f	SPHINCS+-192s	SPHINCS+-256f	SPHINCS+-256s
Security levels	1	1	3	3	5	5
Parameter n	16	16	24	24	32	32
Parameter h	60	64	66	64	68	64
Parameter d	20	8	22	8	17	8
Parameter log t	9	15	8	16	10	14
Parameter k	30	10	33	14	20	22
Parameter w	16	16	16	16	16	16
Signature size (bytes)	16976	8080	35664	17064	49216	29792
Public key size (bytes)	64	64	96	96	128	128
Private key size (bytes)	32	32	48	48	64	64

while Falcon 512 impresses with a compact certificate size, positioning Dilithium as the preferred choice for specific applications. Shifting to multivariate-based signatures, Rainbow and GeMSS showcase efficiency but face TLS implementation challenges due to larger certificate sizes. Rainbow, with sizable keys, experiences key generation latency, whereas GeMSS excels in rapid verification and compact signatures. However, GeMSS encounters difficulties in low-end device implementation, making Rainbow more suitable for such contexts. In the domain of Hash-based signatures, Picnic offers flexibility, impacting signature creation time, verification time, and code size, featuring smaller public keys and larger signature keys. Conversely, SPHINCS+ proves ideal for secure messaging, supporting message recovery, and utilizing a tree-based publickey structure.

The transition from current cryptographic practices to post-quantum cryptography poses significant challenges due to the algorithms' demands for large key sizes, substantial memory, and computational power. Furthermore, post-quantum cryptography is currently not equally understood as widely-established algorithms, which emphasizes a revolutionary nature and signifies a significant divergence from traditional cryptographic techniques. Carefully examining three essential features is necessary to ascertain whether digital signatures are quantum in nature. This includes using quantum algorithms such as Shor's or Grover's, depending on cryptographic protocols that are immune to quantum errors, and using quantum hardware or simulators for the formation and validation of signatures a departure from conventional cryptography methods. In the absence of quantum computers, researchers usually use liboqs, an open-source multi-platform that makes it easier to construct quantum algorithms. In an experiment described in [9], the configuration was installed on a virtual machine with six processor cores and 6GB of RAM.

TABLE XIV
FEASIBILITY MATRIX OF 6 POST-QUANTUM DIGITAL SIGNATURE ALGORITHM AGAINST 14 REAL-WORLD APPLICATIONS

Applications	Dilitium	Falcon	Rainbov	GeMSS	Picnic	SPHINCS+
3SKey	9	8	7	4	8	7
EMV-SDA	8	9	9	8	10	8
EMV-DDA	5	4	7	4	8	7
CA Key	12	12	11	8	12	10
ICAO 9303	10	10	9	8	10	8
GSM eSIM	9	10	7	4	8	7
TLS Server	12	10	12	8	10	10
TLS Client	12	12	11	8	10	8
Bitcoin	12	11	11	7	8	6
FIDO	9	8	5	4	8	6
S/MIME	12	12	12	10	12	12
PDF-AES	12	12	11	8	12	10
PDF-QES	9	8	7	4	8	7
Code-Sign	12	12	11	10	12	10

VIII. CONCLUSION

The authentication method possesses distinctive features, highlighting the significance of making optimal choices tailored to specific implementation requirements. Effectively ad- dressing the complexity inherent in quantum digital signaturesrequires thorough optimization of these algorithms, with a focus on minimizing necessary qubits, gates, and operation counts for heightened efficiency. The reliability of quantum signatures depends on advancements in error correction methods within the evolving realm of post-quantum cryptography. The exploration of hybrid quantum-classical systems, where specific tasks are delegated to classical processors, holds promise for reducing overall computational burdens and enhancing efficiency. It is noteworthy that, although this study currently lacks implemented algorithms, this is anticipated to change in the future. As for future work, we can concentrate on the standard PQC digital signature algorithms (Dilithium, Falcon, and SPHINCS+), which are expected to be the subjectof in-depth investigations into side-channel attack mitigation, scalability, optimization, quantum-secure hybrid systems, security analysis, and real-world implementations. The optimization of post-quantum cryptography systems entails strategic considerations in a broader context, encompassing the enhancement of quantum algorithms for increased efficiency, ensuring qubit stability, and exploring hybrid systems thatharness the strengths of both quantum and classical methods, ultimately facilitating quicker and more secure signature pro- duction.

REFERENCES

[1] Beckwith, L., Nguyen, D.T. and Gaj, K., 2023. Hardware Accelerators for Digital Signature Algorithms Dilithium and FALCON. IEEE Design Test.

[2] Johansen, K.F., 2021. Dilithium, a Quantum Safe Signature (Master's thesis, NTNU).

[3] Reis, P.R. and Borges, F., 2019, September. Digital Signatures in a Quantum World: Evaluating The Trade-off Between Performance and Security for GeMSS. In Anais do V Workshop de Regulação, Avaliação da Conformidade e Certificação de Segurança (pp. 23-32). SBC.

[4] Soni, D., Basu, K., Nabeel, M., Aaraj, N., Manzano, M. and Karri, R., 2021. Hardware architectures for post-quantum digital signature schemes. Springer.

[5] Ugwuishiwu, C.H., Orji, U.E., Ugwu, C.I. and Asogwa, C.N., 2020. An overview of quantum cryptography and shor's algorithm. Int. J. Adv. Trends Comput. Sci. Eng, 9(5).

[6] Bavdekar, R., Chopde, E.J., Bhatia, A., Tiwari, K. and Daniel, S.J., 2022. Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. arXiv preprint arXiv:2202.02826.

[7] Zeydan, E., Turk, Y., Aksoy, B. and Ozturk, S.B., 2022, February. Recent advances in post-quantum cryptography for networks: A survey. In 2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ) (pp. 1-8). IEEE.

[8] Kampanakis, P. and Sikeridis, D., 2019, November. Two post-quantum signature use-cases: Non-issues, challenges and potential solutions. In Proceedings of the 7th ETSI/IQC Quantum Safe Cryptography Workshop, Seattle, WA, USA (Vol. 3).

[9] Raavi, M., Wuthier, S., Chandramouli, P., Balytskyi, Y., Zhou, X. and Chang, S.Y., 2021, June. Security comparisons and performance analyses of post-quantum signature algorithms. In International Conference on Applied Cryptography and Network Security (pp. 424-447). Cham: Springer International Publishing.

[10] Alagic, G., Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.K., Miller, C., Moody, D., Peralta, R. and Perlner, R., 2019. Status report on the first round of the NIST post-quantum cryptography standardization process.

[11] Kales, D. and Zaverucha, G., 2020. Improving the performance of the picnic signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.154-188.

[12] Casanova, A., Faugere, J.C., Macario-Rat, G., Patarin, J., Perret, L. and Ryckeghem, J., 2017. GeMSS: a great multivariate short signature (Doctoral dissertation, UPMC-Paris 6 Sorbonne Universités; INRIA Paris Research Centre, MAMBA Team, F-75012, Paris, France; LIP6-Laboratoire d'Informatique de Paris 6).

[13] Petzoldt, A., Bulygin, S. and Buchmann, J., 2010. Selecting parameters for the rainbow signature scheme-extended version. Cryptology ePrint Archive.

[14] Beullens, W., 2021, June. Improved cryptanalysis of UOV and rainbow. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 348-373). Cham: Springer International Publishing.

[15] Sim, M., Eum, S., Song, G., Kwon, H., Jang, K., Kim, H., Kim, H., Yang, Y., Kim, W., Lee, W.K. and Seo, H., 2022. K-XMSS and K-SPHINCS $^{+}$: Hash based Signatures with Korean Cryptography Algorithms. Cryptology ePrint Archive.

[16] Tan, T.G., Szalachowski, P. and Zhou, J., 2022. Challenges of post-quantum digital signing in real-world applications: a survey. International Journal of Information Security, 21(4), pp.937-952.

[17] Gupta, N., Jati, A., Chattopadhyay, A. and Jha, G., 2023. Lightweight Hardware Accelerator for Post-Quantum Digital Signature CRYSTALS-Dilithium. IEEE Transactions on Circuits and Systems I: Regular Papers.

[18] Hasija, T., Ramkumar, K.R., Kaur, A., Mittal, S. and Singh, B., 2022, June. A Survey on NIST Selected Third Round Candidates for Post Quantum Cryptography. In 2022 7th International Conference on Communication and Electronics Systems (ICCES) (pp. 737-743). IEEE.

[19] Santini, P., Baldi, M. and Chiaraluce, F., 2019, July. Cryptanalysis of a one-time code-based digital signature scheme. In 2019 IEEE International Symposium on Information Theory (ISIT) (pp. 2594-2598). IEEE.

[20] Shim, K.A., Lee, S. and Koo, N., 2022. Efficient Implementations of Rainbow and UOV using AVX2. IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.245-269.