A Systematic Survey of Post-Quantum Cryptography Algorithms and Security Models

P. Vamshi Krishna[1*], Meeravali Shaik[2]
[1]Research Scholar, Department of Computer Science and Engineering, School of Engineering, Malla Reddy University, Hyderabad, Telangana, India
[2]Professor & Head, Department of Computer Science and Engineering, School of Engineering, Malla Reddy University, Hyderabad, Telangana, India
*Corresponding author: P. Vamshi Krishna

Abstract
The rapid advancement of quantum computing poses a significant threat to traditional cryptographic algorithms, necessitating the development of robust security solutions under the realm of Post-Quantum Cryptography (PQC). This survey provides a comprehensive analysis of the state-of-the-art PQC algorithms, emphasizing their potential to safeguard information in a post-quantum world. It delves into various classes of PQC algorithms, including lattice-based, code-based, multivariate polynomial, hash-based, and isogeny-based cryptographic schemes. Each category is critically evaluated in terms of its security strengths, computational efficiency, key sizes, and resilience to quantum attacks. The survey also discusses the challenges of implementing PQC algorithms, such as their integration into existing systems, scalability, and performance overheads. Moreover, it highlights the ongoing standardization efforts by organizations like NIST and the practical considerations for transitioning from classical to quantum-resistant cryptographic protocols. The article concludes by identifying future research directions that address the current limitations and explore innovative approaches to enhancing the security, efficiency, and adaptability of PQC algorithms, ensuring the longevity and reliability of cryptographic systems in the quantum era.

Keywords: Post-Quantum Cryptography, Quantum-Resistant Algorithms, Lattice-Based Cryptography, Isogeny-Based Cryptography, Code-Based Cryptography, Multivariate Cryptography, Hash-Based Signatures
DOI Number: 10.48047/nq.2024.22.3.NQ24036 **NeuroQuantology 2024; 22(03): 324-339**

1. Introduction

The first communication requirement is to ensure transmission quality, evaluated by the bit error rate. In addition, the need for information security for users, ensuring the integrity of information, or the ability to resist attacks to falsify or steal information is also a highly demanding essential requirement [1]. Moreover, the advent of the concept of quantum computers and quantum algorithms, such as Shor's algorithm, threatens to collapse cryptography based on mathematical difficulties. Therefore, researchers have embarked on research and testing of cryptographic algorithms to resist attacks by quantum computers in the future.

A quantum computer is a type of computer that uses the principles of quantum mechanics to perform calculations. Unlike classical computers, which use bits that can be either 0 or 1, quantum computers use quantum bits or qubits, which can be in multiple states simultaneously. This property of qubits allows quantum computers to

perform certain types of calculations much faster[2]. For instance, quantum computers can solve specific mathematical problems that are computationally infeasible for classical computers, such as factoring large integers. Quantum computers are still at an experimental stage and are not yet widely available[3]. However, significant progress in recent years has been made in building prototypes and demonstrating their potential capabilities. They can revolutionize many fields, from cryptography to optimization and machine learning. However, there are also significant technical and practical challenges to address before quantum computers perform useful computations at scale.

PQC refers to cryptographic algorithms designed to be secure against attacks by quantum computers. Quantum computers have the potential to break many of the cryptographic protocols that are currently in use, including those that are widely used to secure Internet communications. PQC aims to develop new cryptographic protocols that can resist such attacks. The threat posed by quantum computers arises from their ability to perform specific calculations much faster than classical computers. Specifically, quantum computers can solve specific mathematical problems that are computationally infeasible for classical computers[4]. One example is factoring large integers, the basis for many current cryptographic protocols. Post-quantum cryptography is an active area of research and development, with many different proposals for new cryptographic algorithms evaluated for their security and practicality. The goal is to develop algorithms that can replace existing cryptographic protocols, ensuring the long-term safety of sensitive information[5]. People need to pay attention to PQC while the large-scale quantum computer is still far from reality. A few reasons can be listed here. (1) Preparation: Developing PQC algorithms allows us to prepare for the future threat of quantum computers. Cryptographic systems are often used to protect data for long periods, so it is essential to start planning for the possibility of quantum-based attacks now. (2) Longevity: PQC algorithms are designed to secure against classical and quantum-based attacks[6]. This means they will remain secure even if classical computing power continues to increase. (3) Adoption: it takes time for cryptographic systems to be developed, tested, and adopted. By starting work on PQC algorithms now, we can ensure that there will be suitable replacements for current cryptographic systems when needed.

The first significant work on PQC started in the late 1990s. At that time, mathematicians and computer scientists realized that quantum computers could break widely used cryptographic systems such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC), which rely on mathematical problems that can be solved efficiently by a quantum computer[7]. The discovery of this threat led to a renewed interest in developing cryptographic algorithms that would resist quantum-based attacks. One of the earliest PQC algorithms proposed was the McEliece cryptosystem. It was introduced in 1978 by Robert McEliece and is based on the theory of error-correcting codes. The McEliece cryptosystem is known for its resistance to quantum-based attacks, but it has yet to see widespread adoption due to its large key sizes. Another approach to PQC is lattice-based cryptography. This involves using lattices, which are mathematical structures that can be used to generate encryption keys.

Figure 1 outlines the timeline and selection process of the Post-Quantum Cryptography (PQC) standardization effort led by NIST, divided into four rounds. The first round, from December 2016 to January 2019, saw 82 submissions, with 69 valid candidates, out of which 26 were selected based on their strengths and weaknesses. The second round, spanning January 2019 to July 2020, further narrowed down the candidates to 26, selecting 7 primary and 8 alternate algorithms while evaluating their software and hardware implementations. In the third round, from July 2020 to November 2022, 7 candidates were considered, comprising 4 Public Key Encryption/Key Encapsulation Mechanisms (PKE/KEM) and 3 digital signatures. From these, 1 PKE/KEM and 3 signatures were selected, with 4 candidates advancing to the

fourth round. The fourth round, starting in November 2022 and ongoing, focuses on the remaining 4 PKE/KEM candidates, including BIKE, Classic McEliece, and HQC, with additional scrutiny following published attacks on SIKE.

Figure 1. PQC the standardization process of NIST.

2. PQC Classification

Figure 2 categorizes various PQC methods into five primary groups: Isogeny, Codes, Lattices, Multivariate, and Hash. Each category represents a distinct approach to achieving quantum-resistant security.Each of these PQC methods has its own set of strengths and weaknesses, reflecting the ongoing efforts to find the most secure and practical solutions in the face of advancing quantum computing capabilities. The current landscape of PQC research is dynamic, with continuous evaluation and development needed to ensure these methods can meet the future demands of secure communications.

2.1 Isogeny-based Cryptography:

Isogeny-based methods[8] rely on the mathematical properties of elliptic curves, specifically isogenies between them. Supersingular Isogeny Key Encapsulation (SIKE) is the most prominent isogeny-based scheme, known for its small key sizes, making it suitable for low-bandwidth environments. However, it has recently faced challenges due to emerging attacks, raising concerns about its long-term viability.Isogeny-based cryptography is grounded in the mathematics of elliptic curve isogenies. SIKE represents this category and is based on the difficulty of finding isogenies between supersingular elliptic curves. SIKE is particularly attractive because of its small key sizes, which are a significant advantage in bandwidth-constrained environments. Despite these benefits, SIKE has faced recent challenges due to cryptanalytic attacks that have compromised its security, bringing its long-term viability into question. These developments have sparked further research into refining isogeny-based techniques or finding alternative schemes within the same category.

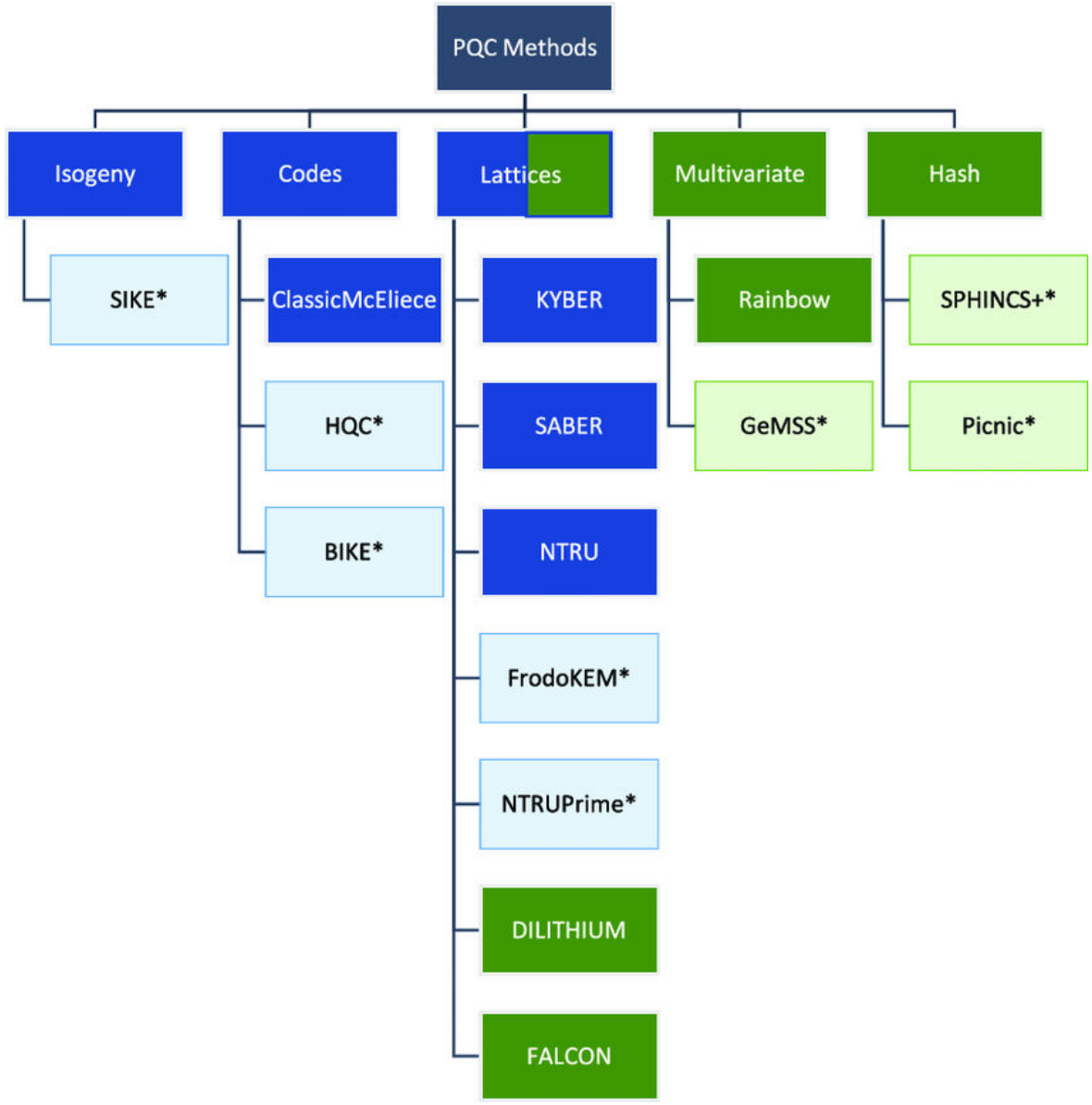

Figure 2. Different PQC Methods.

2.2 Code-based Cryptography

Code-based cryptography relies on the hardness of decoding a general linear code, a problem considered resistant to quantum attacks. Classic McEliece is a well-established code-based encryption scheme, valued for its strong security guarantees but criticized for its large key sizes. Other notable schemes include HQC (Hamming Quasi-Cyclic) and BIKE (Bit Flipping Key Encapsulation), both of which aim to improve upon the efficiency and practicality of code-based methods while maintaining robust security.

- **Classic McEliece:** Code-based cryptography relies on the hardness of decoding randomly generated linear codes. The Classic McEliece scheme is one of the oldest and most studied cryptographic systems in this category[9]. It offers strong security guarantees, withstanding cryptanalytic attacks over decades. However, it is often criticized for its large key sizes, which can be cumbersome in some applications. Despite this, Classic McEliece remains a strong candidate for post-quantum security due to its well-understood security properties.
- **HQC:**HQC is a modern code-based scheme that aims to improve the efficiency and practicality of code-

based cryptography. It uses quasi-cyclic codes, which allow for more efficient implementations, particularly in terms of key sizes and computational requirements [10]. HQC retains the strong security characteristics of traditional code-based systems while attempting to address some of their limitations, making it a promising candidate in the PQC landscape.

- **BIKE:**BIKE leverages the structure of low-density parity-check (LDPC) codes to provide efficient and secure key encapsulation mechanisms. BIKE's design focuses on achieving a good balance between security and efficiency, making it suitable for a wide range of applications [11]. By using LDPC codes, BIKE can achieve smaller key sizes and faster encryption and decryption processes compared to older code-based systems like Classic McEliece.

2.3 Lattice-based Cryptography

Lattice-based methods are among the most promising approaches in PQC, leveraging the hardness of problems like the Learning with Errors (LWE) and Short Integer Solution (SIS). Schemes like KYBER and SABER are leading candidates for key encapsulation, offering a good balance between security, efficiency, and practicality. NTRU and its variant NTRUPrime, along with FrodoKEM, are other notable lattice-based schemes, each with unique strengths in terms of computational efficiency and resistance to quantum attacks. Additionally, DILITHIUM and FALCON are prominent lattice-based digital signature schemes, known for their high security and relatively small signature sizes.

- **KYBER:** KYBER is a key encapsulation mechanism (KEM) based on the hardness of the LWE problem. It is highly regarded for its efficiency and security, making it one of the leading candidates in the NIST PQC standardization process [12]. KYBER's strength lies in its ability to provide secure and efficient key exchange protocols, which are essential for secure communications in the post-quantum era.
- **SABER:** SABER is another lattice-based KEM that uses the Module-Learning with Rounding (MLWR) problem. SABER is known for its simplicity and efficiency [13], particularly in terms of its computational requirements. It provides a good balance between security, speed, and key size, making it an attractive option for post-quantum secure communications.
- **NTRU and NTRUPrime:** NTRU is a public-key encryption algorithm based on lattice problems. It is one of the earliest lattice-based cryptosystems and has been studied extensively for its security properties. NTRUPrime is a variant of NTRU that improves upon the original design by providing stronger security guarantees and reducing certain vulnerabilities. Both NTRU and NTRUPrime are considered strong candidates for PQC due to their well-established security foundations [14].
- **FrodoKEM:**FrodoKEM is a lattice-based KEM that avoids structured lattices, relying instead on unstructured LWE problems. This approach provides additional security assurances, particularly against certain types of algebraic attacks [15]. While FrodoKEM may be less efficient than structured lattice schemes like KYBER, it is valued for its robust security guarantees.
- **DILITHIUM:** DILITHIUM is a digital signature scheme based on lattice problems, specifically the Fiat-Shamir with Aborts technique. It is designed to be both efficient and secure, providing small signatures and fast verification times [16]. DILITHIUM has gained significant attention for its potential to replace existing digital signature schemes in a post-quantum world.
- **FALCON:** FALCON is another lattice-based digital signature scheme that uses the Fast Fourier Sampling

technique. It is known for its compact signatures and fast performance, making it a strong contender in the PQC landscape [17]. FALCON's design prioritizes efficiency, making it suitable for use in resource-constrained environments where performance is critical.

2.4 Multivariate-based Cryptography

Multivariate cryptography is based on the difficulty of solving systems of multivariate quadratic equations, a problem that remains hard even for quantum computers. Rainbow is a well-known multivariate scheme, notable for its potential efficiency in certain applications. However, it has faced scrutiny due to vulnerabilities exposed by recent cryptanalysis. GeMSS is another multivariate scheme that focuses on achieving a balance between security and computational efficiency, though it, too, has encountered challenges related to its security assumptions.

- **Rainbow:** Rainbow is a multivariate public-key signature scheme that relies on the hardness of solving systems of multivariate quadratic equations. Rainbow is known for its potential efficiency and the ability to generate small signatures quickly [18]. However, it has faced significant cryptanalytic challenges, leading to concerns about its long-term security and suitability for standardization.
- **GeMSS (Great Multivariate Signature Scheme):**GeMSS is another multivariate-based scheme that focuses on providing robust security while maintaining reasonable efficiency. It improves upon earlier multivariate schemes by offering better resistance to certain types of attacks [19]. However, like Rainbow, GeMSS has also faced scrutiny due to the inherent challenges of ensuring the security of multivariate cryptographic systems.

2.5 Hash-based Cryptography

Hash-based cryptography builds on the security of cryptographic hash functions, offering a quantum-resistant approach primarily for digital signatures. SPHINCS+ is a stateless hash-based signature scheme that provides strong security guarantees but at the cost of larger signatures and slower performance compared to other PQC methods. Picnic is another hash-based scheme that combines hash functions with zero-knowledge proofs to create a secure and efficient signature scheme, offering an alternative to more traditional cryptographic approaches.

- **SPHINCS+:** SPHINCS+ is a stateless hash-based signature scheme that provides strong security guarantees against both classical and quantum attacks. Unlike other PQC methods, SPHINCS+ does not rely on algebraic structures but instead builds its security on the well-established hardness of hash function problems [20]. The trade-off for its robust security is larger signature sizes and slower performance, but SPHINCS+ is highly valued for its simplicity and long-term security.
- **Picnic:**Picnic is a hash-based signature scheme that combines hash functions with zero-knowledge proofs to achieve post-quantum security. Picnic is designed to be simple and secure, with an emphasis on avoiding the use of number-theoretic assumptions that could be vulnerable to quantum attacks. While Picnic's signatures are larger than some alternatives, its straightforward design and strong security properties make it a notable candidate in the PQC space.

3. Related Work

Algazy et al. [21] proposed the Syrga-1 digital signature algorithm, which employs lattice-based cryptographic techniques to enhance security against quantum attacks. The Syrga-1 algorithm utilizes hard lattice problems to generate cryptographic keys and signatures. The authors conducted performance evaluations and comparative analyses with existing post-quantum algorithms to demonstrate the efficiency and robustness of Syrga-1 in practical applications.Blanco Romero et al. [22] introduced PQSec-DDS, a framework for integrating PQC into Data Distribution Service (DDS) security protocols

tailored for robotic applications. The approach involves adapting DDS protocols to incorporate PQC algorithms, enhancing data encryption and key management against quantum threats. The methodology includes simulations and real-world testing to validate the improved security and functionality in robotic networks.

Choi and Lee [23] proposed a model for securing Internet of Things (IoT) networks using Post-Quantum Media Access Control Security (MACsec). The methodology integrates PQC techniques into MACsec protocols to enhance security against quantum attacks. It involves modifications to existing MACsec standards to include PQC-based encryption and key exchange mechanisms. Performance and scalability are assessed through rigorous testing to ensure effective deployment in large IoT environments.Oliva del Moral et al. [24] examined the application of PQC to enhance cybersecurity in critical infrastructures. Their methodology includes evaluating various PQC algorithms for their suitability in protecting critical systems against quantum attacks. The study involves a comparative analysis of PQC approaches and their integration into existing security frameworks, focusing on robustness and practical implementation.

Akçay and Yalçın [25] proposed a lightweight Application-Specific Instruction-set Processor (ASIP) design tailored for lattice-based post-quantum cryptographic algorithms. The methodology involves developing a custom processor architecture optimized for lattice-based cryptography, focusing on reducing power consumption and improving computational efficiency. Performance metrics are evaluated to ensure the ASIP's effectiveness in resource-constrained environments.Yang [26] analyzed the impact of quantum computing on modern cryptographic systems and proposed PQC solutions. The methodology includes a detailed examination of how quantum computing affects current cryptographic protocols and a review of PQC approaches designed to mitigate these effects. The study highlights the evolution of cryptographic standards in response to emerging quantum threats.Juraev and Mavlonov [27] investigated potential asymmetric cryptographic algorithms suitable for the post-quantum era. Their methodology involves evaluating various asymmetric cryptographic techniques, including lattice-based and multivariate polynomial schemes, for their resistance to quantum attacks. The study includes a comparative analysis of these algorithms' security and performance characteristics.

Nakka et al. [28] proposed a PQC approach for securing IEEE 2030.5-based distributed energy resources networks. The methodology involves integrating PQC algorithms into the IEEE 2030.5 standard to enhance security against quantum computing threats. The authors evaluate the performance of this integration through simulations and practical deployments in energy networks.González de la Torre et al. [29] conducted a structural analysis of code-based cryptographic algorithms submitted to the NIST post-quantum cryptography standardization process. The methodology includes evaluating the security and performance of various code-based algorithms, examining their structure and implementation details to assess their suitability for standardization.Wardhani et al. [30] explored high-and half-degree quantum multiplication techniques for evaluating post-quantum security. Their methodology includes developing and analyzing quantum multiplication algorithms to assess their effectiveness in ensuring post-quantum security. The study involves detailed performance evaluations and comparisons with existing methods.

Ravi et al. [31] investigated kleptographic attacks on lattice-based Key Encapsulation Mechanisms (KEMs) in post-quantum cryptography. The methodology includes analyzing potential backdoor vulnerabilities in lattice-based KEMs and proposing techniques for detecting and mitigating such attacks. The study focuses on enhancing the robustness of lattice-based cryptographic schemes against advanced threats.Señor et al. [32] analyzed the performance of post-quantum cryptographic schemes in securing large-scale wireless sensor networks. Their methodology involves evaluating various PQC algorithms for

their suitability in wireless sensor networks, focusing on efficiency, scalability, and security. The study includes performance metrics and practical implementation considerations.Xie et al. [33] provided a tutorial on hardware circuits and systems design for post-quantum cryptography. The methodology includes designing and implementing hardware architectures optimized for PQC algorithms, with a focus on circuit efficiency and performance. The study offers a comprehensive overview of hardware design considerations and practical implementation strategies.

Chen [34] introduced the PQCMC scheme, which integrates McEliece cryptography with implicit certificates for post-quantum security. The methodology involves developing and analyzing the PQCMC scheme's components, including its cryptographic foundations and certificate management. The study evaluates the scheme's security and efficiency through theoretical analysis and practical tests.Mujdei et al. [35] conducted a side-channel analysis of lattice-based post-quantum cryptographic schemes, focusing on polynomial multiplication. The methodology includes identifying potential side-channel vulnerabilities and proposing mitigation strategies. The study involves detailed side-channel attacks and their impact on lattice-based cryptography.Sonko et al. [36] reviewed the potential of quantum technologies in enhancing US digital security. The methodology includes a comprehensive review of quantum cryptographic approaches and their implications for national security. The study evaluates current and future quantum technologies' impact on encryption and security practices.

Karl et al. [37] proposed a hardware-accelerated approach for implementing post-quantum signatures on RISC-V architectures. The methodology involves designing hardware acceleration techniques to enhance the performance of post-quantum signature algorithms on RISC-V processors. The study includes performance benchmarks and implementation details.Ye et al. [38] developed a highly efficient lattice-based post-quantum cryptography processor optimized for IoT applications. The methodology includes designing a specialized processor architecture to handle lattice-based cryptographic operations efficiently. Performance and energy consumption are evaluated through extensive testing in IoT environments.

Alam et al. [39] analyzed cryptographic algorithms for IoT devices from a quantum perspective. The methodology involves evaluating the security and performance of existing cryptographic techniques against quantum threats and proposing quantum-resistant alternatives. The study focuses on optimizing cryptographic algorithms for IoT applications.Wang et al. [40] proposed integrating PQC with Single Instruction, Multiple Data (SIMD) operations on RISC-V architectures. The methodology includes designing SIMD-based enhancements for PQC algorithms to improve processing efficiency. Performance evaluations demonstrate the advantages of SIMD integration in cryptographic applications.

Govindhan and Kumar [41] proposed a novel approach for enhancing the security of multiple high-resolution millimeter wave images in IoT networks using post-quantum cryptography. The methodology involves integrating advanced post-quantum cryptographic techniques to secure image data transmitted across IoT networks. The study includes a detailed analysis of cryptographic algorithms suitable for high-resolution image data, performance benchmarks, and practical implementation scenarios.Algazy et al. [42] introduced Syrga2, a hash-based signature scheme designed for post-quantum security. The methodology focuses on leveraging hash functions to create robust digital signatures resistant to quantum attacks. The paper provides a detailed description of the Syrga2 scheme, including its cryptographic foundations, security analysis, and performance evaluation. The study demonstrates the scheme's efficiency and resilience compared to other post-quantum signature approaches.

Javaid et al. [43] analyzed the impact of post-quantum digital signatures on blockchain technology. The methodology involves a

comparative analysis of existing digital signature schemes and their vulnerability to quantum attacks. The study evaluates the performance of various post-quantum digital signatures within blockchain systems, highlighting their advantages and limitations in ensuring blockchain security against quantum threats.Sabrina et al. [44] reviewed privacy preservation strategies for the Internet of Medical Things (IoMT) using blockchain technology and post-quantum cryptography. The methodology includes an examination of how blockchain can enhance IoMT security by integrating post-quantum cryptographic techniques. The paper discusses various privacy-preserving mechanisms, their effectiveness in protecting medical data, and the integration challenges with blockchain.Hwang et al. [45] proposed the Billiard Quantum Chaos encryption scheme, designed for image encryption in the post-quantum era. The methodology involves applying quantum chaos principles to develop a novel image encryption technique. The paper includes theoretical analysis, encryption algorithm design, and performance evaluations to demonstrate the scheme's security and efficiency against quantum attacks.

Ojetunde et al. [46] developed a multi-level rule model for selecting appropriate post-quantum cryptographic algorithms for 5G applications. The methodology includes designing a decision-making framework that evaluates various PQC algorithms based on their suitability for 5G networks. The study provides a detailed analysis of criteria for algorithm selection, implementation strategies, and performance assessments.Kaleem et al. [47] introduced new cryptographic techniques aimed at enhancing cloud computing security with a focus on efficiency. The methodology involves developing and evaluating advanced cryptographic algorithms that address the unique security requirements of cloud computing environments. The paper includes performance comparisons with existing methods and practical implementation considerations.Mathews and Panchami [48] proposed QS-Auth, a quantum-secure mutual authentication protocol for heterogeneous delay-tolerant networks. The methodology combines Physical Unclonable Functions (PUF) with post-quantum signatures to provide robust authentication. The study details the protocol's design, security analysis, and performance evaluation, demonstrating its effectiveness in secure communication within delay-tolerant networks.

Hanafi et al. [49] explored the enhancement of post-quantum cryptography using adversarial neural cryptography techniques. The methodology involves applying neural networks to strengthen cryptographic algorithms against quantum attacks. The study includes the design of adversarial neural networks, their integration with PQC algorithms, and evaluation of their impact on cryptographic security and performance.Mohamed et al. [50] proposed a hybrid cryptographic approach using K3S and post-quantum techniques to secure IoMT systems. The methodology involves integrating K3S cryptographic methods with post-quantum algorithms to enhance security for embedded medical systems. The paper includes implementation details, performance assessments, and security evaluations to demonstrate the effectiveness of the hybrid approach in securing IoMT environments.

4. Applications

The PQC is designed to secure data against the potential threats posed by quantum computers. Its applications span various domains, reflecting the growing importance of ensuring data security in a quantum-aware future. Here are some key applications of PQC:

- **Secure Communication**PQC can secure end-to-end encryption in messaging applications, ensuring that communication remains private even if quantum computers become capable of breaking traditional encryption methods.Email services can implement PQC to protect sensitive information from being decrypted by quantum-enabled adversaries.
- **Data Protection**PQC algorithms can be used to encrypt data stored in the cloud, protecting it from unauthorized

access by quantum-capable attackers.Individuals and organizations can use PQC to encrypt files on their devices or in transit, safeguarding them from future quantum threats.

- **Digital Signatures**PQC can enhance the security of digital signatures, which are crucial for verifying the authenticity and integrity of electronic documents and contracts.Developers can use PQC to sign software updates and applications, ensuring that they have not been tampered with and are verified as coming from legitimate sources.
- **Blockchain and Cryptocurrencies:** PQC can secure blockchain transactions and smart contracts, protecting them from quantum attacks that could potentially compromise the integrity of cryptocurrency systems.Implementing PQC in blockchain consensus protocols can help maintain the security and reliability of decentralized networks against quantum threats.
- **IoT Security:** PQC can be used to secure authentication mechanisms for Internet of Things (IoT) devices, ensuring that only authorized devices can access and communicate within a network.PQC can protect the integrity of data collected by IoT devices, making sure that it remains unchanged and secure from quantum-enabled tampering.
- **Public Key Infrastructure (PKI):** PQC can be implemented in certificate authorities to secure digital certificates, ensuring that public key infrastructure remains robust against quantum computing threats.PQC algorithms can replace traditional key exchange mechanisms, ensuring secure key establishment in a post-quantum world.
- **Secure Voting Systems:** PQC can secure electronic voting systems, protecting votes from being intercepted or altered by quantum-enabled adversaries.Ensuring the integrity and authenticity of election results can be enhanced using PQC, safeguarding democratic processes.
- **Financial Transactions:** PQC can protect online banking transactions and financial communications, safeguarding them from potential quantum attacks.Financial institutions can use PQC to secure cryptographic tokens and assets, ensuring their safety against quantum-enabled decryption.
- **Government and Military Applications:** PQC can secure classified communications and sensitive information within government and military sectors, protecting national security from quantum threats.Government and military networks can implement PQC to safeguard against espionage and cyber-attacks facilitated by quantum computing advancements.
- **Healthcare Data Protection:** PQC can secure electronic health records (EHRs) and other sensitive medical data, ensuring patient privacy and data integrity.Securing communications in telemedicine applications with PQC ensures that patient consultations and health data are protected against future quantum attacks.

Implementing PQC in these areas helps future-proof security systems, ensuring they remain resilient and reliable in the face of advancing quantum technologies.

5. Problem statement

As quantum computing advances, traditional cryptographic methods face significant vulnerabilities. The primary challenge is that many widely-used encryption schemes, such as those based on RSA and ECC (Elliptic Curve Cryptography), are at risk of being broken by quantum algorithms like Shor's algorithm, which can efficiently solve problems such as integer factorization and discrete logarithms. This jeopardizes the security of data encrypted with these methods, necessitating the development and adoption of new

cryptographic approaches resistant to quantum attacks. The urgency for PQC has led to increased research into various alternatives, but many of these methods, while promising, still face significant hurdles that hinder their practical deployment and effectiveness.

One of the major issues with current post-quantum cryptographic methods is their performance. Many PQC schemes, including those based on lattice problems, code-based cryptography, or multivariate quadratic equations, often require substantial computational resources compared to classical cryptographic methods. For instance, lattice-based cryptography, while theoretically secure against quantum attacks, can suffer from inefficiencies related to key sizes, encryption and decryption speeds, and overall computational complexity. This performance overhead can be a significant drawback, particularly in resource-constrained environments or applications where computational efficiency and speed are critical.

Another problem with existing PQC methods is their interoperability and integration with current systems. Many post-quantum cryptographic schemes are not designed to work seamlessly with existing infrastructure and protocols. For instance, integrating new PQC algorithms with current Public Key Infrastructure (PKI) systems, secure communication protocols, and authentication mechanisms can be complex and may require significant modifications to existing systems. This lack of compatibility poses a challenge for organizations seeking to transition to quantum-resistant solutions without disrupting their existing operations or incurring substantial costs.

Additionally, the security assurances of many PQC schemes are still under active research and scrutiny. While theoretical models and cryptanalysis suggest that certain post-quantum algorithms are resistant to quantum attacks, real-world security assessments are ongoing. For example, some schemes based on lattice problems or code-based cryptography are yet to be thoroughly tested against practical quantum adversaries, raising concerns about their long-term robustness. Moreover, there is a need for rigorous standardization and validation processes to ensure that these new cryptographic methods provide not only quantum resistance but also adequate protection against other types of attacks.

6. Future Directions

The future directions not only address the current limitations of post-quantum cryptographic methods but also aim to create a more practical, secure, and efficient cryptographic landscape. By leveraging the strengths of hybrid approaches, these objectives seek to advance the field of cryptography and provide robust solutions for the challenges posed by quantum computing.

- To address the limitations of existing post-quantum cryptographic methods, integrating Ring Learning with Errors (R-LWE) Homomorphic Encryption with Supersingular Isogeny Diffie-Hellman (SIDH) presents a promising direction. R-LWE-based homomorphic encryption offers a robust solution for privacy-preserving computations by allowing computations to be performed on encrypted data without decryption. This approach ensures data security even in scenarios where sensitive data needs to be processed in untrusted environments. However, the efficiency of R-LWE homomorphic encryption can be hindered by its computational complexity and large key sizes. By combining R-LWE with SIDH, which provides efficient key exchange mechanisms resistant to quantum attacks, it is possible to enhance the encryption and decryption processes. SIDH, with its smaller key sizes and efficient computational requirements compared to traditional post-quantum schemes, complements R-LWE by optimizing key exchange operations. This hybrid approach aims to leverage the strengths of both methods, resulting in a cryptographic system that not only maintains strong security guarantees but also improves practical performance and efficiency in real-world applications.

- Developing a hybrid key exchange scheme that combines R-LWE Homomorphic Encryption with Elliptic Curve Diffie-Hellman (ECDH) addresses several pressing issues in post-quantum cryptography. While ECDH is a widely adopted key exchange method offering efficient performance and strong security under classical cryptographic assumptions, it is vulnerable to quantum attacks. Incorporating R-LWE Homomorphic Encryption into the key exchange process adds a layer of quantum resistance, enhancing the overall security of the key establishment phase. This hybrid scheme aims to benefit from the strengths of both R-LWE and ECDH: the robust, quantum-resistant properties of R-LWE and the efficiency and established infrastructure of ECDH. Such a combination can provide a more secure and practical solution for key exchange, ensuring that the cryptographic keys remain secure against both quantum and classical adversaries. This development would facilitate a smoother transition to quantum-resistant security while maintaining the performance benefits of existing key exchange protocols.
- The integration of hybrid lattice-based cryptography with SIDH and ECDH mechanisms represents a comprehensive approach to addressing the diverse security needs in the post-quantum era. Lattice-based cryptography offers strong theoretical security guarantees against quantum attacks, but its practical implementation can be complex and resource-intensive. By integrating lattice-based schemes with SIDH and ECDH, which provide efficient key exchange and encryption mechanisms, a more balanced and versatile security framework can be developed. This hybrid framework aims to combine the quantum-resistance of lattice-based cryptography with the efficiency of SIDH and ECDH, addressing both security and performance concerns. Such an integration could offer a robust solution for a wide range of applications, including secure communications, data storage, and transaction processing, ensuring comprehensive protection against emerging quantum threats while maintaining high efficiency and compatibility with existing systems.

7. Future Scope

The literature survey on PQC reveals a dynamic and evolving field grappling with significant challenges and opportunities. The current landscape highlights the robust theoretical foundations of PQC techniques, such as lattice-based and code-based cryptographic schemes, which offer promising solutions for securing data against quantum threats. However, practical implementation issues, including computational overhead, key size limitations, and the need for efficient algorithms, persist. Recent advancements, such as hybrid approaches combining R-LWE and SIDH, and the integration of ECDH with lattice cryptography, demonstrate a proactive effort to enhance security and efficiency. Despite these advancements, challenges remain in balancing performance with quantum resistance and addressing specific application needs, such as in IoT and cloud computing. Future research must focus on refining these hybrid methods, optimizing computational efficiency, and ensuring broad applicability to provide a comprehensive, quantum-secure framework for modern cryptographic needs.

References

[1] Gharavi, Hadi, Jorge Granjal, and Edmundo Monteiro. "Post-quantum blockchain security for the Internet of Things: Survey and research directions." *IEEE Communications Surveys & Tutorials* (2024).

[2] Vithalkar, P. N. (2024). Cryptographic Protocols Resilient to Quantum Attacks: Advancements in Post-Quantum

Cryptography. *Communications on Applied Nonlinear Analysis*, *31*(3s), 520-532.

[3] Liu, Tao, Gowri Ramachandran, and Raja Jurdak. "Post-quantum cryptography for internet of things: a survey on performance and optimization." *arXiv preprint arXiv:2401.17538* (2024).

[4] Hasan, KhondokarFida, Leonie Simpson, Mir Ali Rezazadeh Baee, Chadni Islam, Ziaur Rahman, Warren Armstrong, Praveen Gauravaram, and Matthew McKague. "A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies." IEEE Access (2024).

[5] Opiłka, Filip, Marcin Niemiec, Maria Gagliardi, and Michail Alexandros Kourtis. "Performance Analysis of Post-Quantum Cryptography Algorithms for Digital Signature." *Applied Sciences* 14, no. 12 (2024): 4994.

[6] Mansoor, Khwaja, Mehreen Afzal, Waseem Iqbal, Yawar Abbas, ShynarMussiraliyeva, and Abdellah Chehri. "PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems." *Internet of Things* 27 (2024): 101228.

[7] Ricci, Sara, Patrik Dobias, Lukas Malina, Jan Hajny, and Petr Jedlicka. "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography." *IEEE Access* (2024).

[8] Bhasin, Shivam, Fabrizio De Santis, and Francesco Regazzoni. "Special Issue on Post-Quantum Cryptography for Embedded Systems." *ACM Transactions on Embedded Computing Systems* 23, no. 2 (2024): 1-3.

[9] Rawal, Bharat S., and Anjan Biswas. "A comprehensive survey of post-quantum cryptography and its implications." *Engineering Science & Technology* (2024): 256-269.

[10] García-Cid, Marta Irene, Michail-Alexandros Kourtis, David Domingo, Nikolay Tcholtchev, Evangelos K. Markakis, Marcin Niemiec, Javier Faba et al. "PQ-REACT: Post Quantum Cryptography Framework for Energy Aware Contexts." In *Proceedings of the 19th International Conference on Availability, Reliability and Security*, pp. 1-7. 2024.

[11] Tiwari, Amritansh, Rahul Chauhan, Nischay Joshi, Swati Devliyal, Srinivas Aluvala, and Amit Kumar. "The Quantum Threat: Implications for Data Security and the Rise of Post-Quantum Cryptography." In *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, pp. 1-7. IEEE, 2024.

[12] Allgyer, Winfred, Tyler White, and Tarek A. Youssef. "Securing the Future: A Comprehensive Review of Post-Quantum Cryptography and Emerging Algorithms." *SoutheastCon 2024* (2024): 1282-1287.

[13] Barzen, Johanna, and Frank Leymann. "Post-Quantum Security: Origin, Fundamentals, and Adoption." *arXiv preprint arXiv:2405.11885* (2024).

[14] Abdallah, Walid. "A physical layer security scheme for 6G wireless networks using post-quantum cryptography." *Computer Communications* 218 (2024): 176-187.

[15] Harmalkar, Manjiri, Kurunandan Jain, and Prabhakar Krishnan. "A Survey of Post Quantum Key Encapsulation Mechanism." In *2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*, pp. 141-149. IEEE, 2024.

[16] Ahmed, Nadia. "Quantum Computing Algorithms for Integer Factorization: A Comparative Analysis." *Modern Dynamics: Mathematical Progressions* 1, no. 1 (2024): 6-9.

[17] Alomari, Ahmad, and Sathish AP Kumar. "Securing IoT Systems in a Post-Quantum Environment: Vulnerabilities, Attacks, and Possible Solutions." *Internet of Things* (2024): 101132.

[18]Rawal, Bharat S., and Peter J. Curry. "Challenges and opportunities on the horizon of post-quantum cryptography." *APL Quantum* 1, no. 2 (2024).

[19]Karakaya, Aykut, and Ahmet Ulu. "A survey on post-quantum based approaches for edge computing security." *Wiley Interdisciplinary Reviews: Computational Statistics* 16, no. 1 (2024): e1644.

[20]Shajahan, R., Jain, K., & Krishnan, P. (2024, January). A Survey on NIST 3 rd Round Post Quantum Digital Signature Algorithms. In *2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)* (pp. 132-140). IEEE.

[21]Algazy, K., Sakan, K., Khompysh, A., &Dyusenbayev, D. (2024). Development of a New Post-Quantum Digital Signature Algorithm: Syrga-1. *Computers*, *13*(1), 26.

[22]Blanco Romero, J., Lorenzo, V., Almenares, F., Díaz Sánchez, D., & Serrano Navarro, A. (2024). PQSec-DDS: Integrating Post-Quantum Cryptography into DDS Security for Robotic Applications. *Jornadas Nacionales de Investigación en Ciberseguridad (JNIC)(9º. 2024. Sevilla)(2024), pp. 396-403.*

[23]Choi, Juhee, and Junwon Lee. "Secure and Scalable Internet of Things Model Using Post-Quantum MACsec." Applied Sciences 14, no. 10 (2024): 4215.

[24]Oliva delMoral, Javier, Antonio deMarti iOlius, Gerard Vidal, Pedro M. Crespo, and Josu Etxezarreta Martinez. "Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective." *IEEE Internet of Things Journal* (2024).

[25]Akçay, L., & Yalçın, B. Ö. (2024). Lightweight ASIP Design for Lattice-Based Post-quantum Cryptography Algorithms. *Arabian Journal for Science and Engineering*, 1-15.

[26]Yang, David. "Post-Quantum Cryptography: Effects of Quantum Computing on Modern Cryptography." *International Journal of High School Research* 6, no. 6 (2024).

[27]Juraev, Gayrat U., and Alisher B. Mavlonov. "Delving into Potential Asymmetric Cryptographic Algorithms for the Post-Quantum Era." In *2024 IEEE 25th International Conference of Young Professionals in Electron Devices and Materials (EDM)*, pp. 2510-2513. IEEE, 2024.

[28]Nakka, K., Ahmad, S., Kim, T., Atkinson, L., & Ammari, H. M. (2024, February). Post-Quantum Cryptography (PQC)-Grade IEEE 2030.5 for Quantum Secure Distributed Energy Resources Networks. In *2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (pp. 1-5). IEEE.

[29]GonzÁlez de la Torre, M. A., L. HernÁndez Encinas, and JI Sánchez GarcÍa. "Structural analysis of code-based algorithms of the NIST post-quantum call." Logic Journal of the IGPL (2024): jzae071.

[30]Wardhani, Rini Wisnu, Dedy SeptonoCaturPutranto, and Howon Kim. "High-and Half-Degree Quantum Multiplication for Post-Quantum Security Evaluation." *IEEE Access* (2024).

[31]Ravi, P., Bhasin, S., Chattopadhyay, A., Aikata, A., & Sinha Roy, S. (2024, June). Backdooring post-quantum cryptography: Kleptographic attacks on lattice-based KEMs. In *Proceedings of the Great Lakes Symposium on VLSI 2024* (pp. 216-221).

[32]Señor, Jaime, Jorge Portilla, and Marta Portela-García. "Performance Analysis of Postquantum Cryptographic Schemes for Securing Large-Scale Wireless Sensor Networks." *IEEE Transactions on Industrial Informatics* (2024).

[33]Xie, Jiafeng, Wenfeng Zhao, Hanho Lee, Debapriya Basu Roy, and Xinmiao Zhang. "Hardware Circuits and Systems Design for Post-Quantum

Cryptography–A Tutorial Brief." *IEEE Transactions on Circuits and Systems II: Express Briefs* (2024).

[34]Chen, Abel CH. "PQCMC: Post-Quantum Cryptography McEliece-Chen Implicit Certificate Scheme." *arXiv preprint arXiv:2401.13691* (2024).

[35]Mujdei, Catinca, Lennert Wouters, Angshuman Karmakar, Arthur Beckers, Jose Maria Bermudo Mera, and Ingrid Verbauwhede. "Side-channel analysis of lattice-based post-quantum cryptography: Exploiting polynomial multiplication." *ACM Transactions on Embedded Computing Systems* 23, no. 2 (2024): 1-23.

[36]Sonko, Sedat, Kenneth Ifeanyi Ibekwe, Valentine Ikenna Ilojianya, Emmanuel Augustine Etukudoh, and Adefunke Fabuyide. "Quantum cryptography and US digital security: a comprehensive review: investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security." *Computer Science & IT Research Journal* 5, no. 2 (2024): 390-414.

[37]Karl, Patrick, Jonas Schupp, Tim Fritzmann, and Georg Sigl. "Post-quantum signatures on RISC-V with hardware acceleration." *ACM Transactions on Embedded Computing Systems* 23, no. 2 (2024): 1-23.

[38]Ye, Zewen, Ruibing Song, Hao Zhang, Donglong Chen, Ray Chak-Chung Cheung, and Kejie Huang. "A Highly-efficient Lattice-based Post-Quantum Cryptography Processor for IoT Applications." *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2024, no. 2 (2024): 130-153.

[39]Alam, Md Mokarram, Anamika Arora, Aditya Bhatt, Swati Devliyal, and Srinivas Aluvala. "Cryptographic Algorithms for IoT Devices: A Quantum Analysis." In *2024 3rd International Conference for Innovation in Technology (INOCON)*, pp. 1-7. IEEE, 2024.

[40]Wang, Liang-Ni, Ju-Hung Li, Chi-Bang Kuan, and Yi-Chiao Su. "Support Post Quantum Cryptography with SIMD Everywhere on RISC-V Architectures." In *The 53 rd International Conference on Parallel Processing (ICPP'24) Workshops Proceedings*, p. 23. 2024.

[41]Govindhan, P., & Kumar, K. (2024, May). Post-quantum cryptography for Multiple high-resolution millimeter wave images for enhanced security in IOT Networks. In *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)* (pp. 529-533). IEEE.

[42]Algazy, Kunbolat, Kairat Sakan, Saule Nyssanbayeva, and Oleg Lizunov. "Syrga2: Post-Quantum Hash-Based Signature Scheme." *Computation* 12, no. 6 (2024): 125.

[43]Javaid, Muhammad Abdur Rehman, Muhammad Ashraf, Tayyab Rehman, and Noshina Tariq. "Impact of Post Quantum Digital Signatures On Block Chain: Comparative Analysis." *The Asian Bulletin of Big Data Management* 4, no. 1 (2024): Science-4.

[44]Sabrina, Fariza, Shaleeza Sohail, and Umair Ullah Tariq. "A Review of Post-Quantum Privacy Preservation for IoMT Using Blockchain." *Electronics* 13, no. 15 (2024): 2962.

[45]Hwang, S. O., Waseem, H. M., & Munir, N. (2024). Billiard Quantum Chaos: A Pioneering Image Encryption Scheme in the Post-Quantum Era. *IEEE Access*.

[46]Ojetunde, Babatunde, Takuya Kurihara, Kazuto Yano, Toshikazu Sakano, and Hiroyuki Yokoyama. "A Multi-Level Rule Model for Selecting Post-Quantum Cryptography in 5G Application and Beyond." In *2024 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1-6. IEEE, 2024.

[47]Kaleem, Muhammad, Muhammad Azhar Mushtaq, Uzair Jamil, Sadaqat

Ali Ramay, Tahir Abbas Khan, Siraj Patel, Rizwan Zahidy, and Sayyid Kamran Hussain. "New Efficient Cryptographic Techniques For Cloud Computing Security." *Migration Letters* 21, no. S11 (2024): 13-28.

[48]Mathews, Mahima Mary, and V. Panchami. "QS-Auth: A Quantum-secure mutual authentication protocol based on PUF and Post-Quantum Signature for Heterogeneous Delay-Tolerant Networks." *Journal of Information Security and Applications* 83 (2024): 103787.

[49]Hanafi, B., Bokhari, M. U., & Khan, I. (2024, February). Enhancing Post-Quantum Cryptography with Adversarial Neural Cryptography. In *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1706-1712). IEEE.

[50]Mohamed, EI-Hadedy, Patricia V. Ankunda, James Ung, and Wen-Mei Hwu. "Securing the Internet of Medical Things (IoMT) with K3S and Hybrid Cryptography: Integrating Post-Quantum Approaches for Enhanced Embedded System Security." In *2024 IEEE 17th Dallas Circuits and Systems Conference (DCAS)*, pp. 1-6. IEEE, 2024.