IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 17 November 2025, accepted 7 January 2026, date of publication 19 January 2026, date of current version 22 January 2026.

Digital Object Identifier 10.1109/ACCESS.2026.3655100

TOPICAL REVIEW

A Systematic Literature Review of Lattice-Based Key Encapsulation Mechanisms and Digital Signatures: Current Status, Research Gaps, and Future Directions

DEREJE WASIHUN MELLESE[1,2], ZEBENE GIRMA TEFERA[1,2], MELAKU BERHE BELAY[1,2], GIZACHEW HAILE SEFFA[3], ADEM GULUMA NEGEWO[1,2], ZELALEM GIZACHEW ACHAM[3], MEKONNEN ANDUALEM ATINAF[3], AND DANIEL MERKEBU ADAMU[3]

[1]High Performance Computing and Big Data Analytics Center of Excellence, Addis Ababa Science and Technology University, Addis Ababa 16417, Ethiopia
[2]Mathematics, Physics and Statistics Division, Addis Ababa Science and Technology University, Addis Ababa 16417, Ethiopia
[3]Information Network Security Administration, Addis Ababa 124498, Ethiopia

Corresponding author: Dereje Wasihun Mellese (dereje.wasihun@aastu.edu.et)

ABSTRACT The progress made in the field of quantum computing has drawn the attention of the cryptographic community to the existing systems' security. Thus, researchers are looking for post-quantum cryptographic solutions that would be able to defend against the upcoming quantum attacks. To this end, different cryptographic approaches have been proposed. Among these approaches, lattice-based cryptography stands out as a promising candidate because of it's efficient parameters and performance characteristics. The robustness of these post-quantum methods has been tested against the NIST criteria so that the security they offer can be trusted. In this work, we conducted a systematic literature review on lattice-based KEM and signature schemes. We have analyzed 41 papers taken from five major databases and addressed four research questions that include the current landscape of lattice-based post-quantum cryptography, the gaps in the existing literature on lattice-based post-quantum cryptography, identifying mathematical hard problems used in the papers, and future research directions. The reviewed papers primarily focus on key encapsulation mechanisms (KEM) and signature schemes. One of the key findings of this study is the identification of promising lattice-based cryptographic schemes beyond the NIST finalists, such as Qu-Octonion NTRU, Tyber, and HAETAE etc., which clearly shows there is notable progress in lattice-based post-quantum systems. In addition, this review identifies key gaps in current research, including a lack of emphasis on the tradeoffs between security and efficiency, and an insufficient design of hybrid cryptosystems. Finally, the strengths and limitations of the current lattice-based Cryptosystems and future research directions are presented.

INDEX TERMS Lattice-based cryptography, lattice-based cryptosystems, lattice-based schemes, cryptanalysis of lattice-based schemes, post quantum.

I. INTRODUCTION

A. BACKGROUND

The security of most modern cryptographic systems, particularly public key cryptosystems, depends on hard mathematical problems such as integer factorization and the discrete logarithm problems. Classical computers cannot solve these problems efficiently; however, the rise of quantum computing poses a serious threat to these systems because Shor's and Grover's algorithms can solve the problems efficiently [1].

Quantum computing represents a paradigm shift in computational capabilities, applying principles of quantum mechanics that are fundamentally different from classical computers. Due to their superposition characteristics,

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

quantum computers can perform calculations simultaneously, offering significant speed advantages for solving specific mathematical hard problems. This competence increases concerns about the potential for quantum computers to break current cryptography, posing a serious threat as larger quantum systems could compromise sensitive data, fake digital signatures, and weaken secure communications [2].

In response to these threats, emerging research is focused on developing post-quantum systems that depend on hard mathematical problems resilient to quantum attacks, such as hash-based, lattice-based and code-based methods. These approaches aim to provide strong security to sensitive information when quantum computers threaten to compromise modern cryptographic methods [3].

Although the widespread adoption of post-quantum cryptosystems is underway, much remains to be done. Some of the more prominent advancements include the ongoing standardization process involving institutions like NIST, which has finalized evaluating post-quantum KEMs and signature schemes in 2024. With increased awareness and urgency presented by the potential threats posed by quantum computing, total adoption is still lofty and would likely take years. The timeline may be more closely tied to the maturity of quantum technologies and the deployment of secure standards on a wide scale [5], [6], [17].

The cryptographic community should be encouraged to focus more on the development of post-quantum cryptographic schemes that offer security against attacks from quantum computers when quantum computing becomes widely used in the near future. To achieve this, gaining an in-depth understanding of the field, knowing the landscape, identifying research gap and identifying the future focus areas are crucial. We have conducted this systematic literature review in order to ensure that the aforementioned primary tasks are accomplished. The review is also meant to serve as a reference for anyone who want to understand the landscape in the area of PQCs.

B. OVERVIEW OF POST-QUANTUM CRYPTOGRAPHY (PQC)

PQC involves the design of cryptographic algorithms with proof against apparent attacks by upcoming quantum computers. There exist several promising families of cryptosystems in this arena: namely lattice-based, multivariate polynomial based, code-based, hash-based, and isogeny-based cryptographic methods. Each category has its own merits and challenges in the ongoing process of developing secure cryptographic solutions [6].

1) HASH-BASED CRYPTOGRAPHY

Relies on hash functions, which mainly produce digital signatures and are secured by cryptographic hash functions like SHA-3. An asymmetric signature scheme was introduced in 1979 by Ralph Merkle using a one-time signature (OTS). The simplest and most popular hash-based cryptosystems is considered to be the signature scheme. This approach strengthens a weak signature through the use of a hash function [7]. The Merkle signature scheme is an enhancement of Leslie Lamport's original idea for OTS to develop a multi-use signature scheme that allows the generation of signatures multiple times. The signatures generated are hence based on hash functions whose security prevails even against the anticipated quantum attacks. While delivering strong resistance to quantum-based attacks, these systems are predominantly optimized for digital signatures and less effective for encryption purposes.

A major limitation of many practical hash-based signature schemes is the burden placed upon the signer to carefully track the overall count of messages signed previously. A discrepancy in this record could result in a security risk. Another limitation is that although a finite number of digital signatures may be generated, beyond this limit, the digital signatures may become of considerable size. Nevertheless, hash-based digital signature algorithms can be viewed as secure and resilient against quantum attacks, thus offering promise in PQC [8], [9], [10].

2) MULTIVARIATE CRYPTOGRAPHY

Depends on the computational hardness of solving multivariate polynomial equations. Multivariable polynomial systems are NP-complete, a computational complexity property that underscores their suitability for PQC. These cryptographic schemes are highly efficient for cryptanalysis-resistant design and excel in generating digital signatures, producing the shortest signature lengths among PQC algorithms while maintaining robust security. Schemes such as Matsumoto-Imai and Unbalanced Oil and Vinegar (UOV) were used in order to clarify the theoretical security of this approach. Despite its resistance to quantum attacks, it is difficult to implement in real-world applications due to the need for larger key sizes and mathematical complications. Schemes such as Rainbow deliver strong security guarantees but face innate efficiency trade-offs in practical implementations [7].

3) CODE BASED CRYPTOGRAPHY

It is one of the post quantum cryptography that uses error correcting codes and its security is based on difficulty of a coding theoretic problem. In 1978, the earliest example, a public key encryption (PKE) scheme, was introduced by Robert J. McEliece. The McEliece algorithm ensures security by embedding random errors into messages during encryption. Here, the private key comprises a Goppa random binary code.

The public key is constructed from a permuted version of this code to create a randomized generator matrix, and the ciphertext represents the original codeword altered by these errors. Decryption is uniquely feasible for the authorized recipient holding the private key, which enables precise error correction to recover the original message [11].

The security of the McEliece cryptosystem, for instance, is rooted in the computational challenge of decoding general linear codes. Despite these code-based cryptosystems offer advantages over computational efficiency for encryption and decryption, they face critical storage demands of large key sizes, in which public key sizes often range from 100 kilobytes up to multiple megabytes. In 2001, Essential Changes for McEliece's scheme were the conversions by Kobara and Imai which are CCA2(Chosen-Ciphertext Attack, Type 2)-secure [12], [13].

4) ISOGENY-BASED CRYPTOGRAPHY

Derives its security from properties of congruent elliptic curve graphs over super anomalous congruence graphs or finite fields. This approach includes two main system families that rely on isogeny algebra: supersingular isogeny Diffie–Hellman (SIDH) and commutative supersingular isogeny Diffie–Hellman (CSIDH). From this, SIDH has become a prominent protocol and recently gained significant attention. Following the third round of the NIST competition, an isogeny-based PKE scheme called Supersingular Isogeny Key Encapsulation (SIKE) was selected as a PKE and KEM. However, vulnerabilities identified via cryptanalysis led to the removal of this PKE/KEM scheme from the fourth-round candidate algorithms [14].

5) LATTICE-BASED CRYPTOGRAPHY

Derives its security from the complexity of solving mathematical challenges like the Shortest Vector Problem (SVP), the Closest Vector Problem (CVP), and Learning With Error(LWE), which remain intractable for both classical and quantum systems. In addition to its robust security foundation, the framework maintains high operational efficiency, achieving rapid encryption and decryption [15].

C. IMPORTANCE OF LATTICE-BASED PQC

Lattice-based cryptography is a good nominee for PQC because of its theoretical background and resistance to quantum attacks. There are well-investigated hard problems such as the SVP and LWE upon which these schemes are based.

This theory offers security reductions that provide some confidence in their security. Furthermore, it can support a variety of cryptographic primitives such as KEM, digital signatures, and fully homomorphic encryption (FHE). The design is efficient and flexible in parameter selection, offering them as candidates for lightweight settings all the way to high-performance settings, thus ensuring lattice-based cryptography as an implementation of future cryptography standards.

[16] Explains at the developments in lattice based cryptography of the last ten years as well as look forward at how it might be used to offer safe solutions in the post quantum age. It clearly underlines how crucial lattice based cryptography is to the continuous advancement of safe communication systems. In light of the threats posed by quantum computing.

In view of the threats posed by quantum computing to modern cryptography, a variety of cryptographic schemes have been introduced for the quantum period, making it active research area. The formation and standardization of effective post quantum algorithms pose substantial challenges to the academic community. To make well informed choices, we must assess which post-quantum types show the most promise for the future.

As we explore cryptography from various angles, lattice based cryptography is viewed increasingly as a top candidate for PQC systems due to its exceptional advantages. This assessment is grounded in strong security principles, efficiency, flexibility, alignment with NIST standards, resilience against quantum attacks, and other pertinent factors [18], [19].

- **Robust security underpinnings**:
  Lattice problems are characterized by their high complexity in high-dimensional spaces, making them challenging for quantum computations to solve, even with parallel processing. The difficulty of well-known mathematical challenges, such as CVP, LWE, SVP problems and their variants, is the basis for the security of lattice-based cryptography. These problems are generally considered as difficult for both quantum and classical computers to tackle, establishing a strong security foundation. Unlike traditional cryptographic methods that often depend on number-theoretic problems, such as integer factorization, lattice-based systems provide greater resilience against potential quantum threats like Shor's algorithm [20].
- **Adaptability and Effectiveness**:
  The prominence of lattice-based cryptography is due to its adaptability, supporting a diversity of cryptographic functions, including encryption/KEM, digital signatures, identity authentications, and homomorphic encryption. Its adaptability facilitates a range of applications, from communication security to preserving computational privacy [15].
- **The State of NIST Standards**:
  In the standardization of PQC algorithms, the National Institute of Standards and Technology (NIST) has recognized the value of lattice-based cryptography. Throughout the evaluation process, broad aspects were identified to compare candidate algorithms: security check, cost, performance, and algorithm and implementation characteristics. From each round of evaluation, the majority of selected schemes were lattice-based, including Kyber and Dilithium [5], [6], [17].
- **Resistance to Quantum Attacks**:
  Quantum attack resistance nature of the lattice problem is its fundamental advantage for lattice-based cryptography. As the advancements in quantum computing grow, they undermine the security of conventional cryptography.

Lattice-based cryptosystems are particularly designed to thwart threats, making them a promising choice for securing data in this quantum era. Cryptographic algorithms recommended by NIST are constructed to resist both classical and quantum adversaries, ensuring long-term data security [10].

Therefore, based on the above evidence, lattice-based cryptography stands out as a prominent choice due to its robust security, efficiency, endorsement by NIST, and practical applicability [15], [21], [22]. In light of this, we conduct a systematic literature review on lattice-based cryptosystems, emphasizing their potential to enhance the security of digital communications in the post-quantum landscape.

D. OBJECTIVES AND RESEARCH QUESTIONS

Objectives:

The objectives of this review are

- To explore the current status of lattice-based cryptography
- To identify mathematical hard problems that are used in the lattice-based schemes
- To identify gaps in the existing literature on lattice-based cryptography
- To identify the future directions

Research Questions:

This review addresses the following research questions.

- What is the current landscape of lattice-based PQC?
- What mathematical hard problems are used in the lattice-based schemes?
- What are the gaps in the existing literature on lattice-based PQC?
- What future directions can be pursued to address the identified gaps?

E. SIGNIFICANCE OF THE STUDY

The significance of this work lies in its contribution to the field of cryptography by systematically identifying prior work on lattice-based cryptosystems, identifying research gaps, exploring mathematical hard problems used in the schemes, and suggesting future directions.

F. STRUCTURE OF THE PAPER

The rest of the paper is structured into several key sections:

Section II introduces the fundamentals of lattices, the main hard problems such as the SVP and LWEs, and presents different construction methods of cryptographic primitives from lattice-based schemes. Section III presents an overview of existing surveys and systematized literature reviews on lattice-based PQC algorithms. Section IV elaborates on the research design and selection criteria for algorithms, the experimental setup, and the methods used for data collection and analysis. Section V gives a descriptive summary of the studies included, presents the main characteristics of the studies in tables or figures, groups the identified lattice-based algorithms in meaningful categories, gives a brief description of the algorithms' constructions, provides a synthesis of performance metrics and discusses major findings, improvements, and optimization. Section VI explains the findings, points out any shortcomings, and suggests future lines of inquiry for lattice-based cryptography research. Last but not least, Section VII summarizes the key findings and talks about the contributions made to the area, and emphasizes how important lattice-based PQC is for safeguarding data against quantum attacks.

II. FUNDAMENTAL CONCEPTS OF LATTICE-BASED PQC ALGORITHMS (BRIEF OVERVIEW)

Given a vector space $\mathcal{V}$ over the real numbers and n linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathcal{V}$, the lattice Λ is defined as

$$\Lambda = \left\{ \sum_{i=1}^{n} k_i \mathbf{b}_i : k_i \in \mathbb{Z} \right\},$$

where n is the dimension of $\mathcal{V}$, and the vectors $\mathbf{b}_i$ form a basis for the lattice. This implies that every point in Λ can be written as an integer linear combination of these basis vectors [15]. Thus, Λ is discrete and extends infinitely in all directions,consistent with physical and mathematical applications.

Lattices are the fundamental mathematical objects in this area and are applied in many various areas, especially cryptographic security systems that are based on them.

Lattice-based cryptographic schemes depend on a variety of hard mathematical problems, believed to be hard even for quantum computers. Some of the hard problems related to lattices are:

- The SVP focuses on identifying the non-zero shortest vector within the lattice. Solving this problem becomes computationally hard, particularly in higher dimensions. This hardness establishes SVP as a basic problem in PQC [23], [24].
- The CVP wants to solve for the closest lattice point to any given target point in the lattice. Like SVP, solving CVP problems is harder for higher dimensions. i.e., CVP and SVP are NP-hard problems [23], [24], [25].
- LWE is a mathematical problem, focusing on the challenge of recovering a hidden vector (solution) from noisy linear equations. The hardness of solving LWE is considered even against polynomial-time algorithms and has become a basis for PQC schemes [24], [26], [27].
- Ring-LWE is a variant of LWE that operates over polynomial rings. The algebraic structure enables higher computational efficiency while preserving cryptographic security. This balance of efficiency and robust security has made Ring-LWE a foundation of lattice-based cryptography [28], [29].
- Module-LWE (MLWE) is an extension of the LWE to module lattices, algebraic structures that generalize both ideal lattices (used in Ring-LWE) and standard lattices. MLWE is also the problem of solving noisy linear equations over polynomial rings (modules).

It becomes one of the foundations for lattice-based cryptography [30].

III. RELATED WORKS

To contextualize this systematic literature review (SLR), a set of related studies has been studied thoroughly and referenced. These related works provide valuable insights into existing methodologies, research trends, and thematic focuses relevant to lattice-based cryptography. By analyzing their scope, focus, and limitations, we identify where our review aligns with and diverges from previous research.

[31] Bandara et al. explored lattice-based cryptosystems, especially the LWE problem, and discussed existing implementations, focusing on their practicality and performance metrics. The authors compared various LWE-based cryptosystems. They found that the standard LWE approach provides strong security. However, the ring-LWE variant is much more efficient; it cuts down on key size and computational complexity. The study also evaluated practical lattice-based schemes, including Crystals-Kyber, Frodo, and LAC, with a focus on their performance and adherence to the NIST PQC standards. The authors discovered a significant limitation which prevents LWE from working in practical lightweight systems. The public key size of LWE systems exceeds that of classical RSA cryptosystems which use smaller public keys. Research must focus on developing unstructured lattice-based cryptographic schemes that enhance their operational speed and deployment capabilities. The implementation of lattice trapdoors enables simpler applications but developers must solve the challenge of adding new methods to lattice-based systems. The authors proposed two main directions for future work on lattice-based schemes which involve performance enhancements and broader implementation possibilities. Researchers should focus on developing new methods which minimize key sizes while maintaining cryptographic system security.

[20] Wang et al. performed a detailed evaluation of lattice-based cryptography to prove its fundamental position in PQC. The authors reached their objective through their research on cryptanalytic method identification and design principle development and their explanation of mathematical lattice problems (SVP and CVP) which serve as security bases.The authors reviewed a wide range of LBC literature. Their work also included an exploration of algorithmic designs for KEMs and an analysis of established frameworks, like the LWE encryption schemes. The authors explained how traditional public key cryptosystems face quantum threats while confirming lattice-based cryptography depends on hard computational problems for its security. The authors conducted a review to answer essential research questions about lattice-based cryptography by defining its mathematical basis and studying its vulnerability to cryptanalytic attacks. They compared the efficiency and key sizes of lattice-based schemes against traditional public key algorithms. However, the authors did not fully explore the challenges or open problems that persist in the field of lattice-based cryptography.

[19] Sabani et al. reviewed the lattice-based cryptosystem literature aimed at enhancing the security of Quantum Key Distribution (QKD) systems, with the goal of developing robust PQC algorithms systematically focusing on lattice-based protocols. They included theoretical and experimental investigations regarding QKD vulnerabilities, particularly showing how practical implementations might have flaws falling short of theoretical security, owing to detector and optical fiber issues. The authors have shown that non-Markovian dynamics have been incorporated and shown to improve eavesdropping detection and localization, thereby enhancing overall security. Developments in post-quantum algorithms are still underway and require further research and promising advanced QKD protocols while exploring attack vectors and improving cryptographic efficiency. Lattice-based systems such as NTRU, LWE, and Goldreich–Goldwasser–Halevi(GGH) are found to be very robust against quantum attacks and provide a wide spectrum of cryptography primitives, yet they also seem to have some trade-offs between security and efficiency, and may theoretically harbor some possible flaws in the model. Evaluating these systems and their security in the quantum age involves looking directly at their defenses against quantum threats, measuring speeds, encryption performances, and conducting implementation tests that will ensure resilience.

[2] Wahlang and Chandrasekaran conducted a systematic review of literature relative to post-quantum lattice-based cryptography, which dealt with the flaws of existing cryptographic systems, impacted by the introduction of quantum computers. To this end, the authors reviewed twelve papers relevant to the area to assess the performance and security of various lattice-based schemes, addressing major research questions regarding their implementation and applications in comparison to one another and classical cryptographic systems. The paper presented comparisons of the chosen lattice based cryptographic algorithms. For digital signatures, Crystals-Dilithium is regarded as the best scheme due to its performance advantages over Falcon. In terms of PKE, Crystals-Kyber is preferred for its efficiency and security strength. For KEMs, NTRU outperforms Kyber in encapsulation and decapsulation speed, but Kyber is more efficient in key generation, making the best choice dependent on specific use cases and requirements. The authors suggested more comparisons of additional lattice-based schemes against recognized standards with persistent testing. That might involve comparing their performance metrics, security levels, and implementation feasibility on various platforms. Hybrid schemes enhanced by the different lattice-based schemes' strengths might achieve further efficiency and security for certain practical applications.

[32] Liu et al. provided a detailed classification of digital signatures based on lattice structures to prepare the

field for a future where quantum computers could challenge current methods and to serve as a key resource for ongoing studies in both the theory and practice of digital signatures.In their work, the researchers went through earlier studies on lattice-based digital signatures. They discussed how these systems are built on mathematical lattices, the kinds of security guarantees they offer, and how they stack up against traditional cryptographic methods. The review also pointed out how important lattice cryptography is for the post-quantum era and took a closer look at several signature schemes that use the hash-and-sign technique. They also explored specialized lattice-based digital signature schemes, including group, ring, blind, and proxy signatures, along with their practical use cases in real-world applications. The authors did not explicitly highlight any limitations or unresolved questions in their work. However, the review outlined multiple intriguing paths for upcoming studies, including the fusion of homomorphic signatures with secure multiparty computation—a strategy that could facilitate joint data processing without compromising confidentiality. An additional avenue involves investigating the integration of quantum cryptography and post-quantum cryptography to develop fully robust security frameworks.

[33] Nguyen et al. gave a solid Survey on lattice-based post-quantum crypto. They Focus into the math, the algorithms, and how it all runs on different hardware—CPUs, GPUs, FPGAs, ASICs. A big part was splitting things up by NTT techniques, since those speed up the polynomial math that lattice schemes rely on. It's a clean way to line up and compare the different designs out there. They covered the core theory well: LWE, SIS, and how the choice of polynomial rings (NTT-friendly or not) changes real-world performance. For each platform, they broke down speed, memory use, and power draw. Security wasn't ignored. They pointed out side-channel risks—timing attacks, power analysis—and listed fixes tailored to each kind of hardware. They also stressed writing code carefully to avoid leaks. On the practical side, they tied lattice PQC to things like TLS, and spotlighted standards: Kyber for key exchange, Dilithium for signatures. For what's next, they flagged four main areas: faster algorithms, better and more flexible hardware, stronger side-channel protection, and smoother fit with current systems. Overall, it's a strong bridge between theory and real deployment in quantum-safe security.

The reviewed papers collectively explore a wide array of topics within lattice-based cryptography, reflecting its increasing significance in the post-quantum era. They cover foundational concepts such as the SVP, CVP, and algorithmic structures like LWE, while also comparing lattice-based schemes to classical public-key systems.

Works like [31] and [33] focused on specific areas, such as digital signatures, including group, ring, and blind variants, or on practical implementations of encryption and KEM schemes like Crystals-Kyber, Dilithium, FrodoKEM, and NTRU, emphasizing performance, security, and adherence to NIST standards.

Sabani et al. [19] conducted a distinctive study on lattice-based cryptography applied to the enhancement of QKD, providing experimental analysis of its vulnerabilities and suggesting possible improvements.

Additionally, the papers [2], [19], [20], [31] and [33] do not systematically identify new lattice-based schemes other than NIST's finalists, and also they do not suggest how to address trade-offs between security and efficiency, leaving key questions open.

In contrast to the reviewed studies, our systematic literature review addresses several of the key limitations previously identified. Unlike earlier works that lacked a structured gap analysis or failed to highlight unresolved challenges, our review explicitly describes the open research questions within lattice-based cryptography and identifies new schemes. Furthermore, our study adds value by incorporating more recent and many research papers, allowing us to capture the latest developments in the field, and also helps fill critical knowledge gaps that older reviews have left unaddressed.

IV. METHODOLOGY

For this work, we used a systematic literature review (SLR) as the main method. This let us gather, sort, and closely evaluate the current research on post-quantum cryptography (PQC). An SLR serves as an essential starting point to map out the field's present status and pinpoint gaps or open issues. Here, we adhered to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, following a clear step-by-step process to structure the review.

The main purpose of this systematic review is to assess the current state in the field of lattice-based KEMs and signature schemes. A set of 41 articles was processed in the course of the review, with 6 existing systematic reviews and 35 primary studies being included in the total. The literature search was covering the duration 2020 to 2025.

The cutoff was chosen because the period following 2020 marks significant progress in post-quantum cryptography research, particularly in response to the NIST PQC Standardization process. Therefore, restricting the review to studies published from 2020 onward ensures a focus on the most current and relevant developments in the field. The five major databases: Scopus, Web of Science, IEEE Xplore, SpringerLink, and the IACR ePrint archive served as sources for the search.

A. SEARCH STRATEGY

In this review, we gathered journal articles and conference papers from five trusted sources: Scopus, Web of Science, IEEE Xplore, SpringerLink, and the IACR ePrint archive. We picked these databases for their strong fit with the topic. To find the right material, we built a custom set of search terms and phrases. These terms were designed to explore the relationships between lattic-based cryptography, lattice-based cryptosystems, lattic-based schemes, and the cryptanalysis of these schemes.

The selected search terms have addressed comprehensive research works on lattice-based cryptosystems.

The search strategy combines a comprehensive multi-database approach with a precise controlled search query.

Search Query Design

The initial query is:

("lattice-based cryptography" OR "lattice-based cryptosystems" OR "lattice-based schemes")

AND

("cryptanalysis of lattice" OR "cryptanalysis of lattice-based schemes")

AND

("post-quantum cryptography")

Search String Refinement:

We adjusted the query to match each database's rules and added synonyms to catch more relevant papers. The final search string grouped three core ideas so every hit had to cover all of them:

- Lattice-based: Identifying the underlying mathematical problem.
- Cryptanalysis/Schemes: either breaking or building new algorithms.
- Post-Quantum: tied to the main security target of the whole review.

The search was executed by a pair of primary reviewers and independently verified by another pair of reviewers to ensure the precise application of the query and the correct chronological limits within each database. Any discrepancies were discussed collectively until consensus was reached.

B. INCLUSION AND EXCLUSION CRITERIA

We set clear inclusion and exclusion rules to keep only high quality, relevant research papers were selected. These criteria are summarized in Table 1.

TABLE 1. Inclusion and Exclusion criteria.

Criterion	Inclusion	Exclusion
Topic	Articles focusing on lattice-based KEMs, signature schemes, or their cryptanalysis in the post-quantum context	Articles focusing on non-lattice post-quantum schemes (code-based, isogeny-based, multivariate), or general cryptography not specific to the lattice-based approach
Study Type	Primary research studies (new scheme proposals, cryptanalysis) and existing systematic reviews	Editorials, book chapters, and short conference abstracts without full papers
Timeframe	Publications dated from 2020 to 2025	Publications outside the specified date range
Language	Articles published in English	Articles in other languages

C. STUDY SELECTION

The process for selecting studies was based on a structured approach consisting of different screening stages and was thus compliant with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines.

1) Duplicate Removal: All retrieved records from the five different databases were brought together in Mendeley, a reference management software. Both automated and manual checks were carried out to spot and take away papers that had been retrieved more than once.
2) Title and Abstract Screening: The remaining articles that had unique titles and abstracts were reviewed by two independent reviewers using the Inclusion and Exclusion Criteria. Any differences in their opinions were first addressed through discussion and then by the involvement of a third senior reviewer. The articles that were found to be unrelated at this stage were not included.
3) Full-Text Review: The articles that got through the title and abstract screening were then proceeded to full-text retrieval. The two independent reviewers were responsible for a very detailed study of each article's full text. The final inclusion decision was based on the meticulous application of all inclusion/exclusion criteria (confirming the focus on KEMs or signatures and the specific lattice context). All disagreements were settled through consensus or third person involvement.
4) Reference List Screening (Snowballing): The reference lists of all included review papers (the 6 identified articles) and primary studies were manually screened to identify any missing but highly relevant articles that were not found during the database search, which were then subjected to the same screening process.

We began our screening with 1,625 papers retrieved from five databases. The first step involves removing 327 duplicates. In doing so, we retained the record on the Scopus database and removed those on the other database(s) whenever a record is found in multiple databases. This step resulted in 1,298 papers. Then, screening based on title, we narrowed this down to 370 papers. These 370 papers were used for further screening based on their abstract and full-text reading. A consensus approach, with a panel of three researchers, has been used to decide the screening of papers in each of the screening phases. As shown in the figure, a consensus approach was used to screen papers at each stage — title, abstract, and full-text review. Any discrepancies were discussed collectively until a consensus was reached. Finally, 41 papers were selected for an in-depth analysis. This process followed the PRISMA model, as illustrated in Figure 1.

D. DATA EXTRACTION

A structured data extraction form was developed to systematically gather essential information from the studies included in the SLR. This form is used to gather detailed metadata, such as the article title, authors, publication year, journal or conference name, and DOI for reference management. Additionally, it records the objectives, research

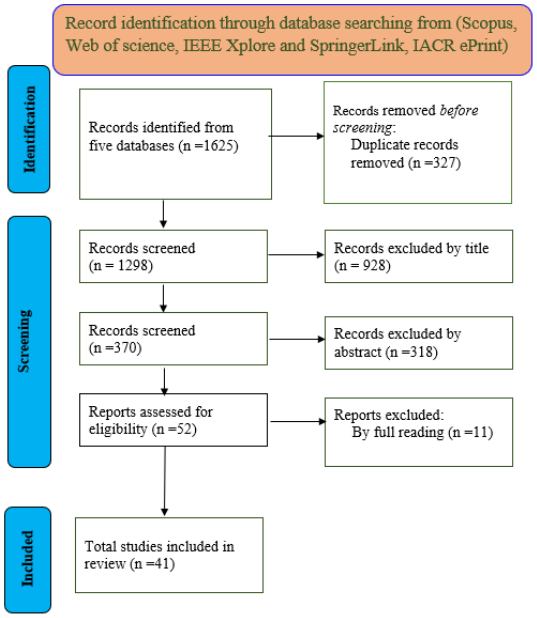

FIGURE 1. PRISMA flow diagram of the SLR.

methodologies, significant findings, and future directions related to lattice-based cryptosystems. The form also shows which research questions were tackled in each paper. Using this method helped us review lattice-based cryptosystems in a clear and complete way. It also made it possible to see the strengths and limitations of every study and to point out areas where future work could build further. This organized approach ensures that the literature review is complete, clearly structured, and in line with the main research objectives. bringing together existing knowledge and provides direction for future studies.

We used a standardized and examined data extraction form to gather specific and relevant information from the studies we included. The form covered the following sections:

- Bibliographic Details: Author(s), Year of Publication, Journal or Conference name, and DOI
- Objectives
- Research Methodologies
- Study Type: Primary study (scheme proposal, cryptanalysis) or Systematic Review
- Cryptographic Primitive: KEM or Signature Scheme.
- Specific Scheme Name: (Kyber, Dilithium, Falcon, etc.)
- Main Results: Security and performance enhancements (speed, key/ciphertext size), or the outcome of cryptanalytic attacks.
- Future Directions

Although this SLR provides comprehensive insights, it has certain limitations. First, the review included 41 primary studies, which may not fully capture niche or emerging works outside the five considered databases. Second, there may be a publication bias, as most included studies report positive outcomes, while unpublished or negative findings might have been excluded. Future research could broaden the search scope and incorporate grey literature to minimize such biases.

E. QUALITY ASSESSMENT METHOD

The primary studies that were included in the review were evaluated in terms of their methodological quality and reliability, and this approach was adopted so as to prepare the ground for the synthesis and interpretation of the findings.

1) Tool selection: A quality assessment checklist custom designed for the purpose was created, focusing on the following main points of the cryptographic rigor:
   - Clarity and Completeness: Is the scheme given in great detail with all parameters?
   - Cryptanalysis: Is the cryptanalysis or the attack claims documented with evidence?
   - Reproducibility: Is the detail of application that is required for reproduction sufficient?
   - Comparative Analysis: Is the scheme/cryptanalysis compared rightly against the literature?
2) Assessment process: The custom checklist was applied by two reviewers independently to each primary study. Discrepancies were resolved either through agreement or by bringing in a third reviewer.
3) Synthesis integration: The quality assessment results were used to assign evidence levels to the studies accordingly. Studies rated as high quality were given more weight in the final synthesis.

V. RESULTS

A. OVERVIEW OF INCLUDED STUDIES

Figure 2 displays the number of publications by year. The analysis shows that while fifteen of the total papers are journal articles, the remaining twenty-six papers are conference papers.

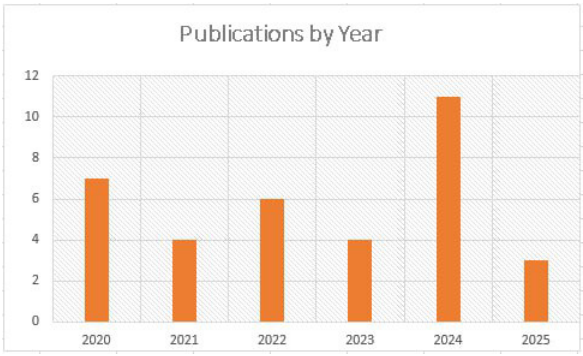

FIGURE 2. Number of Publications by Year.

The databases considered in our review consist of five sources: Scopus, IEEE, WoS, SpringerLink, and the IACR ePrint archive. The publications extracted from each database are shown in Figure 3. The number of publications extracted from the Scopus database appears higher because, whenever duplicates are found, only the publications from the Scopus database are retained.

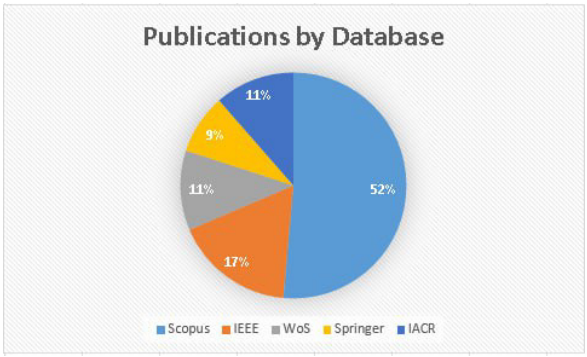

FIGURE 3. Number of Publications by Database.

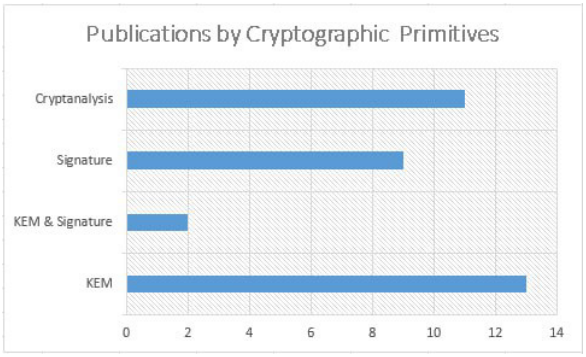

FIGURE 5. Cryptographic primitives.

The underlying hard problems used in the studies include short integer solutions, CVP, SVP, LWE, and their variants. Particularly, these hard problems are: RLWR [34], MLWE & MSIS [35], [36], [37], RLWE & RLWR [38], CVP & SVP [39], [40], [41], [42], [43], [44], [45], [46], [47], RLWE & RSIS [48], LWE [26], [49], [50] & [51], NTWE [52], MPLWE & PLWE [53], RLWE [54] & [55], SVP [56]. Figure 4 shows the details of the underlying mathematical hard problems.

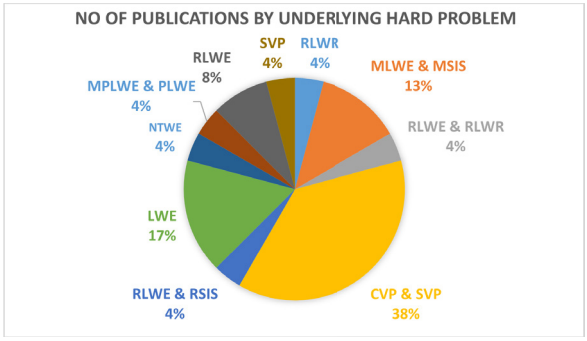

FIGURE 4. Underlying Hard Problems.

Regarding the cryptographic primitives addressed in the reviewed papers, Thirteen papers proposed the majority of schemes for KEMs [26], [34], [38], [39], [40], [43], [46], [49], [50], [51], [52], [54], [55]; nine papers developed schemes for signature [36], [37], [41], [42], [44], [45], [47], [48], [53]; and two papers designed schemes for both KEM and signature [35], [56]. The remaining eleven works dealt with cryptanalysis. Figure 5 shows the number of publications by cryptographic primitives used.

B. NARRATIVE REVIEW OF INCLUDED STUDIES

The reviewed papers mainly focused on KEM and signature schemes, and cryptanalysis. The papers can be categorized based on the cryptographic primitives they aimed to address in KEM schemes, signature schemes, both KEM and signature schemes, and cryptanalysis.

1) KEMs

[34] Park et al. proposed a KEM based on a new ring structure using cyclotomic trinomials to enhance PQC. The proposed KEM is designed to be secure against chosen-plaintext attacks (CPA-secure), and it employs the Fujisaki-Okamoto transform to ensure security against chosen-ciphertext attacks (CCA-secure). The authors dealt with a 128-bit classical security level by selecting appropriate parameters and compared their implementation results with the KEMs NewHope, LAC, Round5, Saber, and Kyber. The proposed KEM results in shorter secret keys and ciphertexts, while maintaining negligible decryption failure rates without the need for error correction codes.

[38] Jung et al. proposed a new and original KEM LizarMong, which leverages ring-LWE and ring LWE rounding (RLWR), focusing on optimization from various perspectives. To achieve this, the researchers studied and examined the leading NIST candidate algorithms, synthesizing the strengths of each. After developing this new scheme, they conducted a security analysis, confirming that it maintains security under the IND-CPA framework of the IND-CPA PKE variant of LizarMong, based on the assumption of RLizard's IND-CPA security. They compared their scheme with other approaches, evaluating multiple factors including security, correctness (decryption failure probability), capacity (size of encrypted text and public key), and performance (CPU processing cycles for encryption, decryption, and key generation) in comparison to RLizard and NIST's candidate algorithms. Their scheme, termed LizarMong, stands out as the most advanced key encapsulation algorithm within the RLWE framework at that time.

[46] Hajaje et al. combined the benefits of NTRU with MATRU, a version of NTRU, to theoretically explore the PMTRU cryptosystem. A comparison of PMTRU, NTRU, and MATRU carried out by the authors. Consequently, they have demonstrated that while PMTRU's encryption and decryption speeds are comparable to those of MATRU, PMTRU's speed is $K^{(4-\log_2(7))}$ times quicker than NTRU's. Additionally, PMTRU significantly increases resistance to lattice-based and brute-force attacks in comparison to NTRU

and MATRU. Furthermore, PMTRU requires less memory to encode ciphertext and public keys than MATRU and NTRU, which lowers message security costs.

[39] Abo-Alsood and Yassein. present an improved design of an NTRU PKE scheme based on a Qu-Octonion subalgebra for enhanced security and efficiency. The security level of QOTRU is higher than that of OTRU for key security, while the message security level remains the same for both systems. The challenges highlighted include practical realization and integration of Qu-Octonion algebra into systems as issues relating to scalability in larger datasets or other computing provisions. Future works will include a better study of QOTRU security, improvement in key generation, encryption/decryption process, and applicability of this scheme in more secure communication, digital signatures.

[50] Wang et al. introduced a variant of the LWE problem called Learning With Modulus (LWM). This variant can be thought of as erasing the higher-bit information of the inner product of the secret vector and the random vector, in contrast to LWR, which can be regarded as erasing the low-bit information of the inner product. The authors proved the reducibility of LWM from LWE. An algorithm that can solve either Search-LWM or Decision-LWM can also solve Search-LWE. This led to the development of a PKE scheme that significantly decreases the ciphertext size. The authors compared the encryption processes with Lindner–Peikert and Lizard schemes, emphasizing the trade-offs between ciphertext sizes and encryption speeds. For a 128-bits plaintext, the proposed scheme achieved a 46.43% reduction compared to the Lindner–Peikert scheme and a 28.57% decrease relative to the Lizard scheme, keeping comparable decryption speed of only 0.015 ms longer than the LP scheme and other performance metrics.

[40] Kundu et al. examined strategies to enhance public key compression and performance of polynomial multiplication in the NTRU-NTT architecture, a lattice-based encryption mechanism intended to be resistant to quantum attacks. Their work identifies and addresses flaws in earlier hybridized NTT-Karatsuba methods by introducing a mathematically validated approach to decrease the prime modulus q. That plays a crucial role in reducing public key size without compromising security guarantees. The authors report significant reductions in key sizes and computational efficiency compared to earlier work by evaluating their framework against existing NTRU-NTT implementations. The results show notable advancements in implementing high-dimensional lattice frameworks, addressing a key challenge in current NTRU-NTT methodologies.

[49] According to Boudgoust et al., the PV-LWE, and its associated dec-PV-Knap issues, related to key recovery attacks on PASS Encrypt were examined. It will be proved that the solution to dec-PV-Knap will give a solution to an approximation of PV-LWE, thus making an easy inter-reduction between both problems. The authors suggest that modifications to PASS Encrypt ensure a smoother transition from deterministic to probabilistic design, enhancing the latter stage with partial Vandermonde transforms. They consider the security of PV Regev Encrypt concerning to key and recovery attacks and plaintext recovery based on hints. Here, the public key is based on PV-LWE, and the encryption masks the message with the random vector in accordance with Regev's design. The organization of the transformation matrix provides protection against attacks; however, it also ties the complexity of solving associated problems, especially in key recovery attacks that exploit the relationship between $\mathbf{b}$ and $\left(V\Omega^T \cdot \mathbf{s} + \mathbf{e} \mod q\right)$.

[55] Jin et al. offered strong steps in the PQC discipline via a new key encapsulation method upon the E8 lattice. The authors emphasized the best sphere packing density of the E8 lattice by first considering the LWE and Ring-LWE problems, which are believed to be resistant against quantum attacks. Since this density renders efficient encoding and decoding and also improves error correction capabilities, all these features need to be secured in adversarial conditions in the age of quantum computing. Extending the E8 lattice-based AKCN framework to an efficient key exchange, method, which is expected to even more efficient than NewHope-KEM is interesting. One strong point about AKCN-E8 is that its shared-key size is twice that of NewHope-KEM, which is beneficial from the standpoint of being resistant to quantum lookup via Grover's algorithm, which reduces the effective security of symmetric keys by half. AKCN-E8 is a suitable candidate to serve as the foundation of safe communications because of its factor of two property, which seems to act as a buffer against future developments in quantum cryptanalysis. Furthermore, it allows for more compact ciphertexts, which enhances transmission efficiency and improves storage without compromising or even raising security. The system's flexibility in parameter choice allows it to be set by the user for given security requirements and targeted error rates. The best authors emphasize the requirement to adapt to the changes in the cryptographic threat landscape, especially as the power of quantum threats increases. There they lay their position on the need for resistant cryptography systems. In short, AKCN-E8 not only tries to stand out as a theoretical concept but also does so practically, having certain advantages over existing schemes that allow it to be the strongest in security, efficiency, and adaptive means against quantum threats in the future.

[52] Gärtner articulated the NTWE problem, which is resilient against dual lattice attacks, but lends itself more favorably to primal lattice attacks. He contrasts the methods of key generation concerning decryption error probabilities and the scheme's security against NTRU and ring-LWE.

The two main attacks on the LWE scheme, which have been identified, are primal and dual lattice attacks, where in primal attacks, NTWE is more efficient than others. The NTWE problem, on the other hand, maintains its hardness for all parameters set, unlike NTRU. The paper also discusses the expected hardness of Core SVP concerning Kyber's parameters. The NTWE-based system is compact

and flexible, where public keys increase linearly with module rank, granting strong resistance against dual attacks. The dependability of both attacks must be investigated against the hardness of the NTWE problem for particular applied parameters.

[43] Jonghyun Kim and Jong Hwan Park developed $NTRU^{+}$, which is an update to the NTRU encryption scheme and aimed at achieving efficiency and security in KEMs. The authors try to tackle the weaknesses of the classical NTRU by giving two new transformations, $ACWC_2$ and $FO^{\perp}$, together with a simple encoding scheme called semi-generalized one-time pad (SOTP). The combination is supposed to allow efficient message sampling and chosen-ciphertext security without ciphertext re-encryption, thus providing an optimal encryption process. They provide a comprehensive performance analysis of NTRU+ as compared to known lattice schemes, namely NTRU and KYBER. It has been shown that in terms of execution time and security levels against problems of LWE and NTRU, NTRU+ appears preferable. The results demonstrate that NTRU+ can provide improvements of operational performance while being secure, hence putting itself in quite close competition in the domain of PQC.

[26] Sabani et al. proposed a new efficient variant of LWE cryptographic scheme. The proposed variant incorporates a mapping function that transforms the secret key S with a matrix A, which enables matrix operation in key generation. This transformation allows for parallel processing that preserves both efficiency and security without adding complexity. The paper suggested future research direction, emphasizing the implementation and comparison of different proposed variants as well as investigation of potential vulnerabilities on the cryptographic schemes to enhance their resilience against potential attacks.

[51] Liang et al. proposed the Ternary and Binary Encapsulation Ring (Tyber) a KEM based on trinomial cyclotomic rings, to tackle the inflexibility in choosing parameters for MLWE-based schemes using power-of-two cyclotomic rings, which is a variation of the NIST-standardized Kyber scheme. In reality, the scheme achieved 129, 197, and 276 bits of the desired quantum security levels of 128, 192, and 256 bits. After developing it, they analyzed its security and proved that the PKE system is secure against IND-CPA and that the KEM scheme is safe from IND-CCA. Finally, they demonstrated that Tyber has stronger security levels by 22, 31, and 44 bits compared to Kyber, which achieves 107, 166, and 232 bits.

[54] Homsi et al. propose a new post-quantum cryptographic key generation mechanism that combines the Ring RLWE problem and Elliptic Curve Cryptography (ECC). The goal of this hybrid strategy is to counter the dangers that quantum computing algorithms such as Shor's and Grover's pose to existing RSA and ECC systems. The usages of KECCAK hash functions, to convert ECC keys more specifically, the secp256r1 curve into polynomials suitable for RLWE schemes. The paper describes the process for creating the RLWE lattice ring (R), the public key components A(x) and B(x), the secret key S(x), and the error term e(x) to ensure security aspects of RLWE encryption and compliance with the mathematical structures. The efficiency and feasibility of this combined ECC-RLWE technique as a robust PQC solution are demonstrated by performance analysis, which is measured by CPU cycle usage and key generation time.

Innovative designs that enhance security against novel quantum threats are the focus of recent advancements in PQC and KEMs. A noteworthy contribution is a KEM that uses cyclotomic trinomials to increase security against CPA and CCA. This preserves the dependability of decryption while enabling shorter secret keys and ciphertexts. NewHope and LizarMong distinguish themselves from well-known KEMs such as Kyber by combining ring-LWE and ring learning with error rounding (RLWR), optimizing performance through careful parameter selection, and attaining low decryption failure rates. Tyber achieves higher quantum security levels while addressing parameter flexibility and offering robust defense against attack vectors.

Furthermore, a hybrid mechanism that combines RLWE with elliptic curve cryptography to thwart threats from quantum algorithms, while QOTRU utilizes Qu-Octonion algebra for increased security and efficiency. Despite these developments, there are still issues with scalability and practical implementations, which calls for more investigation into security flaws and the schemes' wider applicability in secure communications. All of these advancements work together to provide a solid basis for robust cryptographic systems in the changing post-quantum environment.

2) SIGNATURE

[37] Ravi et al. researched Dilithium, which has the underpinnings of the famous Fiat-Shamir with Aborts framework. They engaged in the process of algorithmic optimization of Dilithium by presenting the optimized signing process in Dilithium for software implementations on the prevalent Intel Core i5-4460 and ARM Cortex-M4 CPUs. The proposed optimization reduces computations on rejected iterations by letting, the conditional checks evaluated earlier. Inlining, unrolling, etc. had been implemented to speed up signing further. They also provided thorough evaluation results related to the performance improvement and memory requirements for the pre-computed intermediates. The optimized signing procedure gives speed increases up to 31% against all updated parameter sets of Dilithium on the Intel Core i5-4460 CPU. Finally, they also contributed to getting the fastest software results out of it for ARM Cortex-M4F by improving the open-source implementation available in the pqm4 library, giving speed improvements between 6% and 35%.

[36] The digital signature scheme SKCN was developed by Gong et al. is an extension of the existing Dilithium scheme that relies on module lattices. Salient features include increased computational efficacy, bandwidth, and the modular nature of supporting numerous parameter configurations-all under the maximum post-quantum security

against adaptive chosen-message attacks. Parameter optimization yields smaller public and secret keys. For instance, SKCN-II produces a public key of 1312 bytes and a signature of size 2573 bytes. These are more compact than the corresponding sizes for Dilithium-III. Besides, SKCN-II also exhibits better efficiency in computation during key generation, signing, and verification. Thus, SKCN is the secure, efficient, and flexible for specific applications, which would be relatively more complicated because of required higher repetitions for the signing algorithm concerning parameter choices.

[48] Sharafi and Daghigh introduced a lattice-based digital signature based on the Lindner-Peikert cryptosystem, specifically by combining Ring-LWE and a Ring-SIS problems. It achieves post-quantum security with compact key and signature sizes (1-1.5 KB). The security is rigorously proven in the QROM with cryptanalysis conducted using methods from Aggarwal et al. and Chen et al. The focus is on differentiating between decoding, primal, and dual attacks. It also balances security and efficiency by achieving security levels up to 92 bits, with comparisons to other Ring-LWE schemes indicating competitive key and signature sizes. It achieves UF-CMA security in QROM, with public key sizes of 826-1032 bytes and signature sizes of 1255-1565 bytes.

[53] Zhang et al. proposed a lattice-based digital signature scheme to withstand threats from quantum adversaries. The authors present a variant of Lyu's signature scheme by integrating the middle-product operation and combining it with a quantum-safe chameleon hash function. To validate the feasibility and security of the proposed scheme, they conducted rigorous theoretical analysis and provided a formal security proof based on the Middle-Product-LWE problem. The construction is proven to be existentially unforgeable under adaptive chosen-message attacks (EUF-CMA) within the Quantum Random Oracle Model (QROM). Although the integration of the middle-product operation slightly increases computational complexity, it significantly enhances resistance to quantum threats. By offering stronger security guarantees than many existing QROM-based schemes, this work marks a meaningful advancement in the field of PQC. Furthermore, it lays a solid theoretical foundation for developing more advanced primitives, such as identity-based and blind signature schemes in a quantum-safe context.

[47] Espitau et al. developed various techniques to reduce the signature size of lattice-based signatures focusing on hash- and-sign lattice-based signatures over NTRU lattices. Their techniques are based on various features of Gaussian vector encoding, Gaussian sampling, and parameter selection. According to the authors, when applying these techniques to Falcon, one can reduce the signature size by 30-40% at the cost of a few bits of security loss. In addition, authors showed that the Gaussian vectors in signatures can be represented in a more compact way with appropriate coding-theoretic techniques, improving signature size by an additional 7 to 14%.

[41] Kumar et al. proposed a non-commutative version GR-NTRU over the group ring that is based on the dihedral group of order 2N. To enhance the efficiency and security of NTRU, different variant exists; among these, the variant over the ring of Eisenstein integers appears to perform better than NTRU. In this work, they analyzed and conducted an experimentation on a 12th Gen Intel(R) CORE(TM) i9-12900K 3.20GHz and 64GB RAM in Windows 11 Pro (64-bit) operating system to determine the size of the key space for the new NTRU variant. The proposed scheme is compared with other variants of NTRU. While the non-commutative nature of their scheme results in slower performance compared with standard NTRU, it demonstrates improved speed over other non-commutative variants. Concerning lattice attacks, the most prominent attack on NTRU-like cryptosystems, the proposed variants are resilient in comparison to the other considered non-commutative schemes.

[42] Cheon et al. proposed Hyperball bimodAl modulE rejecTion signAture schemE (HAETAE), a new lattice-based digital signature technique that prioritizes a balance between complexity and compactness, making it ideal for environments with limited resources.

Similar to the NIST-approved Dilithium scheme, HAETAE employs the Fiat-Shamir with Abort methodology. This leads to considerable reductions in size-up to 39% for signatures and 25% for verification keys compared to Dilithium, allowing signatures to fit within a single TCP or UDP datagram while ensuring robust security against various threats. HAETAE effectively combines the strengths of the Dilithium and Falcon schemes to uniquely integrate key generation and rejection sampling. The authors also provided a portable, constant time reference implementation, as well as optimized versions that utilize Advanced Vector Extensions 2 (AVX2) instructions and a minimized stack size suitable for Cortex-M4 processors. Additionally, they outline methods to protect HAETAE from implementation attacks, including side-channel analysis, positioning it as a promising solution for IoT and embedded systems.

[45] Lee et al. introduce a new distribution called Generalized Centered Binomial Distribution (GCBD) to replace the bimodal discrete Gaussian distribution used in lattice-based signature schemes like BLISS. While BLISS significantly improved rejection sampling efficiency, its use of a transcendental probability mass function made it vulnerable to side-channel attacks due to difficulties in constant-time integer implementation. GCBD, a generalized form of the centered binomial distribution, allows for simpler, more efficient and constant-time sampling using only integer operations. This helps to prevent side-channel vulnerabilities. Although the proposed GCBD variant of BLISS is about 3.3 times slower than GALACTICS, a previous constant-time implementation, the authors suggest that GCBD serves as a viable alternative for designing secure bimodal lattice signatures, particularly in consideration of the recent machine learning side-channel attacks on GALACTICS.

[44] Espitau et al. proposed a novel trapdoor generation algorithm for NTRU lattices, enhancing the hybrid sampling approach used in the Mitaka signature scheme. Mitaka was developed to address Falcon's complexity and side channel vulnerabilities, which previously suffered from lower security levels and slower key generation. The authors introduce a mathematically elegant method termed Annular NTRU trapdoor generation, which samples trapdoor vectors directly within a constrained annulus in the Fourier domain. This approach enables the generation of high-quality lattice bases that match Falcon's security levels, while maintaining Mitaka's advantages in simplicity, versatility, and implementation efficiency. Their analysis shows that this method achieves better signature compactness and improved key generation speed. Experimental findings show that the proposed approach matches or surpasses the performance and security of Falcon and Mitaka, providing a practical, well-balanced solution for hash-and-sign lattice-based signature schemes.

Recent developments in lattice-based digital signatures show important breakthroughs meant to improve PQC's security, effectiveness, and compactness. By optimizing the signing procedure for both Intel and ARM architectures, reducing computation during rejected iterations, and achieving speed improvements of up to 31% on Intel CPUs and 35% on ARM Cortex-M4F, were achieved. An SKCN, which is an extension of Dilithium, is a versatile choice for a range of applications due to its smaller key sizes and enhanced effectiveness against adaptive chosen-message attacks, and using a different strategy, Ring-LWE and Ring-SIS problems were combined to produce a compact signature scheme that ensures UF-CMA security while achieving competitive key and signature sizes and rigorous security proofs in the Quantum Random Oracle Model (QROM). Utilizing the middle-product operation and a quantum-safe chameleon hash function, a signature scheme that maintains existential unforgeability while providing a strong defense against quantum threats is also suggested. Furthermore, using sophisticated Gaussian sampling techniques reduces signature sizes, and for Falcon signatures, they were able to achieve a reduction of 30–40%. The HAETAE scheme strikes a balance between compactness and complexity, resulting in significant reductions in the sizes of verification and signature keys while maintaining strong security for environments with limited resources, and the Generalized Centered Binomial Distribution (GCBD) was proposed. to improve sampling efficiency and guard against side-channel vulnerabilities in lattice signatures. Finally, by using a new trapdoor generation technique, the Mitaka signature scheme's key generation speed and signature compactness, establishing it as a competitive alternative to other schemes, were improved. In general, these advancements highlight the continuous attempts to protect digital signatures from quantum threats while maintaining their usefulness and security.

3) KEM AND SIGNATURE

[35] Zhang et al. proposed asymmetric extensions of lattice-based cryptographic foundations, specifically asymmetric module LWEs (AMLWE) and asymmetric module short integer solution (AMSIS), aiming for size-optimized KEM and digital signature. Building on Crystals-Kyber and Crystals-Dilithium frameworks, they designed an IND-CCA secure KEM and an SUF-CMA secure signature scheme that reduces the sizes of public keys, ciphertexts, and signatures. These schemes were implemented on a 64-bit Ubuntu system (Intel Core-i7, 3.6 GHz,4GB RAM) via AVX2-optimized C code, the schemes achieve a KEM public key of 896 bytes and ciphertext of 992 bytes, and signature public key of 1312 bytes with a 2445 byte signature, all for 128-bit quantum security. The research performs security analysis that confirms AMLWE/AMSIS matches standard assumptions' hardness while enabling flexible parameterization, with significant size and speed gains over NIST Round 2 post-quantum candidates.

[56] Henry Bambury and Phong Q. Nguyen introduced a novel blockwise reduction algorithm that improves the efficiency of solving the SVP in lattice-based cryptography, especially for NTRU and hypercubic lattices. The study shows that blockwise reduction can effectively halve the required block size for solving SVP in these lattices, and for hypercubic lattices, it can relax the approximation factor to $\sqrt{2}$. This paper addresses the first provable result showing that breaking NTRU lattices can be simplified to finding shortest lattice vectors in half dimension, addressing a conjecture from Eurocrypt 2006.

The heuristic primal attack generally requires a blocksize of $\frac{n}{2} + O(n)$ for both $\mathbb{Z}^n$ and NTRU lattices. The authors further analyze this requirement and show that the inclusion of q-vectors in NTRU reduces the necessary blocksize to $\frac{4n}{9} + \frac{n}{\log n}$. Unlike previous approaches, the proposed algorithm is more general, incorporates well-defined termination criteria, and tolerates approximate-SVP procedures. These properties may enable faster solutions to problems such as the $\mathbb{Z}^n$-Lattice Isomorphism Problem (Z-LIP).

The goal of recent developments in lattice-based cryptography has been to increase security and efficiency. Building on Crystals-Kyber and Crystals-Dilithium, an IND-CCA secure KEM and an SUF-CMA secure signature scheme were developed, and the AVX2-optimized implementation outperformed NIST Round 2 candidates and achieved compact sizes for both public keys and signatures, guaranteeing 128-bit quantum security. In addition, using the blockwise reduction algorithm, the SVP for NTRU and hypercubic lattices can be solved more effectively, which offers a provable simplification for breaking NTRU lattices by reducing the necessary block size by half and relaxing the approximation factor. All things considered, these studies demonstrate notable advancements in strengthening lattice-based cryptography systems' defenses against quantum attacks.

4) CRYPTANALYSIS

[57] With the aid of the Chernoff-Cramer (CC) bound in parametrizing a new upper bound (UB), Song et al. presented an IND-CCA secure KEM based on the Ring-LWE problem, NewHope. Compared with the prior upper bound (UB), a much improved one on the decryption failure rate (DFR) is presented using constraint relaxation and union bound. When $n = 1024$, conducting comparisons for different error parameters k, it has been shown that the decryption failure rate (DFR) for various upper bounds of the scheme is less than 10^{-126}. In particular, when $k = 8$, it resulted in an improvement by more than 50 orders as compared with that of the CC bound. As k is getting larger, the computational complexity of the anticipated UB significantly rises, and calculating the desired UB is challenging. Since enhancing security and bandwidth efficiency only need minor modifications to NewHope's protocol, which make it simple to implement, have been proven by altering the compression rate of the ciphertext from 3 bits to 2 bits per coefficient. For instance, by changing the error parameter from 8 to 10, bandwidth efficiency was improved by 5.9%, and its security level was enhanced by 2.5%.

[58] A proposal called the two-step lattice reduction strategy, included in the dual lattice attack, was introduced by Qian G. and Thomas J. that improved the distinction and guess step with an innovative distinguisher. First, this algorithm improves the efficiency of solving a security parameter set among the Round-3 submissions of Crystals-Kyber and the same around Crystals-Dilithium in both core-SVP and the Random-Access Machine models. The analysis performed by them suggests some parameter sets, such as Kyber512, Dilithium-2 and Dilithium-3 have very limited security margin while others, such as Kyber1024 and Dilithium-5 frightfully close to security limits, while the Kyber768 parameter set completely misses NIST security requirements. Moreover, their techniques for lattice reduction have further improved the current primal attack in the context of the RAM model, showing some parameters close to their claimed values security levels. Specifically, they showed that Kyber768 can be solved using classical gate complexity lower than that of its claimed security.

[59] Yang et al. investigated vulnerabilities in Kyber (an NIST PQC finalist and a lattice-based KEM) to side-channel attacks, specifically by designing a chosen ciphertext correlation power analysis (CPA). Their experimental setup involves testing both the reference implementation and the pqm4 implementation of Kyber512. They demonstrated that chosen ciphertexts significantly amplify attack efficiency. As a result, the attack requires up to five times fewer traces than random ciphertexts, enabling full secret key recovery in minutes rather than days, as opposed to previous methods.

[60] Lee et al. provided a significant analysis of the NTRU+ KEM. Proposed as a post-quantum alternative in cryptography, they put forward a classical chosen ciphertext attack that breaks the claimed NTRU+ scheme is IND-CCA secure in the quantum random oracle model if the underlying NTRU encryption is OW-CPA secure, which leading to a practical attack discussed in their work. As a result, they have shown that by exploiting a few decapsulation queries, the random session key encapsulated in the NTRU+ challenge cipher text can be recovered with all but negligible probability, which shows that the desired robustness against adversarial attacks is absent. They pinpoint that the two novel transformations, ACWC2 and $FO^{\perp}$, which constitute the foundation of NTRU+'s design, are the main weaknesses in its security proofs. It has been shown that the attacker can change ciphertexts so that the session key can be recovered with a very high probability by using ambiguities in the cipher's encoding and decoding procedures. They also talk about how the original security proofs' assumptions of rigidity and injectivity were inadequate. The authors then offer a possible solution to the NTRU+ method by employing the conventional FO transformation rather than $\overline{FO}^{\perp}$, which could increase security at the expense of decapsulation time.

[61] Pursharthi and Mishra re-examined a digital signature scheme that was very recently proposed by Soni et al. While the original proposal was supposed to be a compact and efficient signature related to a lattice problem, the authors identified a serious weakness. More precisely, they prove that an attacker who succeeds in getting the signature of even one message can backtrack and reveal the signer's private key. This occurs because part of the signing procedure inadvertently leaks sufficient information for the key to be reconstructed using only basic arithmetic. Because the secret key is intended to be reused, this defect renders the whole scheme insecure in practice.

To deal with this issue, the authors recommend setup and signing procedure changes while keeping the key-generation method intact. The adjustment they made ensures that one of the signing values can no longer be reversed or mathematically undone, which blocks the key-recovery attack. The fix keeps the original advantages—mostly relatively small keys and reliance on a post-quantum lattice problem—but it does introduce slightly larger signatures.

Overall, their research shows that the vulnerability can be fixed without changing the fundamental concept of the scheme, though further work will be required to improve efficiency and decrease signature sizes in future updates.

[68] Pouly and Shen present a significant contribution to the study of dual attacks on the LWE problem—an essential hardness assumption for post-quantum cryptographic schemes like Kyber. They propose a simplified and provably secure dual attack framework that removes reliance on heuristic assumptions by using a geometric analytical approach to define the effective parameter regimes.This approach provides a cohesive theoretical framework and explains discrepancies in previous studies. Additionally, the authors create a quantum version of the attack that uses a Markov Chain Monte Carlo discrete Gaussian sampler to achieve proven speed-ups. They also offer initial

complexity estimates for possible Kyber assaults. Although their approach improves theoretical knowledge, its usefulness is constrained by the need for around $m \approx 2n$ LWE samples, which are more than are usually available in actual systems. Future work is indicated by the omission of optimizations like lattice coding and modulus flipping. All things considered, the research provides insightful information about the structural robustness of LWE and guides the choice of secure parameters in PQC.

[69] Lin et al. has studied that the Peregrine signature method, which is a high-performance version of the NIST-standardized Falcon algorithm that was submitted to the Korean PQC competition has serious security flaws. To improve computing efficiency, Peregrine substitutes a centered binomial distribution for Falcon's Gaussian sampler; nevertheless, this change compromises its proved security assurances and leaves it vulnerable to possible information leaking. These flaws are similar to those found in previous hash-and-sign methods, such as GGH and NTRUSign. The authors label this vulnerability the Hidden Transformation Problem (HTP). Building on the parallelepiped-learning approach introduced by Nguyen and Regev (2006), they integrate gradient-descent refinements proposed by Tibouchi and Wallet (2020) and decoding strategies from Prest (2023) to reconstruct approximate secret keys from signature data. Their results demonstrate full key recovery with high probability—requiring around 25,000 samples for the reference implementation and approximately 11 million samples for the official Peregrine-512 specification—achieved within a few hours on conventional hardware. This study highlights the inherent risks of employing heuristic, non-verified security mechanisms in lattice-based digital signatures. It strengthens the body of research on statistical and structural attacks in PQC and reinforces the importance of GPV-style randomization in preventing information leakage in NTRU-based systems.

[67] Bambury et al. studied the DEFI signature scheme by solving systems of quadratic Diophantine equations over rational integers. They then exposed serious security problems in the scheme that allow an attacker to extract the secret key from fewer than ten (message, signature) pairs, hence rendering the scheme highly vulnerable. In this way, their analysis shows that current security assumptions are too weak and that a stronger security framework ought to be developed to assess the scheme's ability to withstand attacks. They discussed the sublattice recovery problem with an emphasis on how lattice reduction may be applied in the context of NTRU lattices. They argue that methods of analyzing the security of lattice-based schemes might be inadequate, for they do not consider the particular weaknesses that arise in the case of the DEFI scheme. Therefore, a more comprehensive security analysis has to take into account the peculiarities of underlying mathematical structures. For the identified vulnerabilities, the authors have also proposed possible countermeasures, such as larger parameters or a change to the generation procedure of isotropic vectors. However, the authors warn that any such countermeasures would have to be carefully considered so as not to introduce new weaknesses. They proposed the importance of further investigation in lattice-based cryptography to ensure that proposed solutions do not compromise the overall security of the signature scheme.

[63] Pulles et al. present a cryptanalysis of EagleSign, a structured lattice-based Fiat-Shamir signature scheme submitted to NIST's additional post-quantum signatures round. Their research shows that the lack of rejection sampling causes the signature distribution to leak private key information, allowing full key recovery with a few hundred known-message signatures for all V_1 parameter sets. Using algebraic methods for ideal recovery and meet-in-the-middle search for sparse generators, the attack approximates secret matrix columns by taking advantage of conditional expectancies on sparse challenge vectors and ring automorphisms. Flaws in the security proofs are identified, and EagleSign- V_2 is affected by a related vulnerability that requires more signatures (up to 10^9) but is still feasible below claimed security levels, as validated experimentally. The findings draw attention to important trade-offs in lattice signature performance optimization ensuring zero-knowledge properties.

[66] Raya et al. performed a comprehensive cryptanalysis on the BQTRU cryptosystem, a non-commutative, NTRU-style scheme constructed over a quaternion algebra. They note that while most NTRU variants use commutative rings, BQTRU and others explore non-commutative structures to potentially improve speed or resistance to attacks. BQTRU was presented as a high-performance hybrid, merging the strong key security of the earlier NTWO system's lattice structure with the efficiency of QTRU's quaternion algebra to overcome decryption issues. Its designers claimed it was the fastest NTRU variant. Despite these claims, the authors uncovered critical security vulnerabilities. They specifically showed that the quaternion structure selected for performance optimization inadvertently created a weakness. Their proposed, practical ''folding'' attack exploits this structural flaw, effectively reducing the lattice dimension for key and message recovery. This attack successfully broke the parameters intended for moderate security and proved that the highest-security parameters offer significantly less protection than claimed. As a result, the authors strongly advise against deploying BQTRU currently and cast doubt on the overall practicality of similar hybrid lattice designs.

[65] Satoshi and Wang performed a security analysis of the CRYSTALS-KYBER and SABER cryptosystems, specifically targeting vulnerabilities related to randomness reuse attacks. Their research leveraged and expanded the meta-PKE model previously introduced by Wang et al. The authors established that an attacker could successfully retrieve Bob's secret randomness with a surprisingly low number of queries if he repeatedly employed the same randomness during

the encryption procedure. Their analysis provided specific figures: in CRYSTALS-KYBER, an adversary required a maximum of 4, 3, and 4 queries to recover randomness for security levels I (equivalent to AES-128), III (AES-192), and V (AES-256), respectively. For the corresponding security levels, SABER required no more than 6, 6, and 4 queries. The substantial risk posed by randomness reuse in these NIST PQC finalists was highlighted by experimental validation, which confirmed the attack success rate of 100% in all parameter sets tested. Although Okada and Wang explored that there are difficulties in putting these mitigations into implementation, they also looked at possible solutions like mandatory randomness refreshing and defenses against attacker-controlled queries. Their research fundamentally emphasizes how important it is to protect against misuse situations in actual PQC implementations.

Despite the fact that many cryptanalytic aspects have already been discussed, we have concisely summarized them: Recent PQC research has revealed both major advancements and significant weaknesses in a several of lattice-based schemes, and ring-LWE-based schemes like NewHope have seen reduce decryption failure rates, thanks to efforts to increase bandwidth efficiency and establish stricter upper bounds. However, the security risks of parameter choices in schemes such as Kyber768 have been exposed by new lattice reduction methods.

Further research has revealed weaknesses in side channels that affect Kyber implementations as well as vulnerabilities in NTRU and Kyber key encapsulation mechanisms that enable session key recovery through cipher text manipulation, and concerns about integrity and information leakage have been raised by additional analyses that have highlighted structural issues in signature schemes such as DEFI and Peregrine.

Similarly, serious weaknesses have been identified in the BQTRU cryptosystem and EagleSign, which is at risk of key recovery attacks. Moreover, studies on CRYSTALS-KYBER and SABER have stressed the dangers of reusing randomness and the need for proper entropy management. Overall, these findings highlight the ongoing need for careful parameter selection, secure implementation practices, and new design strategies when developing post-quantum cryptographic systems.

VI. DISCUSSION

This systematic literature review utilized five well-established databases: Scopus, Web of Science, IEEE Xplore, SpringerLink and IACR ePrint, covering the period from 2020 to 2025. We reviewed a total of 35 journal articles and conference papers and identified various known mathematical hard problems and their variants.

In our exploration of lattice-based post-quantum schemes, we focused particularly on key KEMs and signature schemes. Among the identified schemes, the majority are KEMs, followed by signature schemes, with some functioning as both. Additionally, eleven schemes concentrate on cryptanalysis.

The study reveals changes and the addition of new features in both KEMs and signature schemes, highlighting important progress in lattice-based post-quantum cryptography. All of these advancements show a strong dedication to developing secure and practical cryptographic solutions that can resist the challenges presented by quantum technologies in the future.

A. STRENGTHS AND LIMITATIONS OF CURRENT LATTICE-BASED CRYPTOSYSTEMS

With an emphasis on KEM and digital signature schemes, the thorough review provides the most recent advancements in lattice-based cryptosystems and lists both established and emerging lattice-based cryptosystems, pointing out any weaknesses and suggesting future research directions. Important security issues, such as flaws in current lattice-based cryptosystems, such as the $NTRU^+$ KEM, which falls short of its stated security, have been critically examined, and significant contributions have been made from a variety of researchers [60].

Despite these strengths, the reviewed literature has a few significant limitations. The lack of thorough mathematical analysis and rigorous proofs for many suggested schemes is a critical weakness. Furthermore, the development of a systematic comparison is challenged by the absence of well-established metrics for assessing novel schemes such as Qu-Octonion NTRU, Tyber, HAETAE, and asymmetric module LWE (AMLWE). Since many studies place more emphasis on theoretical considerations than on practical resilience, another significant weakness is the absence of a strong defense mechanism against implementation attacks, such as side-channel attacks.

Furthermore, the lack of strategies for optimally balancing security and efficiency in real-world applications is a clear limitation, even though performance trade-offs are acknowledged. These present challenges show how urgently more research is needed to advance lattice-based cryptosystems for widespread acceptance.

B. IMPLICATIONS OF THE FINDINGS

The identification of promising lattice-based cryptographic schemes outside of the NIST finalists, like Qu-Octonion NTRU, Tyber, and HAETAE, etc., is one of the key findings of our systematic literature review. These algorithms demonstrate new design features and reflect the active development of alternative solutions in the PQC landscape, despite the fact that they are not yet standardized.Their occurrence in recent works signals that practicable options outside the NIST process are gaining traction and deserve further academic and practical consideration.

Researchers should keep exploring and validating these alternatives because this suggests that the field is broader than what the current standardization efforts suggest. Furthermore, the existence of these new schemes highlights the necessity of conducting a rigorous comparison between them and the NIST-standardized algorithms. Future studies and possible diversification of cryptographic standards would be guided

by these comparisons, which would concentrate on performance, security, and implementation feasibility and offer greater insight into their relative strength and suitability for different use cases.

C. FUTURE RESEARCH DIRECTIONS

Despite promising theoretical studies, the following research gaps have been observed in this work: Many PQC schemes still struggle with scalability, Most parameter selections are still heuristic. In addition lattice-based schemes also suffer from side-channel and key recovery attacks, thus requiring more robust implementation-hardening techniques. There is still an efficiency-security trade-off in terms of compact key size versus high security levels, Hybrid and algebraic extensions, like RLWE–ECC and QOTRU, respectively, require further studies for secure integration and optimized performance. The inconsistencies between the current security proof models call for a unified theoretical framework. Lastly, the absence of standardized benchmarking across architectures calls for comprehensive evaluation methods to ensure reliable and efficient quantum-resistant implementations.

Although the above research gaps should be addressed in future studies, we have also identified additional research directions.

- **Comprehensive Comparative Analysis of Emerging Schemes:**
  There is an immediate need for a strict, standardized framework to compare emerging lattice-based cryptosystems like Qu-Octonion, NTRU, Typer, HAETEA, and asymmetric module LWE (AMLWE) to the NIST standardized algorithms like Kyber and Dilithium. This architecture should include unified metrics for security, computational effectiveness, key size, and bandwidth needs across different application scenarios, including resource-constrained contexts like IoT devices. These comparisons will highlight the practical benefits and limitations of developing methods, facilitating their adoption in real-world systems.
- **Analysis and evaluation of new Algebraic Structures:**
  More in-depth study of the algebraic structures supporting new schemes, like Qu-Octonion algebra and the mathematical underpinnings of HAETAE, TYBER, etc., is crucial. Future research should concentrate on characterizing their cryptographic properties, identifying potential weaknesses, and optimizing their constructions for enhanced efficiency and security. The theoretical foundations of PQC and the creation of more robust lattice-based primitives may come from this work.
- **Development of Hybrid Cryptographic schemes:**
  To completely explore the unexplored potential of hybrid cryptographic models and dynamic parameter adaptation, more research is required. Research should examine how lattice-based schemes might have adaptive mechanisms to adjust to evolving threats or varying computational resources. Hybrid models that combine lattice-based encryption with other post-quantum or classical techniques may also provide transitional solutions that ensure compatibility with existing systems while enhancing security against quantum threats.

Lattice-based cryptography can benefit from recent advancements and get around existing limitations. By taking these paths, it offers secure, efficient, and quantum-resistant cryptographic solutions for the future.

VII. CONCLUSION

With an emphasis on modifications and new features integrated into KEM and signature schemes, we observed the development of lattice-based post-quantum crypto systems in this study. We assessed the state of lattice-based PQC by looking at a wide range of recent research. Significant limitations of earlier surveys were addressed in our analysis, such as narrow coverage, a lack of critical investigation, a lack of emphasis on the trade-offs between efficiency and investigation, and inadequate identification of research gaps. We identified several encouraging cryptographic schemes, including Qu-Octonion NTRU, Tyber, and HAETAE that go beyond the NIST finalists. This indicates that PQC is developing even outside of official standardization procedures. Such diversification is necessary to promote long-term cryptographic flexibility by reducing the risks associated with dependency on a single algorithm.

In order to direct future research, we recommended comparing these new schemes to NIST-standardized algorithms to evaluate their effectiveness, security, and usefulness as well as thoroughly analyzing the mathematical structure of these schemes. Investigating hybrid approaches, like integrating various KEM mechanisms, could also improve resilience in a variety of application scenarios and could leverage the strengths of multiple algorithms.

Lastly, the necessity for continues updates to cryptographic standards is underscores by the rapid advancement of quantum computing threats. In order to create dynamic evaluation frameworks that align with both theoretical advancements and real-world deployment challenges, we support cooperative efforts between academic institutions, industry leader, and policymakers. In general, this review provides a current viewpoint on how lattice-based cryptography is developing and offers insightful information to guide future post-quantum research, development, and standardization initiatives.

ACKNOWLEDGMENT

Dr. Seble Hailu, Director of Computing and Analytics at the Information Network Security Administration in Ethiopia, is acknowledged by the authors for her assistance and direction throughout this work.

REFERENCES

[1] R. Bavdekar, E. Jayant Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, "Post quantum cryptography: A review of techniques, challenges and standardizations," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2023, pp. 146–151, doi: 10.1109/ICOIN56518.2023.10048976.

[2] R. Wahlang and C. K., "Unbreakable security in a quantum age: A systematic literature review on post-quantum lattice-based standards," in *Proc. IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, Sep. 2023, pp. 131–141, doi: 10.1109/QCE57702.2023.00023.

[3] M. Alvarado, L. Gayler, A. Seals, T. Wang, and T. Hou, "A survey on post-quantum cryptography: State-of-the-art and challenges," 2023, *arXiv:2312.10430*.

[4] M. V. Yesina, Y. V. Ostrianska, and I. D. Gorbenko, "Status report on the third round of the NIST post-quantum cryptography standardization process," *Radiotekhnika*, no. 210, pp. 75–86, Sep. 2022, doi: 10.30837/rt.2022.3.210.05.

[5] *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, Nat. Inst. Standards Technol. (NIST), U.S. Dept. Commerce, Washington, DC, USA, Aug. 2024.

[6] *Module-Lattice-Based Digital Signature Standard*, U.S. Dept. Commerce, NIST, Fed. Info. Proc. Std. Publication 204, Washington, DC, USA, Aug. 2024.

[7] S. M. Hosseini and H. Pilaram, "A comprehensive review of post-quantum cryptography: Challenges and advances," *Int. J. Data Netw. Sci.*, vol. 9, no. 2, pp. 267–288, 2025. [Online]. Available: https://eprint.iacr.org/2024/1940

[8] L. Li, X. Lu, and K. Wang, "Hash-based signature revisited," *Cybersecurity*, vol. 5, no. 1, p. 13, Dec. 2022, doi: 10.1186/s42400-022-00117-w.

[9] D. A. Cooper, D. C. Apon, Q. H. Dang, M. S. Davidson, M. J. Dworkin, and C. A. Miller, "Recommendation for stateful hashbased signature schemes," *NIST*, vol. 800, no. 208, pp. 208–800, 2020, doi: 10.6028/NIST.SP.800-208.

[10] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*. Washington, DC, USA: National Academies Press, 2018. [Online]. Available: https://nap.nationalacademies.org/read/25196/chapter/1

[11] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH," in *Proc. Annual International Conference Theory Applications of Cryptographic Techniques*, 2023, pp. 423–447, doi: 10.1007/978-3-031-30589-4.

[12] K. Kobara and H. Imai, "On the one-wayness against chosen-plaintext attacks of the Loidreau's modified McEliece PKC," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3160–3168, Dec. 2003, doi: 10.1109/TIT.2003.820016.

[13] Y.-M. Kuo, F. García-Herrero, O. Ruano, and J. A. Maestro, "RISC-V Galois field ISA extension for non-binary error-correction codes and classical and post-quantum cryptography," *IEEE Trans. Comput.*, vol. 72, no. 3, pp. 682–692, Mar. 2023, doi: 10.1109/TC.2022.3174587.

[14] D. Jao. (2019). *Supersingular Isogeny Key Encapsulation*. National Institute of Standards and Technology Post-Quantum Cryptography Standardization. [Online]. Available: https://www.sike.org/files/SIDH-spec.pdf

[15] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Postquantum Cryptography*. Springer, 2009, pp. 147–191, doi: 10.1007/978-3-540-88702-7_5.

[16] C. Peikert, "A decade of lattice cryptography," *Found. Trends Theor. Comput. Sci.*, vol. 10, no. 4, pp. 283–424, Mar. 2016, doi: 10.1561/0400000074.

[17] *Stateless Hash-Based Digital Signature Standard*, National Inst. Standards Technol. (NIST), U.S. Dept. Commerce, NIST, Fed. Info. Proc. Std. Publication 205, Washington, DC, USA, 2024, p. 10.

[18] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Comput. Surveys*, vol. 51, no. 6, pp. 1–41, Nov. 2019, doi: 10.1145/3292548.

[19] M. E. Sabani, I. K. Savvas, D. Poulakis, G. Garani, and G. C. Makris, "Evaluation and comparison of lattice-based cryptosystems for a secure quantum computing era," *Electronics*, vol. 12, no. 12, p. 2643, Jun. 2023, doi: 10.3390/electronics12122643.

[20] A. Wang, D. Xiao, and Y. Yu, "Lattice-based cryptosystems in standardisation processes: A survey," *IET Inf. Secur.*, vol. 17, no. 2, pp. 227–243, Mar. 2023, doi: 10.1049/ise2.12101.

[21] B. S. Rawal and A. Biswas, "A comprehensive survey of post-quantum cryptography and its implications," *Eng. Sci. Technol.*, vol. 5, no. 2, pp. 256–269, Mar. 2024, doi: 10.37256/est.5220244169.

[22] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, May 2022, doi: 10.1038/s41586-022-04623-2.

[23] X. Wang, G. Xu, and Y. Yu, "Lattice-based cryptography: A survey," *Chin. Ann. Math., Ser. B*, vol. 44, no. 6, pp. 945–960, Nov. 2023, doi: 10.1007/s11401-023-0053-6.

[24] A. Mariano, T. Laarhoven, F. Correia, M. Rodrigues, and G. Falcao, "A practical view of the state-of-the-art of lattice-based cryptanalysis," *IEEE Access*, vol. 5, pp. 24184–24202, 2017, doi: 10.1109/ACCESS.2017.2748179.

[25] P. van Emde Boas. (1981). *Another Np-Complete Partition Problem and the Complexity of Computing Short Vectors in a Lattice*. [Online]. Available: https://cir.nii.ac.jp/crid/1571698600177703168

[26] M. E. Sabani, I. K. Savvas, and G. Garani, "Learning with errors: A lattice-based keystone of post-quantum cryptography," *Signals*, vol. 5, no. 2, pp. 216–243, Apr. 2024, doi: 10.3390/signals5020012.

[27] S. Goldwasser, Y. T. Kalai, C. Peikert, and V. Vaikuntanathan, "Robustness of the learning with errors assumption," Tsinghua Univ., Beijing, China, Tech. Rep., 2010. [Online]. Available: http://hdl.handle.net/1721.1/73191

[28] C. Bootland, W. Castryck, and F. Vercauteren, "On the security of the multivariate ring learning with errors problem," *Open Book Ser.*, vol. 4, no. 1, pp. 57–71, Dec. 2020, doi: 10.2140/obs.2020.4.57.

[29] A. A. Agarkar and H. Agrawal, "LRSPPP: Lightweight R-LWE-based secure and privacy-preserving scheme for prosumer side network in smart grid," *Heliyon*, vol. 5, no. 3, Mar. 2019, Art. no. e01321, doi: 10.1016/j.heliyon.2019.e01321.

[30] Y. Wang and M. Wang, "Module-LWE versus ring-LWE, revisited," *Cryptology ePrint Archive*, 2019. [Online]. Available: https://eprint.iacr.org/2019/930.pdf

[31] H. Bandara, Y. Herath, T. Weerasundara, and J. Alawatugoda, "On advances of lattice-based cryptographic schemes and their implementations," *Cryptography*, vol. 6, no. 4, p. 56, Nov. 2022, doi: 10.3390/cryptography6040056.

[32] F. Liu, Z. Zheng, Z. Gong, K. Tian, Y. Zhang, Z. Hu, J. Li, and Q. Xu, "A survey on lattice-based digital signature," *Cybersecurity*, vol. 7, no. 1, p. 7, Apr. 2024, doi: 10.1186/s42400-023-00198-1.

[33] H. Nguyen, S. Huda, Y. Nogami, and T. T. Nguyen, "Security in post-quantum era: A comprehensive survey on lattice-based algorithms," *IEEE Access*, vol. 13, pp. 89003–89024, 2025, doi: 10.1109/ACCESS.2025.3571307.

[34] S. H. Park, S. Kim, D. H. Lee, and J. H. Park, "Improved ring LWR-based key encapsulation mechanism using cyclotomic trinomials," *IEEE Access*, vol. 8, pp. 112585–112597, 2020, doi: 10.1109/ACCESS.2020.3002223.

[35] J. Zhang, Y. Yu, S. Fan, Z. Zhang, and K. Yang, "Tweaking the asymmetry of Asymmetric-Key cryptography on lattices: KEMs and signatures of smaller sizes," in *Proc. Public-Key Cryptography*, 2020, pp. 37–65, doi: 10.1007/978-3-030-45388-6.

[36] B. Gong, L. Cheng, and Y. Zhao, "SKCN: Practical and flexible digital signature from module lattice," in *Proc. 25th Australas. Conf. Inf. Secur. Privacy*, Perth, WA, Australia, 2020, pp. 62–81, doi: 10.1007/978-3-030-55304-3.

[37] P. Ravi, S. S. Gupta, A. Chattopadhyay, and S. Bhasin, "Improving speed of Dilithium's signing procedure," in *Proc. 18th Int. Conf. Smart Card Res. Adv. Appl.*, 2020, pp. 57–73, doi: 10.1007/978-3-030-42068-0.

[38] C. Jung, J. Lee, Y. Ju, Y. Kwon, S. Kim, and Y. Paek, "LizarMong: Excellent key encapsulation mechanism based on RLWE and RLWR," in *Proc. 22nd Int. Conf. Inf. Secur. Cryptol.*, 2020, pp. 208–224, doi: 10.1007/978-3-030-40921-0.

[39] H. H. Abo-Alsood and H. R. Yassein, "QOTRU: A new design of NTRU public key encryption via qu-octonion subalgebra," *J. Phys., Conf. Ser.*, vol. 1999, no. 1, Sep. 2021, Art. no. 012097, doi: 10.1088/1742-6596/1999/1/012097.

[40] R. Kundu, A. de Piccoli, and A. Visconti, "Public key compression and fast polynomial multiplication for NTRU using the corrected hybridized NTT-Karatsuba method," *Cryptology ePrint Archive*, 2022. [Online]. Available: https://eprint.iacr.org/2022/108

[41] V. Kumar, R. Das, and A. K. Gangopadhyay, "GR-NTRU: Dihedral group over ring of Eisenstein integers," *J. Inf. Secur. Appl.*, vol. 83, Jun. 2024, Art. no. 103795, doi: 10.1016/j.jisa.2024.103795.

[42] J. H. Cheon, H. Choe, J. Devevey, T. Güneysu, D. Hong, M. Krausz, G. Land, M. Möller, D. Stehlé, and M. Yi, "HAETAE: Shorter lattice-based fiat-shamir signatures," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2024, no. 3, pp. 25–75, Jul. 2024, doi: 10.46586/tches.v2024.i3.25-75.

[43] J. Kim and J. H. Park, "NTRU+: Compact construction of NTRU using simple encoding method," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 4760–4774, 2023, doi: 10.1109/TIFS.2023.3299172.
[44] T. Espitau, T. T. Q. Nguyen, C. Sun, M. Tibouchi, and A. Wallet, "Antrag: Annular NTRU trapdoor generation," *Cryptology ePrint Archive*, 2023. [Online]. Available: https://eprint.iacr.org/2023/1335
[45] S. Lee, J. Woo, J. Kim, and J. H. Park, "Generalized centered binomial distribution for bimodal lattice signatures," *IEEE Access*, vol. 13, pp. 2203–2214, 2025, doi: 10.1109/ACCESS.2024.3523521.
[46] H. Hajaje, Z. E. A. Guennoun, and M. Guennoun, "PMTRU: An efficient and resistant variant of the NTRU public key cryptosystem," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, Aug. 2020, pp. 1–8, doi: 10.1109/CCECE47787.2020.9255710.
[47] T. Espitau, M. Tibouchi, A. Wallet, and Y. Yu, "Shorter hash-and-sign lattice-based signatures," in *Proc. 42nd Annu. Int. Cryptol. Conf.*, 2022, pp. 245–275, doi: 10.1007/978-3-031-15979-4.
[48] J. Sharafi and H. Daghigh, "A Ring-LWE-based digital signature inspired by Lindner–Peikert scheme," *J. Math. Cryptol.*, vol. 16, no. 1, pp. 205–214, Aug. 2022, doi: 10.1515/jmc-2021-0013.
[49] K. Boudgoust, A. Sakzad, and R. Steinfeld, "Vandermonde meets regev: Public key encryption schemes based on partial Vandermonde problems," *Designs, Codes Cryptography*, vol. 90, no. 8, pp. 1899–1936, Aug. 2022, doi: 10.1007/s10623-022-01083-7.
[50] Z. Wang, D. Tang, H. Yang, and F. Li, "A public key encryption scheme based on a new variant of LWE with small cipher size," *J. Syst. Archit.*, vol. 117, Aug. 2021, Art. no. 102165, doi: 10.1016/j.sysarc.2021.102165.
[51] W. Liang, Z. Liu, X. Zhao, Y. Yang, and Z. Liang, "Flexible and compact MLWE-based KEM," *Mathematics*, vol. 12, no. 11, p. 1769, Jun. 2024, doi: 10.3390/math12111769.
[52] J. Gärtner, "NTWE: A natural combination of NTRU and LWE," in *Proc. 14th Int. Workshop Post-Quantum Cryptography*, 2023, pp. 321–353, doi: 10.1007/978-3-031-40003-2.
[53] Z. Zhang, H. Chen, and Y. Chen, "A provable secure signature in the quantum random Oracle model," in *Proc. Int. Conf. Blockchain Technol. Inf. Secur. (ICBCTIS)*, Jul. 2022, pp. 43–46, doi: 10.1109/ICBCTIS55569.2022.00021.
[54] A. Homsi, M. Al-Fayoumi, and M. Al-Fawa'reh, "Lattice-based RLWE key generation using ECC," in *Proc. Int. Jordanian Cybersecurity Conf. (IJCC)*, Jordan, Dec. 2024, pp. 82–86, doi: 10.1109/ijcc64742.2024.10847283.
[55] Z. Jin, S. Shen, and Y. Zhao, "Compact and flexible KEM from ideal lattice," *IEEE Trans. Inf. Theory*, vol. 68, no. 6, pp. 3829–3840, Jun. 2022, doi: 10.1109/TIT.2022.3148586.
[56] H. Bambury and P. Q. Nguyen, "Improved provable reduction of NTRU and hypercubic lattices," in *Proc. 15th Int. Workshop Post-Quantum Cryptography*, 2024, pp. 343–370, doi: 10.1007/978-3-031-62743-9.
[57] M. Song, S. Lee, D.-J. Shin, E. Lee, Y.-S. Kim, and J.-S. No, "Analysis of error dependencies on newhope," *IEEE Access*, vol. 8, pp. 45443–45456, 2020, doi: 10.1109/ACCESS.2020.2977607.
[58] Q. Guo and T. Johansson, "Faster dual lattice attacks for solving LWE with applications to CRYSTALS," in *Proc. 27th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, vol. 13093, Dec. 2021, pp. 33–62, doi: 10.1007/978-3-030-92068-5.
[59] Y. Yang, Z. Wang, J. Ye, J. Fan, S. Chen, H. Li, X. Li, and Y. Cao, "Chosen ciphertext correlation power analysis on kyber," *Integration*, vol. 91, pp. 10–22, Jul. 2023, doi: 10.1016/j.vlsi.2023.02.012.
[60] J. Lee, H. Ryu, M. Lee, and J. Park, "Cryptanalysis on 'NTRU+: Compact construction of NTRU using simple encoding method,'" *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 9508–9517, 2024, doi: 10.1109/TIFS.2024.3471074.
[61] K. Pursharthi and D. Mishra, "Cryptanalysis with countermeasure on the SIS based signature scheme," in *Proc. 13th Int. Conf. Secur., Privacy, Appl. Cryptogr. Eng.*, 2024, pp. 92–100, doi: 10.1007/978-3-031-51583-5.
[62] H. N. H. Al-Jabbari and A. Maarefparvar, "A digital signature scheme based on module-LWE and module-SIS," 2024, *arXiv:2409.02222*.
[63] L. N. Pulles and M. Tibouchi, "Cryptanalysis of EagleSign," in *Proc. 14th Int. Conf. Secur. Cryptography Networks*, 2024, pp. 165–186, doi: 10.1007/978-3-031-71073-5.
[64] A. Raya, "Efficient noncommutative KEMs from twisted dihedral group ring," *Cryptology ePrint Archive*, 2025. [Online]. Available: https://eprint.iacr.org/2025/795
[65] S. Okada and Y. Wang, "Recovery attack on Bob's reused randomness in CRYSTALS-KYBER and SABER," in *Proc. 15th Int. Conf. Provable Secur. Provable Practical Security*, Nov. 2021, pp. 155–173, doi: 10.1007/978-3-030-90402-9.
[66] A. Raya, V. Kumar, A. K. Gangopadhyay, and S. Gangopadhyay, "Giant does NOT mean strong: Cryptanalysis of BQTRU," in *Proc. 16th Int. Workshop Post-Quantum Cryptography*, 2025, pp. 312–348, doi: 10.1007/978-3-031-86599-2.
[67] H. Bambury and P. Q. Nguyen, "Cryptanalysis of an efficient signature based on isotropic quadratic forms," in *Proc. 16th Int. Workshop Post-Quantum Cryptography*, 2025, pp. 153–175, doi: 10.1007/978-3-031-86602-9.
[68] A. Pouly and Y. Shen, "Provable dual attacks on learning with errors," in *Proc. 43rd Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2024, pp. 256–285, doi: 10.1007/978-3-031-58754-2.
[69] X. Lin, M. Suzuki, S. Zhang, T. Espitau, Y. Yu, M. Tibouchi, and M. Abe, "Cryptanalysis of the peregrine lattice-based signature scheme," in *Proc. 27th IACR Int. Conf. Pract. Theory Public-Key Cryptography*, 2024, pp. 387–412, doi: 10.1007/978-3-031-57718-5.

DEREJE WASIHUN MELLESE received the B.Ed. degree in mathematics from Bahir Dar University, Bahir Dar, Ethiopia, in 2002, and the M.Sc. degree in 2007, and the Ph.D. degree in algebra from Addis Ababa University, Addis Ababa, Ethiopia, in 2020. Since 2020, he has been an Assistant Professor with the Mathematics Department, Addis Ababa Science and Technology University. He was the Head of the Department of Mathematics, from 2021 to 2023. He is currently the Head of the Mathematics, Physics, and Statistics Division with Addis Ababa Science and Technology University. He has published over six articles in peer-reviewed journals. His research interests include algebraic structures and cryptography.

Dr. Mellese is a member of Ethiopian Mathematics Professional Association. He is also a member of the Artificial Intelligence and Robotics Center of Excellence and an Associate Member of the High Performance Computing and Big Data Analytics Center of Excellence at Addis Ababa Science and Technology University.

ZEBENE GIRMA TEFERA received the B.Sc., M.Sc., and Ph.D. degrees in mathematics from Addis Ababa University, Ethiopia.

He is currently an Assistant Professor of mathematics with the Division of Mathematics, Physics, and Statistics with Addis Ababa Science and Technology University. He has published five articles in peer-reviewed journals. His research interests include cryptography, coding theory, group divisible designs, t-designs, topological indices and enumerative combinatorics.

Dr. Tefera is a member of Ethiopian Mathematics Professional Association and also a member of the Artificial Intelligence and Robotics Center of Excellence and an associate member of the High Performance Computing and Big Data Analytics Center of Excellence at Addis Ababa Science and Technology University.

MELAKU BERHE BELAY is currently an Associate Professor with the Division of Mathematics, Physics, and Statistics, Addis Ababa Science and Technology University, and the Ph.D. degree in operational research and cybernetics from the Central China Normal University, Wuhan, China.

He has published over 20 articles in peer-reviewed journals. His research interests include topological indices of chemical graphs and extremal graphs, combinatorics, cybernetics, and cryptography.

Dr. Belay is a member of Ethiopian Mathematics Professional Association and nanotechnology Center of Excellence with Addis Ababa Science and Technology University. He is also an Associate member of the High Performance Computing and Big Data Analytics Center of Excellence with Addis Ababa Science and Technology University.

GIZACHEW HAILE SEFFA received the B.Sc. degree in applied mathematics from Addis Ababa University, Ethiopia, in July 2009.

He is currently a Cryptography Researcher with the Information Network Security Administration. His research interests include cryptology, contributing to the development of cryptographic schemes and secure communication systems, and post-quantum research.

ADEM GULUMA NEGEWO received the M.Sc. degree in mathematics from Addis Ababa University, and the M.Sc. degree in software engineering from Addis Ababa Science and Technology University.

He is currently a Lecturer with the Department of Mathematics, Physics, and Statistics, Addis Ababa Science and Technology University. His research interests include operations research, cybersecurity, data science, deep learning, computer vision, and trustworthy AI.

Mr. Negewo is a member of Ethiopian Mathematics Professionals Association and the Artificial Intelligence and Robotics Centre of Excellence with Addis Ababa Science and Technology University. He is also an Associate member with the High Performance Computing and Big Data Analytics Centre of Excellence, Addis Ababa Science and Technology University.

ZELALEM GIZACHEW ACHAM received the B.Sc. degree in mathematics from Bahir Dar University, Bahir Dar, Ethiopia.

He is currently a Cryptology Researcher with INSA, Ethiopia. In this role, he focuses on post-quantum cryptographic research, contributing to the development of various security systems, and guiding the cryptographic research division. His research interests include cryptography, information security, and algorithm design.

MEKONNEN ANDUALEM ATINAF received the B.Sc. degree in mathematics from Bahir Dar University, Ethiopia.

He is currently a Cryptology Researcher with the Information Network Security Administration (INSA), Ethiopia. His current work focuses on the theoretical analysis and security of post-quantum cryptographic schemes, particularly those based on hard lattice problems, with applications to secure communication systems. His research interests include cryptography, post-quantum cryptography, and lattice-based cryptographic constructions.

DANIEL MERKEBU ADAMU received the B.Sc. degree in computer science from Bahir Dar University.

He is currently a Cryptology Researcher with the Cryptography Division with the Information Network Security Administration. His research interests include post-quantum cryptography, cryptographic protocols, and secure algorithm development.