eISSN 2310-290X
Vol. 14, No. 2, 2025

https://revistas.unitec.edu/innovare

INNOVARE
Revista de ciencia y tecnología

Review

OPEN ACCESS

A survey in Lattice-Based Post-Quantum Cryptography and its appliances on IoT systems

Un estudio sobre criptografía postcuántica basada en redes y sus aplicaciones en sistemas IoT

Andrea Gisselle Menjivar [1]

[1] Master of Science in Internet of Things Florida International University Miami, Florida

Abstract / **Introduction**. This review delves into lattice-based encryption and its implications for bolstering the protection of Internet of Things (IoT) systems. The survey extensively explores the post- quantum robustness of inherent in lattice-based cryptographic techniques, highlighting their potential to effectively address the evolving security challenges within the IoT domain. **Methods**. The literature review not only scrutinizes traditional, pre-quantum cryptography methods but also conducts a thorough analysis of quantum computing and its possible influence on existing encryption techniques, emphasizing the necessity for post-quantum solutions. **Developing.** The paper discusses the pivotal role of the National Institute of Standards and Technology (NIST) in standardizing post-quantum cryptography as well as presenting a comprehensive analysis of their work in this domain. A focused examination of NIST finalists reveals lattice-based cryptography as a key area of research, delving into its mechanisms and operational principles. **Conclusion.** The paper concludes with an in-depth exploration of diverse lattice-based cryptography applications within various IoT systems, encompassing domains such as E- health, smart cities, smart grids, vehicular communications, and industrial IoT systems. This comprehensive analysis provides valuable insights into the multifaceted landscape of lattice-based encryption and its versatile implementation across different IoT domain.
Keywords: Computer science, Cryptography, Cybernetics, Internet, Quantum theory

Resumen / **Introducción.** Esta revisión general profundiza en el cifrado basado en red y sus implicaciones para reforzar la protección de los sistemas del Internet de las Cosas (IoT). El estudio explora exhaustivamente la robustez poscuántica inherente a las técnicas criptográficas basadas en red, destacando su potencial para abordar eficazmente los desafíos de seguridad en constante evolución dentro del dominio del IoT. **Métodos.** La revisión bibliográfica no solo examina los métodos criptográficos tradicionales precuánticos, sino que también realiza un análisis exhaustivo de la computación cuántica y su posible influencia en las técnicas de cifrado existentes, enfatizando la necesidad de soluciones poscuánticas**. Desarrollo.** El artículo analiza el papel fundamental del National Institute of Standards and Technology (NIST) en la estandarización de la criptografía poscuántica y presenta un análisis exhaustivo de su trabajo en este ámbito. Un examen centrado en los finalistas del NIST revela la criptografía basada en red como un área clave de investigación, profundizando en sus mecanismos y principios operativos. **Conclusión.** El artículo concluye con una exploración exhaustiva de diversas aplicaciones de la criptografía basada en redes en diversos sistemas del IoT, que abarcan ámbitos como la salud electrónica, las ciudades inteligentes, las redes inteligentes, las comunicaciones vehiculares y los sistemas industriales del IoT. Este análisis exhaustivo proporciona información valiosa sobre el panorama multifacético del cifrado basado en redes y sus versátiles implementaciones en diferentes dominios del IoT.
Palabras clave: Aplicación informática, Cibernética, Criptografía, Internet, Teoría cuántica

Recepción: 22 de enero 2025 / Aceptación: 28 de junio de 2025 / Publicación: 05 de diciembre de 2025.
Corresponding author: anmenj003@fiu.edu

Citation: Menjivar A.G. (2025). A survey in Lattice-Based Post-Quantum Cryptography and its appliances on IoT systems. *Innovare, Revista de Ciencia y Tecnología, 14*(2), 1-11. https://doi.org/10.69845/innovare.v14i2.444

INTRODUCTION

In present, it is true that a large percentage of the world's population has access to communications through the internet, but what many do not know is that our online communications must be kept secure so that no one else can have access to them. When we browse the internet, all our information is shared and exposed to various entities that can intercept that information and use it. That's why it's important to keep online communications secure.

Encryption plays a fundamental role in protecting online communications by providing a layer of security that safeguards the confidentiality and integrity of transmitted information. By implementing encryption techniques, data is trans- formed into an unreadable form during transmission, and only the authorized recipient, having the appropriate decryption key, can reverse this process and access the information in its original form. Encryption ensures that even in the case of interception by unauthorized third parties, the information remains inaccessible and protected. End-to-

end encryption is a technique that guarantees that only the sender and the recipient of a message can access its content, and not even the service provider can view the transmitted information.

From ancient times, when the Egyptians used hieroglyphics to conceal and send messages, to the present day, encryption has played a crucial role in the history of communications, constantly evolving. Over time, two main types of encryptions have emerged: symmetric and asymmetric. Asymmetric encryption, currently more widely used, provides greater security in communications. Symmetric encryption utilizes a single key for both the encryption and decryption processes. In contrast, asymmetric encryption involves a pair of keys: a public key for encrypting data and a corresponding private key for its decryption. This methodology ensures a more prominent stage of protection, as the private key, essential for decryption, remains secret.

From antiquity to the current digital era, encryption has been essential to preserve the confidentiality of information and ensure security in communications (Luo, Ouyang, Liu, & Cao, 2019). Depending on the use case, there are many types of encryptions, historically RSA has been a popular choice by including securing communications and digital signatures, bit in recent years other encryption algorithms have gained prominence like the ECC which is the Elliptic Curve Cryptography long side with the other well-known standard which is AES defined as Advanced Encryption Standard (Hamza & Kumar, 2020).

Despite these advancements, there are ongoing concerns and challenges regarding online privacy. Additionally, it is important to highlight that online security is a constantly evolving field, and threats and technologies change over time. Therefore, it is essential for individuals to be aware of recommended security practices and use services that provide robust encryption to protect their online communications. Current encryption techniques face various threats in the contemporary digital environment. One of the most significant challenges arises from technological advancements that can potentially compromise the robustness of encryption algorithms. Brute- force attacks and the increasing computational capacity of modern devices can test the strength of encrypted keys.

One of the greatest challenges that current cryptography will have to face is the emergence of quantum computing. There is a competition between quantum computing and traditional cryptography techniques that have been safeguarding the internet, blockchain and online communications over the years. While it seems unlikely that the slowly advancing field of quantum computing will imminently surpass and overcome traditional cryptography, the cautionary message from the fable remains pertinent (Castelluccio, 2021).

METHODS

The present survey involves systematic exploration of latticed-based post-quantum cryptography and its implementation in the context of Internet of things (IoT) systems. It commences with an extensive literature review, delving into a explanation on pre-quantum cryptography, quantum computing, NIST standardization, post-quantum cryptography finalist schemes including a deep explanation on lattice-based cryptography and its appliances in different IoT systems. The scope is meticulously defined, outlining the specific dimensions of lattice-based cryptography, and emphasizing its relevance in the IoT context. A pre-quantum and post- quantum cryptography analyzing their strengths and weak- nesses is presented. This survey investigates the practical applications of lattice-based cryptography within IoT, evaluates performance metrics, assess security guarantees, and address challenges and future directions. Real-world case studies and implementations are examined for insights, and the survey concludes by summarizing key findings and providing perspectives on future research directions. This methodology ensures a comprehensive examination of lattice-based post-quantum cryptography and its contributions to IoT security.

DEVELOPING

Quantum Computing

Current encryption techniques work assuming nobody, even using computational resources, will be able to solve a very difficult mathematical problem in a reduced amount of time, but that is not the case with quantum computing. With the utilization of substantial quantum computers, it becomes possible to compromise all existing classical asymmetric algorithms employed for key distribution and digital signatures (Cavaliere, Mattsson, & Smeets, 2020).

Quantum computing represents a sophisticated computational paradigm that harnesses the principles of quantum mechanics. In contrast to classical computing, which relies on bits representing either 0 or 1, quantum computing utilizes qubits. Qubits have the unique ability to exist simultaneously in a superposition state, indicating that it can represent both 0's as well as 1's at the same period of time. Superposition is the fundamental principle in quantum mechanics it denotes that a quantum system, for example a qubit in a quantum computer, can exist in multiple states simultaneously (Maslov, Nam, & Kim, 2019).

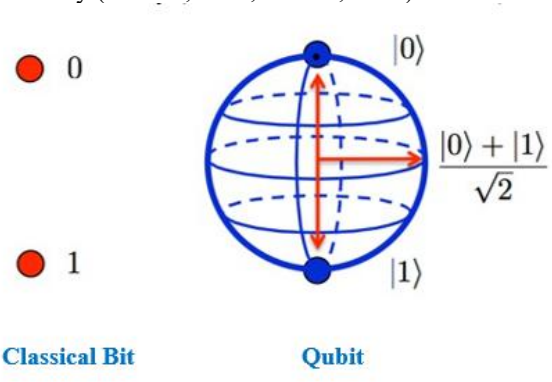

Figure 1. Shows an illustration of the difference between classical bits and qubits, which can represent both classical bits 0 and 1 at the same time.

Using qubits and the principle of superposition, quantum computers can employ Shor's algorithm to efficiently factor

large numbers, a task that would be extremely challenging for classical computers. This quantum advancement poses a possible danger to current cryptography systems, as many of them depend on difficulty of factoring large numbers to ensure security. The ability of quantum computers to perform this task more efficiently could compromise the integrity of cryptographic keys currently in use, underscoring the need to explore and develop cryptography methods resistant to quantum computing (Bhatia & Ramkumar, 2020).

Shor's algorithm uses the qubits to perform multiple calculations simultaneously, exploring different possibilities at the same time, instead of checking each possible factor one by one, which can take a lot of time with large numbers, it uses quantum parallelism to efficiently find the prime factors. This becomes a threat to our current RSA cryptography, quantum computing with the utilization of this algorithm can easily determine the private key for the public key.

Although quantum technology promises many things and is constantly evolving, it faces some challenges for its implementation. Quantum computers are currently in the initial phases of advancement, and practical, large scale quantum computers suitable for general use have not yet become accessible. One of the principal concerns facing implementation of quantum technology lies in the fragility of qubits, the basic components of quantum information. These qubits are extremely sensitive to external interferences and environmental fluctuations, which can result in errors in quantum computations. Additionally, the precise creation and manipulation of qubits require controlled environments and extremely low temperatures, complicating the construction and maintenance of large-scale quantum computers. Furthermore, the coexistence of quantum technology with existing infrastructures and standards presents additional challenges.

Despite these difficulties, the scientific and techno- logical community continues to address these issues in search of solutions that will unlock the full potential of quantum computing in the future (Córcoles, 2020). However, despite the challenges, there has been significant progress in building small-scale quantum processors, and many enterprises and governments are actively working on advancing quantum computing technology. Shor's algorithm, a groundbreaking quantum algorithm developed by Peter Shor in 1994, stands as a pivotal achievement in the realm of quantum computing. Its primary objective is to efficiently factorize large integers into their prime components—a task widely considered intractable for classical computers when dealing with sufficiently large numbers. The algorithm's strength lies in its ability to leverage quantum parallelism to perform computations at an exponential speed, particularly in the crucial step of finding the periodicity of modular exponential functions.

This quantum Fourier transform-based approach allows Shor's algorithm to break down the complexity of integer factorization into polynomial time, posing a significant threat to widely used cryptographic systems, such as RSA, which depend on presumed the challenge of factoring large numbers to ensure security. Difficulty of factoring large numbers for security. While Shor's algorithm represents a groundbreaking advancement, its practical implementation faces substantial challenges. The need for a large-scale, fault-tolerant quantum computer with a sufficient number of qubits and low error rates remains a formidable obstacle. As of the latest knowledge update in January 2022, quantum computers meeting these criteria are still in the early stages of development. Nevertheless, Shor's algorithm has spurred significant research in quantum- resistant cryptographic techniques, as its successful execution on a quantum computer would compromise the security foundations of current cryptographic standards. As quantum technologies progress, the potential impact of Shor's algorithm underscores the importance of exploring and implementing post-quantum cryptographic solutions to ensure the strength of digital security against future developments in quantum technology.

Researchers have coined the term Y2Q to signify the moment when the tortoise surpasses the hare, representing the year when quantum code-breaking capabilities will pose the ultimate existential threat to traditional cryptography. The timing of this event remains speculative, but the consensus is that it is inevitable. In 2018, a report from the U.S. National Academies of Sciences, Engineering, and Medicine projected that a potent quantum computer utilizing Shor's algorithm could decrypt a 1,024-bit RSA (Rivest-Shamir-Adleman) encryption implementation in less than 24 hours (Castelluccio, 2021).

Given that this is a race against time, it is necessary to seek solutions as soon as possible to anticipate the potential risks posed by the impending danger of quantum computing. To address this issue, NIST (The National Institute of Standards and Technology) the organization responsible for establishing standards in the United States, has implemented a plan for the standardization of post-quantum cryptography.

NIST Standardization

The National Institute of Standards and Technology (NIST) is currently engaged in the standardization of post-quantum cryptographic algorithms, with a collaborative initiative focused on delivering secure and interoperable solutions. In 2016, NIST started the work and process of standardizing post-quantum cryptography, conducting three rounds to narrow down candidate schemes. The final 13 schemes are now undergoing continuous analysis.

NIST started 2016 with a call for post quantum schemes proposals, based on three key research areas being lattice-based, hash-based, and code-base cryptography. Lattice-based cryptography utilizes mathematical structures called lattices for quantum-resistant encryption. Hash-based encryption de- pends on quantum-resistant hash algorithm to secure data and communications. Finally, Code-based cryptography Leverages error-correcting codes as the foundation for cryptographic systems capable of withstanding attacks from quantum adversaries (Hegde, Jamuar, & Kulkarni, 2023).

By November 2017 round 1 was analyzed with a result of 69 schemes divided into 1/3 signature and 2/3 PKE schemes. These algorithms underwent rigorous testing and analysis by the scientific community and security experts to assess their performance and security. By March 2019, round 2 was finished and proposed schemes were narrowed to 26, nine signature and 17 PKE schemes. After numerous and rigorous analysis NIST

choose round's 3 finalist which they divided into 7 finalists and 8 alternative schemes. Between the finalists in key encapsulation mechanisms latticed based are three including Kyber, NTRU and Saber. By 2022-2023 there is a draft standard and NIST final standard is expected to be announced in 2024 (I. T. L. Computer Security Division, 2024).

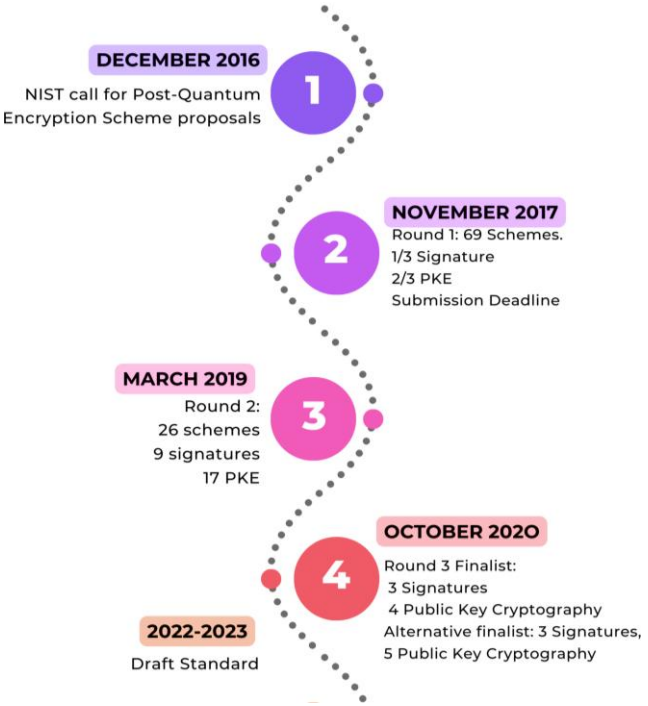

Figure 2. NIST post-quantum standardization timeline. Basis Vectors with Generated Lattice.

NIST priorities for round 3 include cryptanalysis for a better understanding of CoreSVP Hardness of lattice-based schemes. Does choice of lattice matter? Decide between three lattice based final candidates. As for the implementation, they are analyzing side-channel resistant implementation, difficulty in implementation, performance metrics in internet protocols, and performance data for hardware implementations (I. T. L. Computer Security Division, 2024).

The presence of three lattice-based algorithms among the NIST finalists is intriguing, prompting a deeper exploration into the workings of lattice-based cryptography and potential applications within our contemporary setting. Understanding the principles behind lattice-based cryptography becomes crucial as we seek robust and quantum-resistant cryptographic solutions for our ever-evolving digital landscape. Exploring the applications and implications of lattice-based algorithms in our current security infrastructure is essential for preparing and adapting to the future challenges of quantum computing.

Transition Challenges

Transitioning from classical to post-quantum cryptographic methods presents a set of challenges, as highlighted by (Ott, Peikert, & al., 2019). These challenges encompass ensuring backward compatibility with existing systems, updating protocols to accommodate new algorithms, addressing the computational demands as- sociated with these novel cryptographic approaches, devising effective key management strategies, maintaining algorithm agility to adapt to evolving threats, and ensuring interoperability within diverse computing environments. Successfully navigating these challenges is crucial for a seamless and secure integration of post-quantum cryptographic techniques, marking a significant stride in fortifying the robustness of digital communication in the face of advancing technological landscapes. Also, one primary concern that requires careful consideration: Attackers can record encrypted communications now and decrypt them retroactively once a quantum computer is available.

Devising effective key management strategies is paramount to the success of post-quantum cryptography. As the cryptographic landscape evolves, the ability to securely generate, distribute, and update cryptographic keys becomes increasingly intricate and demands innovative solutions. Algorithm agility is another critical facet, emphasizing the need for cryptographic systems that can dynamically adapt to emerging threats without requiring a complete overhaul of existing infrastructure. Achieving interoperability within diverse computing environments, encompassing various devices and platforms, further heightens the complexity of implementing post-quantum cryptographic techniques on a broad scale.

Amid these challenges, it is crucial to acknowledge a primary concern – the potential for attackers to record encrypted communications today and decrypt them retroactively once a quantum computer becomes available. This temporal vulnerability underscores the urgency of adopting quantum-resistant cryptographic measures promptly. Successfully navigating this intricate landscape requires collaborative efforts from researchers, industry experts, and policymakers to develop standardized and widely accepted post-quantum cryptographic solutions. Ultimately, overcoming these challenges will signify a substantial stride towards fortifying the robustness of digital communication in anticipation of the transformative effects of quantum computing on traditional cryptographic practices.

Lattice-Based Cryptography

Lattice-based cryptography constitutes a specialized branch of cryptography techniques grounded in the computational complexity of specific problems related to mathematical lattices. In essence, a lattice manifests as a systematic arrangement of points or dots within a space with multiple dimensions, shaping an output of grid-like structure. The security underpinning lattice-based encryption depends on the intricacy inherent in solving mathematical challenges associated with these lattices. From a mathematical standpoint, a lattice can be precisely characterized as ensemble of all integer's linear combinations for basis vector. This approach harnesses the unique properties of lattices, offering a resilient foundation for cryptographic schemes that resist conventional and potential quantum-based attacks. The elegance of lattice-based cryptography lies in its ability to leverage the complexity of lattice problems to fortify the security of digital communication in our increasingly sophisticated and interconnected world (Khalid, McCarthy, O'Neill, & Liu, 2019). As lattices are essentially infinite structures, their application in cryptography requires adaptation to the finite

memory constraints of computers. To overcome this limitation, a practical approach involves utilizing the concept of a basis. In this context, a basis is a set of compact vectors that possesses the ability to represent any point within the lattice's grid. This allows for a more efficient and manageable computation, ensuring that the intricacies of lattice-based cryptography can be effectively implemented within the computational resources of a computer, despite the infinite nature of lattices.

In mathematical terms, a lattice is characterized as a discrete subgroup within the real numbers, of all linear combination. According to lattice theory, lattices that share the same bases are considered equivalent; therefore, it is impossible for two lattices to have the same basis.

Figure 3 Shows a lattice that was generated by four vectors, [B1,B2] and [X1,X2] which are two pairs of totally different vectors. Here we can find two types of basis. Vectors [X1,X2] are defined as a bad basis because if you only know a bad basis for the same lattice it could be much harder to solve the problem. [B1, B2] are defined as a good basis of vectors because they are almost orthogonal, and it is easier to solve the mathematical problem with this good basis. But what is the mathematical problem lattices help to solve? The problem is the shortest vector problem.

The Shortest Vector Problem

It is easy to say Lattice a was generated by basis (x1,x2) but the hard questions in lattice problems come when you ask: Which point on the lattice is closest to the origin, not including the lattice point at the origin? Also, which combination of the vector basis is closest to the origin? That presents the shortest vector problem.

The shortest vector problem refers to finding the lattice point which is closest to but not equal to the origin in a set of basis. The method of trying different combinations that seemed good to solve the problem is inefficient, it consumes a lot of time and resources. It is possible that the optimal solution comes from adding many blue and red vectors. In two dimensions a solution can probably be reasoned out, but the shortest vector problem gets very hard in higher dimensions.

If two basis vectors are used with two coordinates a two-dimensional lattice is created, but if a three vectors basis with three coordinates is used, the output will be a three- dimensional lattice. And for example, a 17-basis vector gives a 17-dimensional lattice as shown in Fig. 3.

Asif (2021) mentioned there are more possibilities in higher dimensions and the shortest vector problem is even harder. This problem belongs to a collection of related problems known as lattice problems which experts believe to be hard problems, especially in hundreds of dimensions. In other words, it will generally take a computer a very long time to get the answer for the shortest vector problem and importantly for the post-quantum era purpose, computer scientists also believe that it would be very difficult for a quantum computer to solve these problems That is what makes them good candidates for the mathematical basis for a quantum secure cryptographic protocols (Tateiwa, 2021). The closest vector problem becomes significantly more challenging to solve on a bad basis compared to a good basis. If an individual possesses knowledge of a good basis for the lattice, it becomes relatively straightforward to find the closest vector. However, when only a bad basis for the same lattice is known, the difficulty of solving the problem increases substantially. The determination of the closest vector in such a scenario may involve adding and subtracting numerous vectors, presenting a more complex computational challenge. The intricacies of the closest vector problem are further underscored when considering the impact of the choice of basis for a lattice. The distinction between a good basis and a bad basis plays a pivotal role in the computational complexity of solving this problem. In scenarios where an individual is equipped with knowledge on a good basis, the task of finding the closest vector is considerably simplified. A good basis provides a set of vectors that efficiently span the lattice, facilitating a more direct and streamlined approach to the solution.

Conversely, when only a bad basis is known for the same lattice, the challenges in solving the closest vector problem escalate markedly. The reliance on a less optimal basis introduces computational hurdles that demand a more intricate approach. In such instances, determining the closest vector may necessitate the addition and subtraction of numerous vectors, contributing to a heightened level of computational intricacy. The inherent difficulty in manipulating a bad basis intensifies the computational effort required, making the problem more intricate and emphasizing the critical role that basis quality plays in the resolution of the closest vector problem.

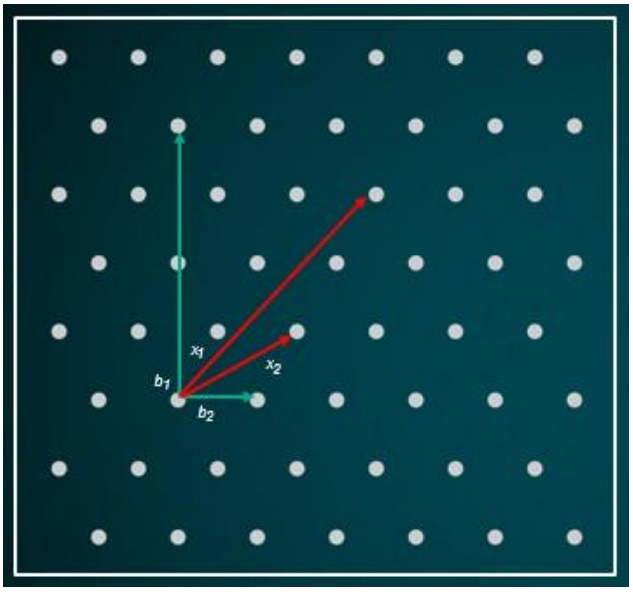

Figure 3. Basis Vectors with Generated Lattice. The nuanced interplay between the nature of the basis and the complexity of the problem highlights the significance of a well-structured basis in lattice-based algorithms.

Lattice-Based Problems Applied To Cryptography

One notable application of lattice-based problems is in the design of lattice-based cryptographic schemes, including encryption and digital signatures, which are considered too withstand attacks by classic computers and quantum computers. The cybersecurity of these schemes depends on computational difficulty of lattice problems, offering a promising avenue for developing robust cryptographic methods in the age of post-

quantum computers. The way it works is when the recipient sets up a lattice with two different pairs of vector basis. In other words, both pairs of basis generated the same lattice. One is going to be the good basis and the other is the bad basis, as mentioned above the difference between both. So, the recipient will keep the good basis as a secret, becoming the Private Key in cryptography, and recipient will tell the sender the bad basis which is the Public Key in cryptography. The sender uses the bad basis and embeds a message in the lattice. The sender chooses another point on the lattice which is going to be the encrypted message and sends back the coordinates to the recipient. The recipient has the secret good basis, or secret key, so he uses it to figure out which point is the closest to the mentioned lattice to recover the encrypted message.

Lattice-Based Final Post-Quantum Schemes

In the final stages of the NIST standardization analysis, particular attention is drawn to the last three finalists, all of which are rooted in lattice-based cryptographic approaches. This section delves into the unique characteristics and strengths of these lattice-based algorithms, emphasizing their significance in terms of post-quantum cryptography. As the cryptographic community awaits the outcomes of the NIST standardization process, understanding the distinctive features of these lattice-based finalists becomes paramount in evaluating their potential role in shaping the future landscape of secure communication and digital information protection. Three latticed-based final- ists are: Kyber, NTRU, and Saber.

Kyber is a key encapsulation mechanism (KEM) based on the hardness of learning with errors (LWE) on module lattices. It provides protecction for both classical and potential quantum attacks. Kyber is notably efficient due to its ability to leverage rapid multiplication facilitated by the negacyclic number-theoretic transform (NTT) (Román, Arjona, López-González, & Baturone, 2022). Kyber contributes to minimizing complexity and provides significantly enhanced scalability when contrasted with ring-LWE. Kyber exhibits performance levels akin to ring-LWE-based schemes when using 256 bits for message encryption. The CRYSTALS- Kyber implementations encompass diverse approaches, including software design as well as hardware (Nguyen, Nguyen, & Lee, 2022).

NTRUEncrypt (NTRU) is a lattice-based public-key cryptosystem. It depends on difficulty of the Short Integer Solution (SIS) problem in polynomial rings over lattices. The NTRU encryption system was introduced in 1998. In 2017, Bernstein, van Vredendaal and two other researchers introduced NTRU Prime by making slight modifications to the primogenitor NTRU cryptography model. It has progressed to the third stage of the NIST post-quantum cryptography competition, emerging as a potential alternative candidate for key encapsulation algorithms. The primary differentiation between NTRU and NTRU Prime lies in the ring structures utilized within these systems (Levina, Kadykov, & Valluri, 2023). It functions within polynomial rings, and the system's security is predominantly influenced by the chosen parameter. The core idea behind NTRUEncrypt is to leverage the difficulty of certain lattice problems, specifically the Short.

Integer Solution (SIS) problem, for cryptographic security. The algorithm involves the use of polynomial rings and employs mathematical structures known as lattices to form the basis of its security (Zhu, y otros, 2022).

NTRUEncrypt is known for its efficiency in terms of key size and computational speed. It provides a balance between security and performance, positioning it as a viable option for secure communication in a post-quantum era. As with any cryptographic system, its security depends on presumed hardness of certain mathematical problems related to lattices. Ongoing research and analysis are essential to ensuring its robustness of against evolving cryptographic threats (Kim & Lee, 2020).

SABER is a lattice-based key encapsulation mechanism (KEM) designed for post-quantum cryptography. It was introduced as a candidate in the NIST Post-Quantum Cryptography Standardization project. The SABER algorithm is built on the hardness of certain mathematical problems related to lattices, rendering it impervious to attacks from both traditional and quantum computers (Lee, Seo, Kim, & No, 2022). The key features of SABER include its efficiency in terms of key sizes and computational performance. It operates on the Ring Learning With Errors (Ring-LWE) problem within polynomial rings over a module, which forms the foundation of its security. SABER offers a balance between security and efficiency, making it a potential candidate for securing communications in the post-quantum era. Ongoing research and analysis are crucial to ensuring the robustness of and adaptability of SABER against emerging cryptographic challenges (Dang, Mohajerani, & Gaj, 2023).

Lattice Based Encryption on IoT Systems

The increasing prevalence of IoT systems has sparked a growing need for robust and secure cryptographic solutions to safeguard communication and data exchange within these interconnected devices. Lattice-based encryption emerges as a promising paradigm in this context, offering a resilient approach to address the security challenges posed by both classical and potential quantum threats. Leveraging the mathematical intricacies associated with lattice problems, this encryption technique provides a foundation for securing sensitive information in IoT systems. This introduction delves into the application of lattice-based encryption within the realm of IoT, exploring its potential to enhance confidentiality, integrity, and overall cybersecurity in the evolving landscape of interconnected devices. In the realm of IoT, traditional cryptographic methods encounter challenges due to the heightened need for a larger number of keys. To address this demand for increased key generation, there is a necessity for the development of standardized lightweight cryptographic schemes and ciphers that exhibit enhanced agility and performance. This requirement has spurred interest in the implementation and application of lattice-based public key cryptosystems in this context.

Some areas of interest in IoT Systems using lattice-based encryption include End to End Encryption: email communication, widely used but often lacking encryption, poses a significant security concern. While many may overlook encryption for less sensitive content, those dealing with critical

information, such as military or political data, cannot afford even 0.01% uncertainty. In the new times of bitcoin, or electronic money, funds are electronically transferred among users using encryption algorithms. The effectiveness of the cryptography is crucial – robust encryption ensures protection against hacking, while a minor flaw can result in significant losses. Altering even a single bit in the database can escalate from a million to a billion. Secure network communications by establishing a secure communication medium, it is essential to enhance the encryption standard.

This has led to the creation of network protocols based on public-key cryptography, such as Netscape's Secure Socket Layer (SSL) and MIT's authentication service, Kerberos. Anonymous Remailers provide a service called remailing, where messages are sent with instructions on where to forward them, removing header information like the original address and forwarding only the message. This process involves multiple anonymous remailers to relay the message, ensuring that only the initial remailer knows the sender's identity. The encryption of such services is lattice-based, ensuring strong anonymity for the message sender. Disk encryption secures entire disks, eliminating concerns about leaving unencrypted data traces. Users define the encryption algorithm and use a password-protected system to access the encrypted disk, ensuring overall system security and preventing unauthorized access. In addition to these, various other domains like Authentication/Digital Signatures, Time Stamping, Pseudonymous Remailers, and many unexplored areas warrant attention (Pradhan, Rakshit, & Datta, 2019).

Latticed based encryption on IoT health

In the realm of IoT eHealth (Internet of Things in electronic health), the integration of lattice-based encryption stands as a pivotal development to ensure the confidentiality and integrity of sensitive health-related data. As the healthcare industry increasingly adopts IoT technologies for remote patient monitoring, data collection, and communication between devices, the need for robust security measures becomes paramount. Lattice-based encryption, leveraging the complexity of lattice problems, offers a resilient solution to protect the privacy of health information exchanged within these interconnected systems. This exploration focuses on the application of lattice- based encryption in the specific context of IoT eHealth, shedding light on its potential to fortify data security and uphold the trustworthiness of electronic health communication.

Gupta, Islam, Obaidat, Karati, & Sadoun (2021) developed an effective LAAC (Lattice- based Attribute-based control over access) protocol tailored for Internet of Things enabled electronic health systems. The researchers created a formal model and conducted a thorough analysis of the provable security of LAAC within that model. Their focus was on ensuring robust quantum attack robustness of, depending on the complexity assumptions on ISIS concern on the mathematical lattices.

Chuang, Fan, & Tseng (2018), mentioned the architectural layout of an e-health system that depends on Internet of Things (IoT) and propose a diagram. The diagram provides an overview of the interconnected components and their relationships within the system. This architecture likely encompasses various elements such as IoT devices, sensors, data storage, communication networks, and possibly cloud infrastructure. The visual representation aims to convey the intricate framework supporting the integration of IoT technologies in the context of e-health.

In the past few years, the significance of an e-health system has grown significantly, fueled by its growing demand in society. Ensuring security and privacy is imperative to authenticate legitimate users seamlessly and to ensure the privacy and integrity of data during transmission over public networks. Numerous authentication protocols have been developed for Internet of things based electronic health systems, employing conventional security methodologies.

Lattice-based cryptographic techniques effectively address security vulnerabilities present in traditional cryptographic methods, leading to enhancements in the computation resource and communication efficiency of Internet of things enabled applications (Chaudhary, Aujla, Kumar, & Zeadally, 2019).

Chaudhary et al., (2018) suggest an innovative lattice-based safe cryptography system tailored for the Ehealthcare infrastructure in foreseen smart industry. LSCSH incorporates a key exchange, important thing is that is lightweight, and a mechanism for authentication at multiple points. Through an evaluation of communication and computation costs, the proposed scheme has demonstrated its effectiveness when compared to other competitive schemes. The results obtained affirm the efficiency of the proposed scheme in comparison to existing alternatives.

Anusuya Devi & Kalaivani (2021) proposed the use of message authentication code alongside with lattice based encryption for healthcare and call it MAC-MELBC. Hybrid Encryption Algorithms (HEA) utilize a blend of cryptographic methods, incorporating both symmetric key techniques like Message Authentication Code which is abbreviated as MAC and asymmetric key approaches such as Modified and Enhanced Lattice-Based Cryptography also known and abbreviated as MELBC. This combination enhances the overall security of the encryption system. This approach leverages the strength of symmetric techniques for high-security levels and asymmetric techniques for effective key administration. Experimental results confirm that the HEA proposed algorithm offers superior security compared to other security algorithms.

Latticed based encryption on residential networks, smart grids and smart cities

In the evolving landscape of digital connectivity, the integration of lattice-based encryption has emerged as a pivotal solution, particularly in the realms of residential networks, smart homes, and smart cities. This introduction sets the stage for exploring the application and significance of lattice-based encryption in the context of residential networks, smart homes, and the broader framework of smart cities. J. Qian, y otros (2022) implemented a lattice-based encryption in a residential network for purposes of smart grid. The researchers introduced an aggregation signature scheme utilizing a novel batch RSA approach. Additionally, they put forth a scheme based on both

the aggregate signature scheme and a qualified homomorphic cryptosystem data. A comparative analysis with Abdallah, representative scheme revealed the heightened security of the proposed approach, incorporating seven essential properties including post-quantum robustness of and privacy. Moreover, the suggested scheme exhibited reduced computation and overhead. The cryptographic algorithms employed were lightweight, rendering the scheme well- suited for extensive intelligent communities and residential area networks. The proposed scheme by the authors possesses the capability to retrieve the individual message prior to aggregation. The privacy of Health Monitoring System (HSM) readings was safeguarded through the application of both the homomorphic cryptography scheme and the aggregate signature scheme. Through performance evaluation and security analysis, it was demonstrated that the proposed scheme ensures message consistency, integrity, user privacy, and accomplishes reduced communication and computational overhead.

As Smart Grids gain prominence globally, the predominant approach for effective management is Demand-Response. This approach involves encouraging clients or the user to adapt their energy consumption behaviors over time, responding to dynamic price fluctuations and promoting reduced energy usage the time where the demand is the most. It is overseen using a network of cloud servers which consistently observe the dynamics of supply and demand. This raises concerns about the security of the system's operations.

Desai, Dua, Kumar, Das, & Rodrigues (2018) propose an approach based on lattice to guarantee robust protection within the network, the suggested scheme has been demonstrated to withstand significant known attacks. The presented approach not only requires very little computation resources and time, but it also validates for security against well-known cryptographic threats, including several attacks. This approach fulfills the criteria of both authentication and front security.

Lattice based for industrial IoT systems

Talking about the Industrial Internet of Things abbreviated as IoT systems, the application of lattice-based cryptographic techniques presents an innovative and promising avenue for ensuring robust security. As IIoT systems become integral to industrial operations, the demand for secure and efficient communication within these networks has intensified. This introduction sets the stage for exploring the implementation of lattice-based cryptography in IIoT, addressing the unique security challenges posed by industrial environments.

The Cloud-assisted Industrial IoT (IIoT) depends on cloud computing to manage extensive storage service for data. To guarantee the privacy and the security of confidential industrial information, it is imperative to encrypt the information before storing it on a cloud storage server. Public-key encryption with keyword search (PEKS) facilitates users in searching for specific encrypted data using keywords. However, several existing PEKS schemes are constructed based on traditional hardness assumptions, rendering them potentially susceptible to threats from malicious actors that owned a quantum computer in the post quantum era. Additionally, these systems are prone to key exposure, meaning that if the encryption keys are compromised, the overall security of the system becomes vulnerable as well. Zhang, Xu, Wang, Zhang, & Wang (2019) introduced a forward-secure Public-Key Encryption with Keyword Search (FS-PEKS) scheme, utilizing lattice assumptions for cloud- supported Industrial IoT, ensuring post-quantum security. They integrated a delegation mechanism based on lattice cryptography into FS-PEKS to ensure front protection, ensuring the system's robustness of even if adversaries compromise the encryption keys. The researchers presented the foundational formal protection model addressing the front security dimension of PEKS, as well as offered substantiation of the security of FS-PEKS within this theoretical framework. Given the inherently low entropy of keywords associated with industrial data.

They expanded the capabilities of the scheme to withstand assaults related to insider attempts at keyword guessing. A thorough assessment of performance showcased the practicality of FS-PEKS in the context of cloud-assisted Industrial Internet of Things (IIoT).

Lattice-based encryption in vehicular IoT communication

The emergence of Vehicular Internet of Things (IoT) communication introduces new challenges and opportunities for securing the exchange of information within vehicular networks. Lattice-based encryption, grounded in mathematical lattice structures, stands as a promising cryptographic approach for addressing the unique security requirements of Vehicular IoT (VIoT). As vehicles become increasingly interconnected, the need for robust encryption methods becomes paramount to safeguard sensitive data and ensuring the integrity of communications. This introduction sets the stage for exploring the application of lattice-based encryption in VIoT communication, aiming to enhance the confidentiality, authentication, and robustness of data exchanged within the dynamic and interconnected environment of vehicular networks.

Li, He, Yang, Xie, & Choo (2022) propose a conditional technique for authorizing in vehicles ad hoc systems (VANET), a critical component of intelligent transportation systems. VANETs work on an open wireless communication ecosystem, exposing edge nodes to different levels of potential attacks. While existing numerous privacy-protection authenticate protocols with conditions in the present writings, many of these, se- cured by classical cryptographic primitives, lack robustness of against quantum attacks. The protocol introduced by the authors aims to simultaneously achieve mutual authentication and privacy protection. The security analysis demonstrates that the proposed protocol is resilient in the random oracle model, relying on the small integer solution problem. Furthermore, the authors assess the protocol's performance, highlighting its potential utility in real-world applications within VANETs.

Lattice Based Encryption for Internet of Things Space Info Networks

Asif (2021) present an innovative approach featuring an innovative a mechanism for semi-aggregated signatures and an

agreement mechanism for session keys were introduced. These mechanisms form the basis for a cutting-edge access authentication scheme called lattice-based access authentication (LAA) designed specifically for Space Information Networks (SIN). Notably, LAA exhibits characteristics such as large capacity, high reliability, and extensive coverage, making it well-suited for applications in the (IoT).

Nevertheless, SIN is susceptible to several attacks as a result of its highly vulnerable connections and the constrained work capacities of satellites Additionally, the instantaneous connection of numerous IoTDs to SIN results in signaling congestion, with no existing authentication protocol tailored for such massive IoTD deployments in SIN. To address these challenges, the authors propose two lattice-based authentication protocols within their model: 1) LAA for extensive Internet of Things Devices (IoTDs). The evaluation of performance showcases the effectiveness of the suggested protocols in terms of signaling overhead, trans- mission overhead, computational overhead, and authentication delay, confirming their ability to deliver substantial efficiency. Setting up a Vehicular AdHoc Network (VANET) involves the deployment and configuration of communication infrastructure to enable seamless connectivity among vehicles and infrastructure elements.

The first step in VANET setup is to equip vehicles with dedicated onboard units (OBUs) and roadside units (RSUs) installed along roadways. These units are equipped with communication interfaces such as Dedicated Short-Range Communication (DSRC) or Cellular Vehicle-to- Everything (C-V2X) technology. A robust security framework is implemented to safeguard communication channels and data exchanged between vehicles and infrastructure. Additionally, the deployment of GPS or other localization systems ensures accurate positioning information, vital for various VANET applications.

VANETs also require a centralized or distributed network management system to efficiently handle communication protocols, address assignment, and network optimization. Coordination with traffic management systems and local authorities is essential to integrate VANETs seamlessly into the overall transportation infrastructure. Overall, the successful setup of a VANET involves a well-coordinated effort to install and configure communication devices, implement security measures, and integrate with existing transportation systems for effective and safe vehicular communication (Luo, Ouyang, Liu, & Cao, 2019).

In the era of IoT advancement, Vehicular Ad-Hoc Networks (VANETs), a common IoT application, are introducing an increasing array of intelligent and convenient services into individuals' daily lives. Despite these advancements, VANETs face persistent challenges in maintaining privacy and security. To address these issues, (Liu, 2019) introducing a pioneering solution, the first-of-its-kind lattice-based encryption scheme that is double for authentication and prevents ring signature also known and abbreviated as DAPRS, the authors employ this innovation to put forth an original privacy-preserving authentication system tailored for Vehicular Ad-Hoc Networks (VANETs). Notably, this system comes equipped with an additional feature, providing enhanced security and protection against potential threats stemming from quantum computers. The novel construction has been validated for security against chosen message attacks. Moreover, the proposed scheme exhibits superior performance compared to other ring-signature methods talking about both the process wait time needed for the message signing and verification phases, as well as the length of the signature.

Thorough analyses confirm the demonstrated security and efficiency of the scheme when applied within the context of Vehicular Ad-Hoc Networks development of an agile infrastructure that can swiftly adapt to the evolving threat landscape. This entails not only investing in cutting-edge technologies but also fostering a culture of innovation and adaptability. Continuous investments in research have become the cornerstone of this strategy, enabling organizations to stay ahead in understanding and developing solutions that can effectively counter the challenges posed by quantum advancements.

Dynamic key management emerges as a linchpin in the future of cryptographic robustness of Organizations must move beyond static encryption protocols, implementing strategies that allow for the seamless rotation and adaptation of encryption keys. Collaborative threat intelligence efforts amplify the collective strength of the cybersecurity community. By sharing insights and intelligence, organizations can create a unified defense against emerging threats associated with quantum computing. Simultaneously, adherence to regulatory compliance requirements specific to quantum-resistant cryptography is paramount. Organizations need to align their cybersecurity practices with evolving regulations to ensure a robust and compliant approach. Moreover, a key element in future-proofing cybersecurity involves a comprehensive focus on user education and awareness. Informed users are essential in recognizing and (VANETs).

IoT cloud systems

Bagla, et al., (2023) introduce lattice-based cryptography as a means to enhance the security of Internet of Things (IoT) and cloud systems. The primary focus is on addressing two key challenges within lattice-based encryption. The paper conducts a comprehensive comparison between the pros and drawbacks of lattice-based cryptography in contrast to traditional methods such as RSA and elliptic curve cryptography. An innovative concept presented, specifically tailored for Internet of Things and the cloud, aiming to ensure confidentiality and integrity throughout the process of data aggregation. The paper delves into various facets. Performance and protection assessments systematically evaluate the proposed algorithm in comparison to alternative data aggregation techniques, highlighting its efficacy in thwarting threats and computational effectiveness.

Additionally, the written work acknowledges the limitations of the proposed approach and puts forward potential avenues for more research in the following years. In conclusion, the suggested lattice-based cryptography stands out as a prospective solution to enhance privacy and security in vulnerable IoT and cloud systems. This positions it as a practical and compelling option for broad implementation.

Future preparedness for post-quantum cryptography

Considering the imminent impact that quantum computing is expected to exert on cryptographic practices, organizations find themselves at the forefront of a paradigm shift in cybersecurity. To fortify their defenses against potential vulnerabilities, it is imperative for these entities to adopt a forward-looking stance.

A critical aspect of future preparedness involves mitigating potential quantum-related threats. Cross-sector collaboration acts as a force multiplier, fostering shared resources and knowledge across industries. Establishing comprehensive incident response planning further solidifies an organization's ability to swiftly and effectively counteract potential security breaches.

As a proactive measure, organizations should consider implementing quantum-safe cryptographic policies. This involves integrating cryptographic algorithms that are resilient to quantum attacks. Quantum Key Distribution (QKD) technologies offer a cutting-edge solution by leveraging quantum principles for secure key exchange. Additionally, adaptive training programs ensure that personnel possess the necessary skills and knowledge to navigate the intricacies of quantum- resistant cybersecurity. Collaborating with vendors becomes instrumental in staying at the forefront of quantum-resistant security measures, ensuring that the technology stack remains up-to-date and resilient.

In conclusion, the quantum era necessitates a holistic and proactive approach to cybersecurity. By encompassing agile infrastructure development, continuous research, dynamic key management, collaborative efforts, regulatory compliance, user education, cross-sector collaboration, incident response planning, quantum-safe policies, QKD integration, adaptive training, and vendor collaboration, organizations can effectively navigate the evolving landscape of cybersecurity. This multifaceted strategy positions them to embrace the challenges and opportunities presented by quantum advancements, thereby ensuring a robust and resilient cybersecurity posture (I. T. L. Computer Security Division, 2024).

CONCLUSION

In conclusion, the findings and analyses presented in this study provide valuable insights into the intricate landscape of lattice-based post-quantum cryptography and its multifaceted applications, shedding light on its significance and potential contributions to the ever-evolving field of secure communication, particularly within Internet of Things (IoT) systems.

As conclusion on lattice-based encryption, it becomes evident that this cryptographic paradigm stands as a resilient bulwark against emerging challenges, particularly those by quantum computing. The lattice structures, forming the foundation of this encryption approach, showcase not only mathematical complexity but also practical versatility across cryptographic primitives.

Finally, the exploration of lattice-based encryption for IoT systems underscores its promising role in addressing contemporary security challenges. The inherent post-quantum robust- ness of lattice-based cryptographic techniques positions them as a viable solution for ensuring the confidentiality, integrity, and authenticity of data in IoT environments. The surveyed literature has highlighted the adaptability of lattice-based schemes to the limitations imposed by constrained resources of IoT devices, showcasing their potential applicability in diverse IoT applications. The integration of lattice-based encryption contributes to a robust security foundation, offering a proactive defense against emerging threats, including those posed by quantum advancements. However, successful implementation requires addressing performance considerations and fostering broader awareness within the IoT community. As we advance into an era of increasingly interconnected devices, lattice- based encryption stands as a valuable ally in fortifying the security posture of IoT systems, paving the way for a more secure and resilient IoT landscape.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Financing

None.

Use of AI

Minimal. Grammarly was used to review the grammar and punctuation of the manuscript.

REFERENCES

Anusuya Devi, V., & Kalaivani, V. (2021). Hybrid cryptosystem in wireless body area networks using message authentication code and modified and enhanced lattice-based cryptography (MAC-MELBC) in healthcare applications. Concurrency and Computation: Practice and Experience, 33(9), e6132. doi:10.1002/cpe.6132

Asif, R. (March de 2021). Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. (MDPI, Ed.) *IoT, 2*(1). doi:10.3390/iot2010005

Bagla, P., Sharma, R., Mishra, A. K., Tripathi, N., Dumka, A., & Pandey, N. K. (2023). An Efficient Security Solution for IoT and Cloud Security Using Lattice-Based Cryptography. (IEEE, Ed.) *2023 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, 462–468. doi:10.1109/ETNCC56807.2023.10175695

Bhatia, V., & Ramkumar, K. R. (October de 2020). An Efficient Quantum Computing Technique for Cracking RSA Using Shor's Algorithm. *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, 89–94. doi:10.1109/ICCCA49541.2020.9250806

Castelluccio, M. (June de 2021). The Quantum Threat to Cryptography. *Strategic Finance*(12), 55–56.

Cavaliere, F., Mattsson, J., & Smeets, B. (September de 2020). The security implications of quantum cryptography and quantum computing. (Elsevier, Ed.) *Network Security*, 9–15. doi:10.1016/S1353-4858(20)30105-7

Chaudhary, R., Aujla, G. S., Kumar, N., & Zeadally, S. (2019). Lattice-Based Public Key Cryptosystem for Internet of Things

Environment: Challenges and Solutions. *IEEE Internet of Things Journal, 6*(3), 4897–4909. doi:10.1109/JIOT.2018.2878707

Chaudhary, R., Jindal, A., Aujla, G. S., Kumar, N., Das, A. K., & Saxena, N. (April de 2018). LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. (IEEE, Ed.) *IEEE Communications Magazine, 56*(4), 24–32. doi:10.1109/MCOM.2018.1700787

Chuang, Y.-L., Fan, C.-I., & Tseng, Y.-F. (2018). An Efficient Algorithm for the Shortest Vector Problem. (IEEE, Ed.) *IEEE Access, 6*, 61478–61487. doi:10.1109/ACCESS.2018.2876401

Córcoles, A. D. (August de 2020). Challenges and Opportunities of Near-Term Quantum Computing Systems. (IEEE, Ed.) *Proceedings of the IEEE, 108*(8), 1338–1352. doi:10.1109/JPROC.2019.2954005

Dang, V. B., Mohajerani, K., & Gaj, K. (2023). High-Speed Hardware Architectures and FPGA Benchmarking of CRYSTALS-Kyber, NTRU, and Saber. (IEEE, Ed.) *IEEE Transactions on Computers, 72*(2), 306–320. doi:10.1109/TC.2022.3222954

Desai, S. K., Dua, A., Kumar, N., Das, A. K., & Rodrigues, J. J. (2018). Demand Response Management Using Lattice-Based Cryptography in Smart Grids. (IEEE, Ed.) *2018 IEEE Global Communications Conference (GLOBECOM)*, 1–6. doi:10.1109/GLOCOM.2018.8647560

Gupta, D. S., Islam, S. H., Obaidat, M. S., Karati, A., & Sadoun, B. (September de 2021). LAAC: Lightweight Lattice-Based Authentication and Access Control Protocol for E-Health Systems in IoT Environments. (IEEE, Ed.) *IEEE Systems Journal, 15*(3), 3620–3627. doi:10.1109/JSYST.2020.3016065

Hamza, A., & Kumar, B. (December de 2020). A Review Paper on DES, AES, RSA Encryption Standards. (IEEE, Ed.) *2020 9th International Conference on System Modeling and Advancement in Research Trends (SMART)*, 333–338. doi:10.1109/SMART50582.2020.9336800

Hegde, S. B., Jamuar, A., & Kulkarni, R. (July de 2023). Post Quantum Implications on Private and Public Key Cryptography. *2023 International Conference on Smart Systems for Applications in Electrical Sciences (ICSSES)*, 1–6. doi:10.1109/ICSSES58299.2023.10199503

I. T. L. Computer Security Division. (2024). *Post-Quantum Cryptography — CSRC — CSRC*. Obtenido de NIST — Computer Security Resource Center (CSRC): https://csrc.nist.gov/projects/post-quantum-cryptography

J. Qian, Q., Cao, Z., Lu, M., Chen, X., Shen, J., & Liu, J. (February de 2022). The Secure Lattice-Based Data Aggregation Scheme in Residential Networks for Smart Grid. (IEEE, Ed.) *IEEE Internet of Things Journal, 9*(3), 2153–2164. doi:10.1109/JIOT.2021.3090270

Khalid, A., McCarthy, S., O'Neill, M., & Liu, W. (June de 2019). Lattice-based Cryptography for IoT in A Quantum World: Are We Ready? *2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*, 194–199. doi:10.1109/IWASI.2019.8791343

Kim, T., & Lee, M.-K. (2020). Efficient and Secure Implementation of NTRUEncrypt Using Signed Sliding Window Method. (IEEE, Ed.) *IEEE Access, 8*, 126591–126605. doi:10.1109/ACCESS.2020.3008182

Lee, D.-H., Seo, E.-Y., Kim, Y.-S., & No, J.-S. (2022). Rethinking on Ciphertext Equality Check of Decapsulation of NIST PQC Standardization 3rd Round Finalist Candidate Saber. (IEEE, Ed.) *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 1483–1486. doi:10.1109/ICTC55196.2022.9952361

Levina, A., Kadykov, V., & Valluri, M. R. (2023). Security Analysis of Hybrid Attack for NTRU-Class Encryption Schemes. *IEEE Access*, 109939–109952. doi:10.1109/ACCESS.2023.3321693

Li, Q., He, D., Yang, Z., Xie, Q., & Choo, K.-K. R. (April de 2022). Lattice-Based Conditional Privacy-Preserving Authentication Protocol for the Vehicular Ad Hoc Network. (IEEE, Ed.) *IEEE Transactions on Vehicular Technology, 71*(4), 4336–4347. doi:10.1109/TVT.2022.3147875

Liu, J. e. (October de 2019). Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks. (T. U. IEEE, Ed.) *Tsinghua Science and Technology, 24*(5), 575–584. doi:10.26599/TST.2018.9010131

Luo, Y., Ouyang, X., Liu, J., & Cao, L. (2019). An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems. *IEEE Access, 7*, 38507–38522. doi:10.1109/ACCESS.2019.2906052

Maslov, D., Nam, Y., & Kim, J. (January de 2019). An Outlook for Quantum Computing [Point of View]. *Proc. IEEE*(1), 5–10. doi:10.1109/JPROC.2018.2884353

Nguyen, T. T., Nguyen, T. T., & Lee, H. (January de 2022). An Analysis of Hardware Design of MLWE-Based Public-Key Encryption and Key-Establishment Algorithms. *Electronics*, Art. no. 6. doi:10.3390/electronics11060891

Ott, D., Peikert, C., & al., e. (2019). *Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility*. doi:10.48550/arXiv.1909.07353

Pradhan, P. K., Rakshit, S., & Datta, S. (2019). Lattice Based Cryptography: Its Applications, Areas of Interest & Future Scope. (IEEE, Ed.) *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, 988–993. doi:10.1109/ICCMC.2019.8819706

Román, R., Arjona, R., López-González, P., & Baturone, I. (2022). A Quantum-Resistant Face Template Protection Scheme using Kyber and Saber Public Key Encryption Algorithms. *2022 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 1–5. doi:10.1109/BIOSIG55365.2022.9897052

Tateiwa, N. e. (2021). CMAP-LAP: Configurable Massively Parallel Solver for Lattice Problems. (IEEE, Ed.) *2021 IEEE 28th International Conference on High Performance Computing, Data, and Analytics (HiPC)*, 42–52. doi:10.1109/HiPC53243.2021.00018

Zhang, X., Xu, C., Wang, H., Zhang, Y., & Wang, S. (2019). FS-PEKS: Lattice-based Forward Secure Public-key Encryption with Keyword Search for Cloud-assisted Industrial Internet of Things. (IEEE, Ed.) *IEEE Transactions on Dependable and Secure Computing*. doi:10.1109/TDSC.2019.2914117

Zhu, Y., Liu, Y., Wu, M., Li, J., Liu, S., & Zhao, J. (January de 2022). Research on Secure Communication on In-Vehicle Ethernet Based on Post-Quantum Algorithm NTRUEncrypt. (MDPI, Ed.) *Electronics, 11*(6), Art. 6. doi:10.3390/electronics11060856