An Effective and Compact Post-Quantum Lattice Cryptosystems for Secure Transmission

Venkata Sathish Kumar Badithala
Research Scholar, ECE dept.
NIT Nagaland
Nagaland, India
sathishbv.ece.nitn@gmail.com

Dr. Roji Chanu Palungbam
Assistant Professor, ECE dept.
NIT Nagaland
Nagaland, India
rojichanu@gmail.com

***Abstract*— With the launch of 5G, the quantity of Internet of Things (IoT) devices available is increasing rapidly. They are present in a large variety of gadgets, from healthcare tracking equipment to our cell phones. Traditional cryptography algorithms will become outdated and vulnerable to quantum assaults using Shor's algorithm with the introduction of 5G and quantum computing. Making Quantum Secure Cryptography Algorithms suitable for 5G IoT settings is therefore necessary. The traditional RSA algorithm, which forms the foundation of many proposed cryptosystems, has exceptional security levels for online integrity and secrecy. However, these levels can be affected by cutting-edge attacks, particularly when it comes to various forms of producing, transferring, and evaluating data by IoT applications. For IoT-driven cloud-based applications, we suggest RSA based on a post-quantum lattice and a lightweight post-quantum SIMECK to protect shared data and information.**

Keywords— IoT applications, post-quantum cryptography, lattice-based cryptography, RSA, SIMECK

I. INTRODUCTION

Assuring transmission quality, determined using the bit error rate, is the first prerequisite for communication. Furthermore, one of the most important and difficult requirements is user oriented information security, which guarantees the information integrity and can fend off attempts to steal or alter data. In recent times, there has been a rapid increase in interest in quantum computing because of the high processing power requirements of Internet of Things (IoT)-based cloud applications [1]. The IoT is a worldwide network of physical objects, identified as "things," which have communications and computing capabilities providing their identification, monitoring, and control through the Internet. The vast quantities of data that these billions of devices will gather about the real world in their surroundings must be sent to a central location (like a cloud server) for processing and archiving. Nevertheless, this conventional IoT paradigm, in which end devices mostly gather data and information mining, further processing, and taking decisions are mainly carried out in the cloud, has led to several issues related to confidentiality and security, latency, and bandwidth concerns. Edge devices need strong defence against a variety of threats since they may handle and keep private data about their owners or users. If the attacker is successful in inserting one or more controlled devices into the network, they can target an edge device from two separate angles: either through the Internet, or through other connected devices. A sophisticated security architecture is necessary to counter these attacks, and it must take into consideration the unique limitations and needs of the IoT. The fact that many IoT devices have extremely limited computational power and network bandwidth is one of the primary obstacles to a secure IoT. The research and development of quantum computers has become the priority of professionals and specialists in computers. Furthermore, the development of quantum machines and quantum methods such as Shor's algorithm affects the efficacy of cryptography based on mathematical difficulties [2]. Therefore, in order to fend against potential attacks by quantum computers, researchers have started studying and testing cryptography techniques.

ISBN : 978-81-978522-2-0 https://doi.org/10.37285/bsp.oaisem2025.31

II. LITERATURE

A. Pre-Quantum Cryptography

These days, it is inconceivable to think about information security without cryptography. Numerous techniques exist for using cryptography to safeguard the confidentiality and integrity of data. Cryptography is cleverly used by many confidentiality-related software and hardware products to accomplish the specific goal of security. Cryptographic activities, like encryption and decryption, key creation, authentication, signatures, etc., are described by well-defined protocols, rules, stages, or mathematical equations known as cryptographic algorithms [3].

There are two primary categories that can be used to characterize cryptographic algorithms: symmetric and asymmetric algorithms. Fig. 1 convey several cryptography techniques consist of complex mathematical functions that are easy to perform in one way while very difficult to calculate in the other [4]. These algorithms can be identified as one-way functions, or acronyms for short.

1) Symmetric Cryptographic Algorithms:

In symmetric cryptography, data is encrypted and decrypted with the same key by both the sender and the recipient. These algorithms are comparatively easy to build and very efficient. However, since the key must to be safely transferred between both individuals prior to conversation commences, key management in symmetric cryptography presents serious difficulties. The main types of attacks that symmetric cyphers are vulnerable to include chosen-plaintext, known-plaintext, linear, and differential cryptanalysis.

2) Asymmetric Cryptographic Algorithms:

Asymmetric cryptography, often known as public-key cryptography, uses two keys: a private key that is kept hidden and a public key that is made public. Using the recipient's public key, the sender encrypts the data, which the recipient decrypts with their private key. Even while asymmetric algorithms are more resource-intensive and demand greater amounts of duration and power, they satisfy important security criteria such as digital authentication and cryptographic key establishment. The main risks to public-key cryptography are attacks known as man-in-the-middle, chosen-ciphertext attacks, and focused assaults related to the beneath mathematical problems.

Using brute force methods algorithms that are symmetric or asymmetric can be targeted [5]. An attacker executing a strategy known as brute force attempts all the keys that can be provided. The size of the key and the amount of processing power needed to generate and apply every key that might be used to crack the encryption determine how resistant the algorithms are. The degree of difficulty of mathematical problems such as the discrete logarithm problem (DLP), its elliptic curve counterpart, the ECDLP, and the integer factoring problem (IFP) determines the security of existing public key cryptosystems. But it's commonly accepted that a quantum computer could handle all of these issues efficiently, which means that practically every digital signature and key exchange system in use today is vulnerable to attack [6]. The processing capacity is always increasing, and as a result, cryptography algorithms must likewise adapt to stay strong. The majority of encryption methods in use today can withstand attacks from a traditional computer. The revolutionary computing device known as a quantum computer is entirely distinct from traditional computers. A quantum computer performs far faster than a conventional one.

B. Post-Quantum Cryptography

A quantum computer is a computer which offers calculations with the ideas of quantum physics. Quantum bits, or qubits, are used by quantum computers instead of classical ones, having bits which have only two values: 0 or 1. Qubits can exist in several states at once. The qubits' states are represented by the symbols $|0\rangle$ and $|1\rangle$. The qubits can be at 0 and 1 at the same time. Certain computations can be performed by quantum computers far more quickly thanks to this qubit property. One mathematical difficulty that quantum computers can solve, for instance, is factoring big integers, which is computationally unfeasible of connection to traditional computers [7].

Quantum computers make use of two essential aspects of quantum mechanics: superposition and entanglement. Unlike classical bits that can only exist in a binary state, qubits can exist continuously in several states due to superposition. Qubits are connected by a special quantum phenomenon called entanglement, which causes the states of one to instantly influence the states of the other regardless of their distance from one another. 2^n values can be represented by n qubits in the condition of superposition state. Every state permits concurrent operation. In mathematics, a qubit under a state of superposition of quantum is represented as follows:

$$|\Psi >= \alpha|1 > +\beta|0 > \quad (1)$$

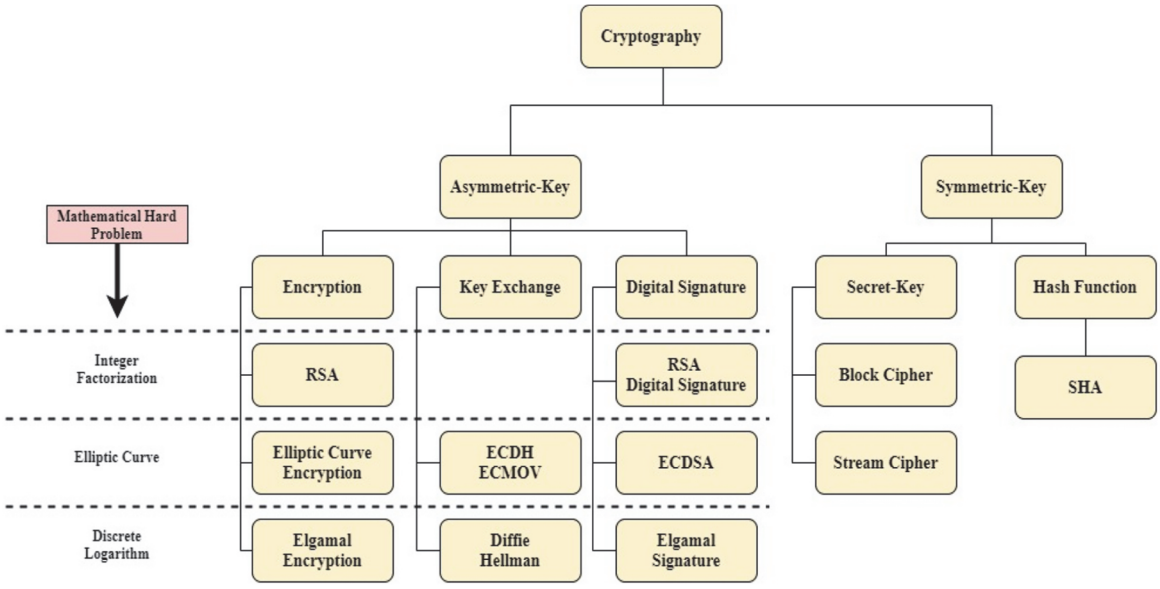

Fig. 1. Branches of cryptography and the related mathematical difficulties.

One of the two eigenvalues generated by any measurement on these qubits will always be observed; however, we are unable to predict which one will be [8]. The probability amplitudes are indicated by α and β. In particular, $|\alpha|^2$ represents the likelihood of an outcome of $|1\rangle$ having a value of 1, and $|\beta|^2$ represents the likelihood of an outcome of $|0\rangle$ having a value of 0. This equation is guaranteed when that state is normalized.

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2)$$

Except for measurements, every activity in quantum computing is reversible. This reversibility requires that the quantum gates have a similar quantity of input as well as output bits, making it possible to retrieve the beginning state from the consequent state without requiring extra information.

The field of cryptography referred to as "post quantum cryptography (PQC)" is responsible for developing encryption methods that prevent an adversary employing quantum computing [9]. End of the 1990s saw the beginning of the majority of the PQC research. At that point, computer scientists and mathematicians noticed that commonly used cryptographic schemes, such elliptic curve cryptography (ECC) and Rivest–Shamir–Adleman (RSA), which depend on mathematical problems that a quantum computer can resolve

quickly, perhaps cracked by quantum computing. The identification of this issue sparked a fresh focus on creating cryptographic algorithms that might fend against attacks using quantum technology.

Lattice-based cryptography, code-based cryptography, hash-based digital signatures, and multivariate cryptography are the four main approaches for implementing public key PQC [10]. Lattice-oriented Frameworks are mathematical structures which are used to create encryption keys, and they form the foundation of cryptography. Lattice-based security is thought to be immune to attacks based on both conventional and quantum techniques because some lattice-based cryptosystems combine small key and ciphertext/signature sizes with good security guarantees (i.e., a decrease of worst-to-average instances with great efficiency), they are promising PQC candidates. Code-based cryptosystems generate a one-way function using an error-correcting code; its security is dependent on how difficult it is to decode a message including random errors and reconstruct the code structure. Although it needs very large key sizes, its immunity from quantum-based assaults has been verified. Hash-based Hashing functions are mathematical operations that take input data of any length and output a predetermined length; one sort of PQC that uses them is cryptography [11]. Benefit of hash-based encryption is that it doesn't require big key sizes and is comparatively simple to implement. Still, there are issues with hash-based systems' effectiveness. Compared to number-theoretic signature techniques, hash-based digital signature schemes—first presented by Ralph Merkle in 1979—have fewer security presumptions and are expected to resist the capabilities of quantum computing. Multivariate cryptography is another approach to PQC that depends on the difficulty of resolving a set of multivariate polynomial equations. Small key sizes are a characteristic of multivariate encryption, although there are some attack vectors that can exploit this weakness.

The creation of lightweight post-quantum cryptography primitives for Internet of Things devices is one of the main areas of research because it has already increased the attack surface available to adversaries. With the growing number of IoT devices, lightweight cryptography has become essential. IoT devices use encrypted data to interact with one another since sensitive data may be involved. Research is also needed in the crucial area of lightweight post-quantum cryptography. Low-overhead, quantum-safe algorithms are needed [12].

III. Methodology and Results

IoT networks involve data aggregation, data transfer, and data sensing via small sensor nodes. To safeguard the data utilized in IoT networks, many security techniques have been implemented in the past. Lattice-based encryption, with its low key sizes, versatility, and quantum resilience, seems to be a better alternative to the current public-key cryptography. The degree of security provided by lattice-based encryption is influenced by the intricacy of the two separate shortest vector problem as well as nearest vector problem.

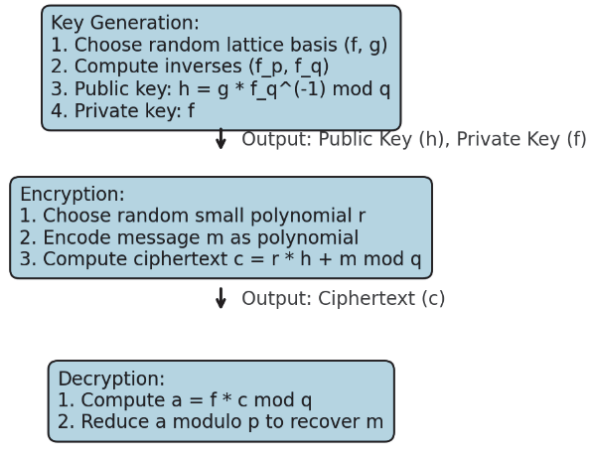

Fig. 2. Flowchart of Lattice –based RSA.

While classical computers are thought to find it difficult to solve conventional RSA [13], since it cannot prolong the key to avoid quantum attacks and keep up with the rate of innovation in quantum computing, this method is not considered quantum-safe. Suggested using a post-quantum lattice-based RSA (LB-RSA) for cloud applications running on IoT devices to protect the information shown in Fig. 2 and other shared data. Bernstein et al.'s post-quantum RSA security design [14] founded on integer factorization; however, we have applied the idea of vectors factorization in lattice-based RSA. In LB-RSA, instead of using the product of two huge prime integers, the cross-product of a pair n-dimensional vectors is employed. Under the worst-case hardness assumption, the suggested approach is provably secure in addition to be relatively simple to understand, effective, and scalable.

SIMECK is a lightweight block cipher designed for efficiency in constrained environments. Its methodology includes the use of a simple F-function, a straightforward key schedule, and an iterative encryption and decryption process shown in Fig.3. Block size and Key size can vary, we used 64 bits and 128 bits respectively and 44 rounds performed. The F-function is a simple and effective non-linear function used in the encryption process. This makes it well-suited for applications in IoT and other resource-limited systems.

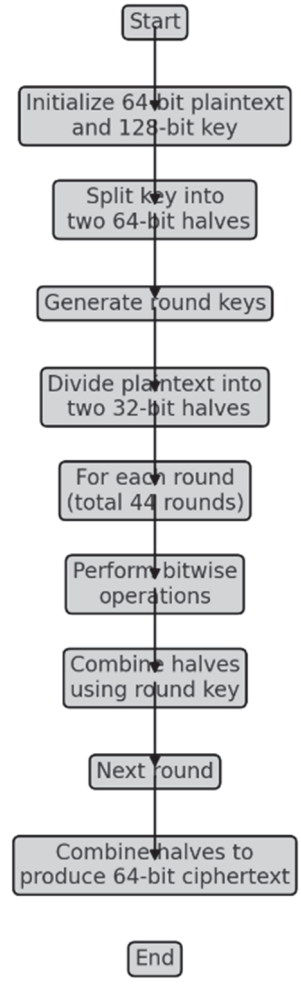

Fig. 3. Flowchart of SIMECK 64/128.

IV. CONCLUSION

The growing number of Internet of Things (IoT) devices in many applications, such as traffic management, health care, and home automation, has increased the need for safe data collection and analysis. Most of the information we interact with these days is encrypted using a process called public-key cryptography, exposing it susceptible to quantum computing. It's likely that a large number of hackers, whether state-sponsored or acting on behalf of nation-states, are capturing and intercepting encrypted messages in anticipation of being able to decrypt them later on when quantum computing resources become available. LB-RSA and SIMECK 64/128 are an efficient, lightweight cipher tailored for environments with limited resources, balancing simplicity, and security to provide a practical solution for post-quantum cryptographic needs.

REFERENCES

[1]. C. Stergiou, K. E. Psannis, B.G. Kim, and B. Gupta, “Secure integration of IoT and cloud computing”, Future Gener. Comput. Syst. 2018, vol. 78, pp. 964-975.

[2]. Regev O. “On Lattices, Learning with Errors, Random Linear Codes, and Cryptography”. Journal of ACM 2009, vol. 56, pp. 1–40.

[3]. Cryptographic algorithm - Glossary | CSRC. (n.d.). Retrieved April 5, 2022, from https://csrc.nist.gov/glossary/term/cryptographic_algorithm.

[4]. Broadbent Anne, Schaffner Christian, “Quantum cryptography beyond quantum key Distribution", Des Codes Cryptogr 2015, vol. 78, pp.351–82. https://doi.org/10.1007/ s10623-015-0157-4.

[5]. Diffie W, Hellman M, “New directions in cryptography”, IEEE Trans Inf Theor 1976, vol. 22(6), pp.644–54. https://doi.org/10.1109/tit.1976.1055638.

[6]. C. Cheng et al., “Securing the Internet of Things in a Quantum World,” IEEE Commun. Mag., vol. 55, no. 2, Feb. 2017, pp. 116–20.

[7]. Duc-Thuan Dam, Thai-Ha Tran, Van-Phuc Hoang, Cong-Kha Pham, and Trong-Thuc Hoang, “A Survey of Post-Quantum Cryptography: Start of a New Race”, MDPI-cryptography 2023, vol. 7(40), pp. 1-18. https://doi.org/10.3390/cryptography7030040.

[8]. Hey. T, “Quantum computing: an introduction”, Comput. Control. Eng. J. 1999, vol. 10, pp. 105–112.

[9]. Kaushik, A., Yakkali, R. T., Indu, S., Ahmed, F., Gupta, D., Nayar, R., and Yadav, S. “A self-configurable event coverage approach for wireless sensor networks”, International Journal of Mobile Computing and Multimedia Communications 2019, vol. 10(2), pp. 1–18.

[10]. D. J. Bernstein, “Introduction to Post-Quantum Cryptography”, Springer, 2009, pp. 1–14.

[11]. Regev O, “On Lattices, Learning with Errors, Random Linear Codes, and Cryptography”, J. ACM 2009, vol. 56, pp. 1–40.

[12]. Ritik Bavdekar, Eashan Jayant Chopde, Ankit Agrawal, Ashutosh Bhatia and Kamlesh Tiwari, “Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations”, International Conference on Information Networking (ICOIN), 2023, DOI: 10.1109/ICOIN56518.2023.10048976

[13]. M. Campagna, “Quantum safe cryptography and security: An introduction, benefits, enablers and challenges”, in Proc. Eur. Telecommun. Stan- dards Inst., 2015, pp. 1-64.

[14]. D. J. Bernstein, ``Post-quantum RSA," in Proc. Int. Workshop Post- Quantum Cryptogr. Cham, Switzerland: Springer, 2017, pp. 311-329.