UtilitasMathematica

ISSN 0315-3681 Volume 122, 2025

A Novel and Hybrid Post Quantum Cryptographic algorithm for Enhanced Security in Wireless Networks

Mutya Sirisha Adapa 1[0000-0001-7937-6059] **Dr.P.Venkateswara Rao**[2] [0000-0002-8499-5994]

1Research Scholar, 2Associate Professor, Department of Computer Science and Engineering

[1,2] AKNU College of Engineering, Adikavi Nannaya University,
Rajamahendravaram, Andhra Pradesh, India
mutyasirisha.thota@gmail.com

Abstract:

Cryptography enables modern-day secure communication. The advancement of quantum algorithms has made classical cryptosystems ineffective. Important data has been encrypted and verified using digital signatures and cryptography. Classical cryptography systems were on the edge of collapse when quantum algorithms were introduced, since quantum computers can solve complex problems in less time. It is important to be prepared for future threats, even if standard cryptosystems are presumably safe for the moment being because quantum computing is not yet developed. One use of quantum cryptography is quantum key distribution (QKD), which is a way to safely share encryption keys between communication parties by utilizing quantum physics. Hybrid classical-quantum methods offer protection from both classical & quantum attackers, which can help smooth the way for the change. We introduce a new way to build hybrid encryption schemes from preexisting ones. First, the paper examines classical cryptosystems vulnerability to quantum computers. Then, it investigate into different families of post-quantum cryptosystems, checks in on the NIST's post-quantum cryptography consistency process, and finally, compares the performance of algorithms using post-quantum cryptography on various platforms. Along with discussing and evaluating current methods, this paper also discusses a novel hybrid quantum cryptographic system that employs message authentication codes with enhanced lattice based cryptography.

Keywords- cryptosystem, security, privacy, post-quantum cryptography, lattice-based cryptography, and quantum computing

1. Introduction:

Today's society is all about communicating to each other. The Internet is the foundational element for any engagement in modern culture. It becomes necessary to safeguard and uphold the confidentiality of transmitted data. The data security and privacy of sensitive information is the only concern of the many academics that work in the area of cryptography, which employs a wide range of security techniques to that end. In the realm of information security, cryptography is a cornerstone. Only the sender and the intended receiver can decipher the encrypted data, which is why cryptography is both an art form and a science. Complex mathematical functions are the basis of most modern cryptography algorithms. Assumptions of computation difficulty are the basis of cryptographic algorithm design. Integer factorization is an example of an asymmetrical task; while it's easy to multiply two integers, factoring a 1000-digit integer is far more challenging.

An encryption technique that uses a public key & a private key to encrypt data; the key's computational impossibility makes it ideal for use in secure communication. Traditional public-key

encryption relies on the idea that while classical computers can swiftly multiply large prime numbers, doing the inverse would take a very long time, at least hundreds of years. The advent of quantum computing has made deciphering data encrypted with traditional public-key cryptography much simpler.

A technology founded on the tenets of quantum theory, quantum computing outperforms classical computing methods in terms of speed. In the hands of quantum computers, classical cryptography techniques are as good as dead. The current information technology infrastructure will become entirely vulnerable during the transition to the quantum computer, necessitating the creation of cryptographic methods that are either quantum-safe or quantum-resistant. Modern supercomputers still can't handle the most complicated scientific problems, but quantum computers could change all that. In every situation, there are opposing viewpoints. Quantum computers, on the one hand, give us reason to be optimistic about our ability to solve several issues in various domains within a limited amount of time. But in other cases, their arrival could pose a danger to our safety. The field of cryptanalysis is one such example. Cracking codes is known as cryptanalysis. Regrettably, quantum computers will eventually be able to crack modern cryptography algorithms that depend on challenging mathematical problems. Despite quantum computers' promise to transform many sectors by solving difficult issues, they pose a serious danger to the safety of current cryptographic methods [1].

Approaching threats posed by developments in quantum computing threaten data security that has hitherto depended on cryptographic protocols upheld by cyphers like RSA or ECC. A big danger to existing encryption systems are quantum algorithms like Grover's and Shor's algorithms. It is possible that RSA and ECC will be cracked soon by quantum computers. Classical computers just cannot complete such a task within a reasonable amount of time. While quantum computing does present some exciting new possibilities for contemporary technology, it also opens the door to some serious security risks for sensitive information[2]. A new set of cryptographic algorithms, post-quantum cryptography (PQC), is required to get around this integrated ambiguity. These algorithms will be difficult for quantum computers to crack.

It bears highlighting that new cryptographic algorithms and remedies must be evaluated based on their various characteristics, including their legal implications. As we move towards post-quantum cryptography, it is essential to have a good grasp of the pros and cons of algorithms in terms of security levels and practical applications. This knowledge can aid in choosing the right solutions for different security scenarios, bearing in mind the various legal requirements and the values and rights at play in each real-world setting. The driving force behind this paper's subject is the realization, made possible by quantum computers, that cyber security must foresee and evade potential dangers. European quantum initiatives, which promote quantum research excellence, are an additional factor that supports exploring the domain of post-quantum cryptography. The goal of this endeavor is to build, refine, and test a framework that will make the shift from classical to post-quantum cryptography as painless and efficient as possible.

New cryptosystems that are impenetrable by classical and quantum computers are the focus of Post Quantum Cryptography. Based on the fundamental issue that the security is built around, cryptosystems are categorized into multiple families. Both classical & quantum computers are

thought to be unable to solve these fundamental challenges. Cryptography based on lattices or isogenies, cryptography based on codes or non-commutative algorithms, digital signatures based on hashes, and multivariate cryptography are the main families [4]. Multiple NIST programs are working toward the common goal of developing secure quantum algorithms for use in cryptography. Whenever the necessity arises, we will discuss on the entries received from all around the world in an effort to speed up the ongoing study into producing a standard [5]. Commenting on the security of several cryptographic algorithms in the presence of quantum adversaries, this paper explores the implications of quantum computers on these methods. It also takes a look at some post-quantum cryptography techniques that have been extensively studied and would be tough for even a quantum opponent to crack. The most promising contenders for the NIST standard are summarized in this survey's final section [6]. It concludes with recommendations for post-quantum cryptography research priorities and an examination of PQC algorithm performance across various platforms. The below figure 1 shows the growth of Quantum cryptography in the recent times

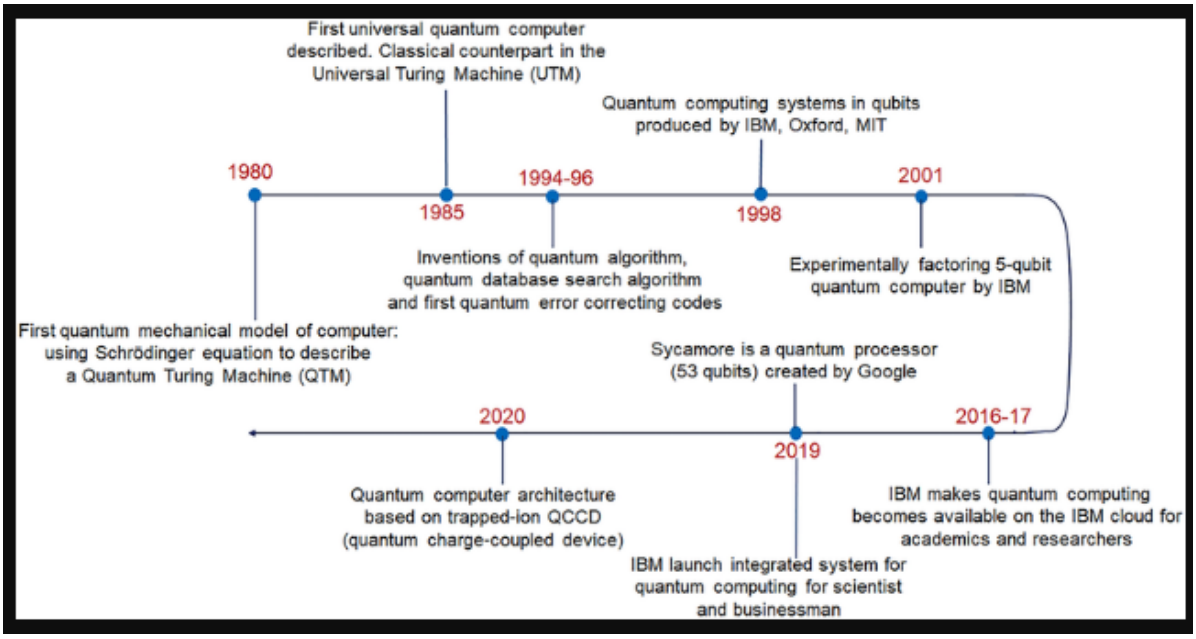

Fig. 1. Quantum computing growth from 1980 to 2020[7]

The Remaining Paper is structured as follows: Section 2 examines the literature from trustworthy publications on Post Quantum Cryptography covering the years 2009 to 2023.Section 3 addresses the motivations underlying the development of our hybrid cryptographic system, while The suggested approach is detailed in Section 4. Section 5 addresses the experimentation and results, while Section 6 concludes the research.

2. Related Works:

The goal of "post quantum cryptography"—a subfield of cryptography—is to develop encryption algorithms that are immune to quantum computing attacks. The protection of asymmetric algorithms is being built upon new number theory difficulties discovered by mathematicians and

cryptographers. Finding new mathematical problems that quantum computers will have a hard time solving are the next stage.

After quantum computing, symmetric algorithms & hash functions remain relatively safe. In terms of square root complexity, Grover's Algorithm can expedite the assaults [3]. Doubling the key size, however, restores the security of most algorithms. At now, the majority of post-quantum algorithms belong to one of six distinct families. Even with the help of quantum computers, many varied mathematical problems remain intractable. New asymmetric algorithms will be based on these mathematical challenges. For Post Quantum Cryptography, NIST started the standardization process in 2016. Novel approaches to digital signatures, key encapsulation, and public key encryption are being searched after.

Google has built a 53-qubit quantum computer using the most recent developments in quantum computing. Nevertheless, this is now close enough to decipher public-key cryptography, shifting the focus from "if" to "when" encryption will be vulnerable. Google and IBM are both in a mad dash to build noise-resistant, high-qubit quantum computers. As a result, numerous novel algorithms have emerged, either by avoiding problems with prime factorization or by making use of parallel computing. These algorithms rely on lattices & error-correcting codes as their foundation. The vast majority of algorithms exploit challenging lattice problems due to their durability in average & worst-case scenarios. National Institute of Standards and Technology (NIST) published a worldwide call for submissions for issues that could replace the existing digital signature systems, key encapsulation mechanisms, and public key encryption schemes in response to the growing need for Post-Quantum Security.

Researchers are exploring several post-quantum cryptographic methods, including isogeny-based, code-based, and lattice-based encryption, to develop cryptographic algorithms that could potentially resist quantum attacks.. To make sure these algorithms are secure, efficient, and widely used even when faced with quantum dangers, additional research is required. A free-space distribution of quantum keys (QKD) system based on the BB84 protocol has been suggested by Majid Safari & Murat Uysal [8] as an approach that uses terrestrial relays. The operation of passive relays has been considered in order to transmit qubits to the receiver or the next relay node without conducting a measurement or discovery process. Using a near-field analysis, they have determined a maximum allowable quantum bit error rate (QBER) for the QKD system that is helped by relays.Two three-party quantum key sharing protocols (QKDPs) have been analyzed for security by Fei Gao et al. [9].

The dense-coding attack could exploit these protocols. It was found that Eve, the eavesdropper, got the session key by sending Alice a bogus signal consisting of entangled qubits and then following Alice's encoding with combined measurements. A dense-coding conversation between Alice and Eve was remarkably comparable to the assault procedure. The use of the collective eavesdropping check in a four-party quantum key distribution mechanism has been addressed by Gan Gao[10] in his cryptanalysis. While the other agents are only required to perform a single qubit procedure, Alice, one of the employers in a four-party QSS protocol, desires to conduct a Bell state measurement. For the purpose of preventing eavesdropping, this protocol makes use of an online eavesdropping-check for classical channels. The dishonest actors in the QSS protocol make it

feasible to eavesdrop on Alice's private conversations.

A system that combines the three protocols for distribution of quantum keys—the implicit (3AQKDP) and the explicit (3AQKDPMA)—was suggested by Ananda Rao et al. [11].

They will be safe from replay, eavesdropping man-in-the-middle, and other attacks if they establish a secure connection. The number of times information has to be relayed has been reduced thanks to their approach. In addition, a long-term secret key has been frequently utilized and shared by two parties. Passive attacks, such as eavesdropping, can be detected using a mix of conventional and quantum cryptography methods.

Using four non-orthogonal two-particle entangled states, Zhu Zhen-Chao et al. [12] presented a mechanism for multi-party quantum secret sharing. The new protocol improves the theoretical efficiency of qubits from 50% to nearly 100%. Except for the entangled states necessary to verify the eavesdropper, all of the other entanglement states can be utilized to generate the private key. We compare the quantum distribution of keys against the so-called opaque cheat attack, a quantum assault on this type of protocol. Genetic algorithms and quantum genetic algorithms were compared by Zakaria Laboudi and Salim Chikhi [13]. The two algorithms were subjected to 500 generations of iteration and ran 25 times each. O(N), where N is the population size, is the global complexity order for QGA. The complexity for a GA is around O(N 2).A linear reduction of complexity has therefore occurred.
To maximize optimization level and computation speed, Rashad et al.[14] presented two optimization algorithms: genetic algorithm, a meta-heuristic approach, and cuckoo optimization, a heuristic method. It is still possible to make modifications and enhancements to the suggested approach and technique in order to make it faster. Assuming an optimization problem exists, the suggested method can be used in a wide variety of industrial and agricultural contexts.

Rawya Rizk et al. [15] devised a two-phase hybrid encryption technique to guarantee the safety of communication in WSNs. Minimizing key maintenance while providing good security is the goal of the suggested approach. It bridged the gap between symmetric and asymmetric cryptography. Data encryption makes use of Elliptical Curve Cryptography (ECC) and the Advanced Encryption Standard (AES). Network authentication and verification is carried out using the XOR-DUAL RSA technique. To ensure the networks' security, Message Digest-5 (MD5) is used. By reducing energy consumption and achieving the shortest cipher text size, this suggested technique improves performance in terms of calculation time in WSN.

To ensure the safe transfer of sensitive health information to the cloud, Qi Jiang et al.[16] proposed three-factor authentication. To provide a high-level authentication mechanism for accessing sensitive health data stored in the cloud, the suggested solution included biometrics, smart cards, and passwords. The cloud's three-factor security is met by this plan. This scheme's strength lies in its ability to thwart offline password guessing attempts and impersonation attacks during registration. There is no mention of how to evaluate the performance of different three-factor authentication schemes in the planned work. A survey of lightweight cryptographic approaches in WSN was conducted by Hala Tawalbeh et al. [17]. Sensors are utilized in several fields such as transportation, healthcare, manufacturing, and farming. The sensors work in tandem with the protocol for wireless communication. Applications require secure data transport to

prevent attacks. Because of these sensors, a limited setting necessitates techniques for light encryption. Modern techniques for public and private key cryptography need extensive computations. The authors contrasted the lightweight encryption methods with industry standards such as elliptic curve cryptography (ECC), RSA, and advanced encryption standard (AES).

In order to keep a watch on the distant healthcare system, Muhammad Usman et al.[18] suggested a novel four-tier design for WBANs. They defined the security requirements and obstacles for each tier of the WBAN. Tiers 1, 2, 3, and 4 make up the WBSN in this study. Tier 1 communications take place inside a living being. All it takes for a tier 2 communication to take place is for one of the people involved to be physically present within a human body. In tier 3, a non-human body contains at least one communication device. Tier 4 encompasses all forms of communication that do not include the human body.

To protect the confidentiality of patients' medical records, Ashish Joshi et al. [19] suggested a system that makes use of the Body Area Network (BAN). Data privacy and security are ensured by the proposed scheme's use of an alternative authentication mechanism to safeguard inter-sensor communication in BANs. All of the models involved in a network's defense and attack are defined by the anticipated method. In this segment, we choose the countermeasures, offer the protocol and formal security verification, and assess the performance. An novel approach to ensuring privacy and security is the plan that has been proposed above. When compared to alternative algorithms, nevertheless, the suggested approach falls short in terms of efficiency.

For WBANs, Sangwon Shin et al.[20] presented PSRSA, an acronym for preprocessed symmetric RSA. Reduced processing, reduced key sizes, and excellent security are requirements for WBAN security. The WBAN requirements are met by the suggested approach.To make the system more secure, RSA with a lower key is used for multi-layer preprocessing. The suggested method has the benefit of a lower key value while maintaining good WBAN security. The computational complexity is a drawback of this method. In their discussion of quantum key distribution (QKD) and its security against assaults, Al-Batool Al-Ghamdi et al.[21] drew on probabilistic model security analyses. The writers detailed how a series of quantum photons encrypts random numbers. By comparing the QKD method to the traditional one, the suggested system demonstrated the superior security of the latter. The potential distance for data transmission from the source to the recipient can be determined using this method. The scheme's main drawback is that it can only communicate the private quantum key to certain distances.

A novel approach to evading security holes in WSNs was put out by Shadi Nashwan [22]. Wireless sensor networks operating in large data settings can benefit from the suggested scheme's anonymous access authentication technique. Offering a suite of security services tailored to the needs of big data environments, this scheme excels at efficiently performing the perfect forward confidentiality feature. Additional security threats to this approach were not considered by the author.

A novel RSA technique for attack-proof data transfer was introduced by Ghassan Kbar et al. [23]. Cryptographic processes are easily crackable if attackers obtain the RSA private key. For both encryption and decryption, the writers relied on three prime numbers. No hacker can deduce the user's or server's secret or public key. The time needed to crack this cryptosystem is increased by

this scheme. The system will remain uncrackable even if the attackers manage to hack the keys. One drawback of this system is how slowly key generation, encryption, and decryption processes are executed.

Kyber uses lattices to accomplish selected ciphertext (IND-CCA) resistant in the MLWE issue; it is a key encapsulation scheme. Kyber uses a PKE method to achieve CPA security in a traditional LWE framework, with algebraic items having the ability of two cyclotomic rings. During the nomination and editing phase, Kyber achieved a CCA secrecy level, making him a potential candidate for a key exchange. Kyber use the SHAKE256 algorithm for key generation. Until now, NIST had selected Kyber to carry out the PKE/KEM standardization. In order to evaluate the performance of the CRYSTALS-Kyber methods with three distinct parameter sets—Kyber-512, Kyber-768, and Kyber-1024—corresponding to one, three, and five security levels, one study [24] utilized a TSMC 40nm LP CMOS process device. Power usage, number of clock cycles, & overall performance are measured for the three steps of the protocol: key creation, encryption, and decryption. This study's findings are contrasted with those of earlier investigations on Cortex-M4. Depending on the protocol step, the results reveal a reduction in energy consumption of 10–20 times and a reduction in the on-chip execution cycle of 3–16 times compared to prior research. In two different studies [25], the authors looked at and evaluated the characteristics of Kyber on RISC-V. Three sets of parameters were evaluated for the keypair, encrypt, and decrypt processes, with levels of security 1, 3, and 5. An article [26] laid out the blueprints for the post-quantum ALU (PQ ALU) set, which would use the expanded instruction set to do out mathematical operations. The next step was to investigate the feasibility of a simple system on a chip (SoC) implementation on a Xilinx ZCU106 board and evaluate its performance, power consumption, and resource utilization. The results show that the PQ ALU structure, when combined with a larger instruction set, is most efficient in terms of both speed and energy use. A matrix-extension-based domain-specific processor was suggested in reference [27]. The following step was to apply this structure to TSMC 28 nm technology. Compared to the Cortex-M4, Sapphire, or VPQ implementations, the assessment findings reveal a cycle count efficiency that is up to 3.5 times higher. Along with supporting Kyber, Dilithium, and future algorithms, one study [28] suggested a PQC coprocessor that had a RISC-V ISA extension. An interface module within the PQC coprocessor connects a RISC-V core to it in this study. The findings demonstrate that the architect boosts the performance of cryptographic primitives and backs NIST's third-round PQC candidate algorithms.

3. Motivation of the Work:

There is a growing demand for cryptographic methods that are both reliable and privacy preserving due to our dependence on digital technologies. The advent of quantum cryptography offers hope for overcoming these challenges, especially in the context of communication systems. To ensure safe transactions that cannot be compromised by quantum computers, quantum computing employs quantum cryptography techniques. Security and privacy concerns must be thoroughly examined before implementing these protocols, which presents a number of challenges. Creating trustworthy protocols for quantum key distribution (QKD) is a major obstacle to the widespread use of quantum crypto currency. When it comes to cryptographic applications, QKD protocols offer a safe way for two parties to generate shared secret keys. The BB84, E91, and B92 procedures are among the

several that have been suggested for QKD. Since current protocols can be easily attacked by quantum computers, new, more secure ones must be created. A further barrier to quantum crypto currency is the development of novel post-quantum cryptography algorithms.

4. Methodology:

In order to guarantee the authenticity of the communication, this section discusses hybrid cryptography that uses augmented lattice-based cryptography and Message Authentication Codes (MACs). There are several steps involved in the proposed method, including authentication, registration, and the production of keys for MELMAC (Modified and Enhanced Lattice Based Cryptography with Message Authentication code). This suggested approach has potential for use in WBANs, or wireless body area networks. There are numerous obstacles to overcome, particularly in the realm of security. The WBAN's patient data is of interest to many hackers. Keeping sensitive patient information safe from hackers is a big issue with this system. It is critical that all WBAN communication participants verify their identities.

Message Authentication Code (MAC)

One kind of authentication that uses symmetric keys is the Message Authentication Code (MAC). Its primary function is to authenticate messages. In order to initiate the MAC procedure, the communicating parties exchange a secret key.Figure 2 shows the whole process in MAC.

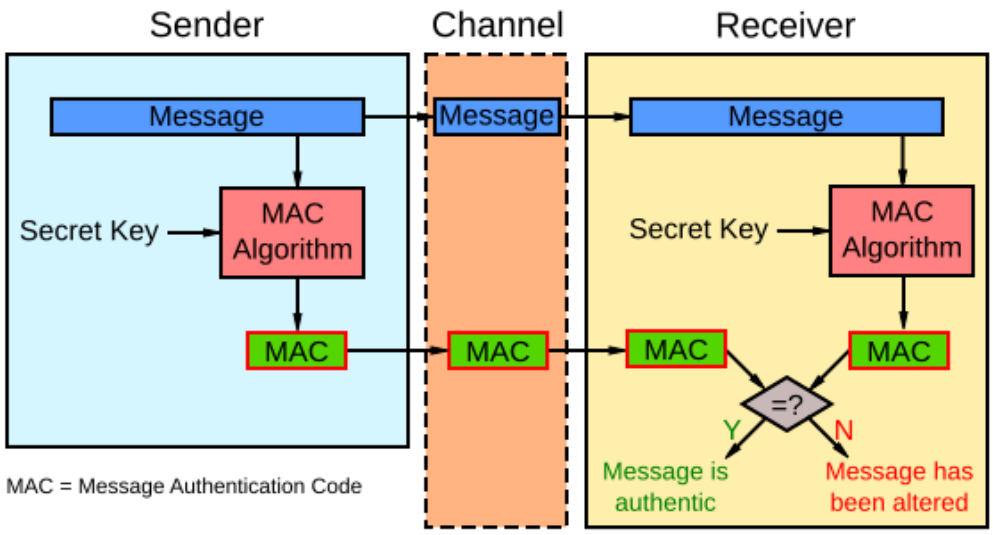

Figure 2.Secure MAC Procedure[29]

The following steps describes the entire MAC process

Step 1: Message, secret key K, and MAC algorithm are the inputs that the sender takes. One possible output is a MAC value.

Step 2: The MAC function takes an input and returns an output of a predetermined length. When compressing this file, MAC makes use of a secret key.

Step 3: The sender includes the MAC addresses in the message and forwards it as a sequential step. Here, MAC only ensures the authenticity of the message's origin and does not guarantee its secrecy. An encryption operation is performed on a communication in order to ensure its confidentiality.

Step 4: After the receiver receives a message with a MAC, it uses the secret key K with the MAC algorithm to recalculate a MACr value.

Step 5: After receiving a MAC address, the receiver verifies that it is identical to the one it calculated (MACr). The recipient can tell that the message came from the intended sender if the MAC value doesn't match.

Step 6: If the received MACr value differs from the sender's MACs value, it might be inferred that the message has been modified at the receiver end. This is where the sender authentication is still being fine-tuned.

Lattice Based Cryptography

Vector, Basis, and Lattices are the three components that make up lattice-based cryptography.

Using a Lattice To encrypt a message, cryptography employs geometric structures. In the lattices, keys can be based on either a good or terrible basis. Given the bases, it is possible to locate the lattice's real nearest point. A decent basis describes that foundation. The locations of the points in the lattices are not nearest to the bases. The choice is still challenging, and it uses a round function to choose the integer closest to the lattice. Such foundations are inadequate. A public key is a bad base, while a private key is a good one. According to the literature, we can encrypt and decode texts using lattice-based methods. The lattices and vectors dispersed across them are shown in the diagrams below.

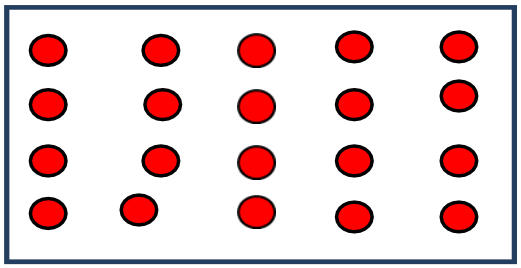

Figure 3.Lattices in the Plane

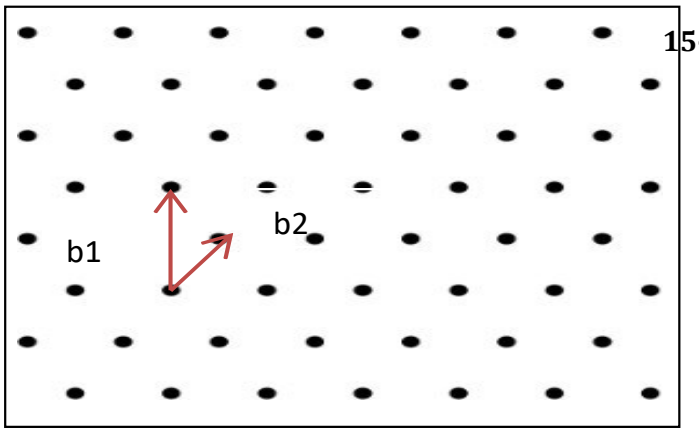

Figure 4. Vectors in the lattices

The Proposed Hybrid Method is shown in Figure 5 Below.

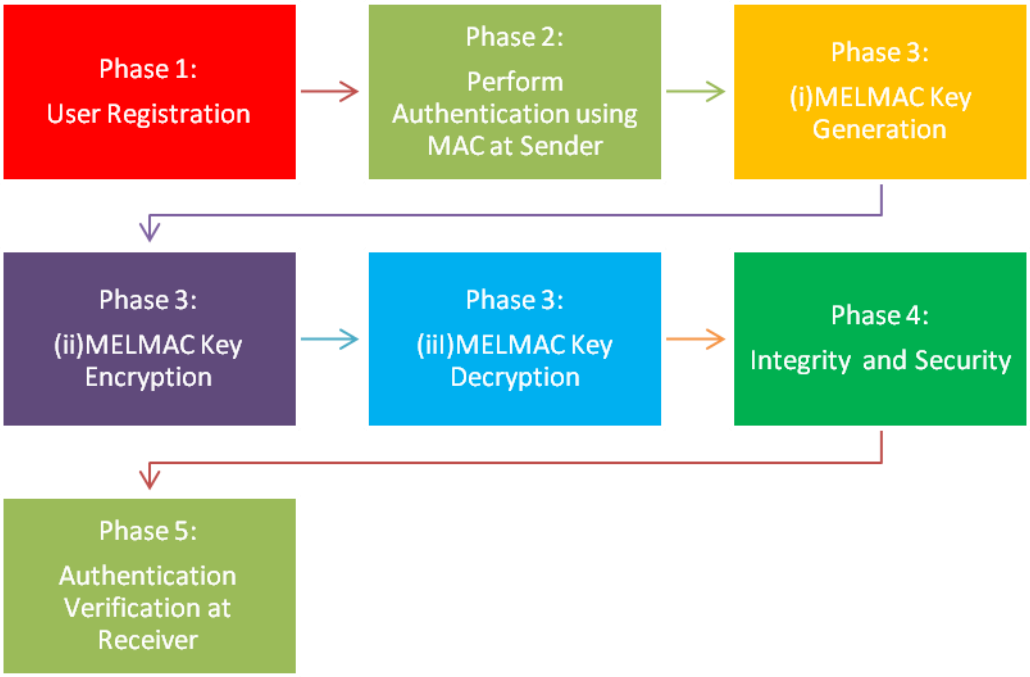

Figure 5.Proposed Hybrid Algorithm Working Procedure

Registration:

Patients who wish to participate in the clinic's remote monitoring and treatment services must first register with the network during the first registration phase. A separate Patient Enrollment Number (PEN) will be assigned to them by the remote healthcare system. Depending on the type of illness, the patient's body may have a number of sensors. The provided body sensor identity (BSI) assigns this particular body sensor a distinct identifier. Thus, a distinct BSI and PEN are required for every sensor and patient.

Authentication:

Phase 2 Authentication involves verifying the patient's and sensor's identities through the transfer of data from the physiological body sensor. Use the MAC algorithm and key K to generate a Message Authentication Code (MAC) value after validating the patient's identify (PEN) & body sensor identification (BSI). In addition, the third phase of the decryption and encryption procedure deals with this Procedure.

The following algorithm illustrates the entire registration and authentication process..

Input: PEN, BSI, MAC Algorithm, and Key K.

Output: WBSN participant's authentication is verified with the help of MAC value and MALMBC.

1. Patients' enrollment numbers (PENs) and body sensor identifiers (BSIs) are registered.

2. The formula to compute the MAC value on the side of the transmitter (the Body Sensor) is:

$$MAC\ value = MAC\ algorithm||K$$

The MAC value should be calculated at the initial stage on the receiver side, which is the hospital server. Both the transmitter and the receiver employ the identical Media Access Control (MAC) protocol and secret key values.

3. From the sender's end, frame the packet "P" by adding the MAC value to the patient's enrollment number and body sensor ID (PEN+BSI).

4. Send P to receiver.

$P = (PEN + BSI\ ||MAC\ value)$

5. The packet "P" was received by the recipient.

6. The receiver has calculated a MAC address; compare it to the one in packet P. Verification of authentication and integrity of medical data is achieved when the Media Access Control (MAC) value in packet P matches the MAC value computed by the receiver . else the packet will be ignored.

MELMAC Key Generation:

Transferring sensitive patient health data is done using Lattice-Based Cryptography (LBC). Intruders have a chance to eavesdrop on the broadcast and steal the data of the patient. Here, robust key generation is performed. The lattice's sample and error vectors constitute the public key, while the secret quantum key is the private key. The data that is sensed is encrypted and decrypted using the public key and private quantum key. In this case, the secret quantum key, sample vector, and error vector are all unknown to the attackers. The system's security is top-notch. The steps for generating a MELMAC key are

Input: Lattice based security parameters

Output: Public key(PU),Private key**(**PR)

Step 1: En, De, M, Sv, Rv, and F are the input parameters in the list. As a security parameter, the symbol m As a security parameter, 'm' is passed to the setup phase of lattice-based cryptography, which then returns the public parameter. The function takes as inputs a prime modulus, a dimension of the identity space, and column and row-wise dimensions; in return, it returns the public key. A prime modulus (r), the column-wise dimension (q), the self space element (s), encoding function (En) to map public id's, the bit-wise disintegration of IDs (De), and a regular arbitrary matrix (M) complete the set M $\in Z_p^{a\times b}$, S_v is the secret vector $S_v \in Z_p^a$, R_v is the random vector $R_v \in Z_p^a$, F is the function $F : Z^a \rightarrow Z^b$. Public key is produced dep[ending on sample vector(s_v) and error vector (e_v) in the lattices as follows. Hence

Public Key= $PK = s_y + e_y$ ----------(4.1)

Step 2: Private key (PR) is secret quantum key

PR = QK(secret quantum key)---------- (4.2)

MELMAC Encryption:

Various Steps in Encryption is as follows:

Input: *plaintext partition p1,p2, Public key PU , secret quantum key Qk*

Output: *Cipher texts : Cipher text 1 (Cip1),Cipher text 2(C_2)*

1.Senders Public Key PK

2.Partition the Plan Text as follows: $p1 = 0 - l/2$

3. Encryption1: E1 = p1. PU + er

There is a twofold encryption method in MELMAC encryption. First, we encrypt the plaintext partition 'p1' using the public key 'PU' and the error vector 'er'. The result is the ciphertext 'c1'.

4. Double Encryption: $Cip1 = DoubleEnc\ (\ Qk(c1)\ )$

For a double encryption procedure, Step 4 accepts "c1" as input and outputs ciphertext using the secret quantum key Qk. *„Cip1'*

5. Plaintext partition p_2 : $p2 = l/2 - 1$

6. Encryption2: $c2 = p2.\ PU + er$

7. Cipher Text Cip1, $c2$

MELMAC Decryption:

Various Steps in Decryption is as follows:

Input: Cipher text (C), Quantum key (QK), public key (PU)

Output: Plain text

Step1: Decryption process cipher text c2

$p2 = decrpt(QK(c2.PU + er))$

$p2 = decrpt(QK(c2.PU + er)PU^{-1})$

Step 2: Where U is a uni modular matrix

$p2 = p2.PU.PU^{-1} + er.PU^{-1}$

Step 3: Here, this rounding method used to eliminate the term $e_r.PU'^{-1}$

$p2 = p2 + er.PU^{-1}$

Step 4: work out the plaintext split p_2

Step 5: Deciphering encrypted data *Cip1*

$p1 = decrpt(cip1)$

Step6: How to decrypt cipher text is c_1

$p1 = decrpt(QK(c1.PU + er))$

Step 7: To decrypt, repeat steps 2 and 3 on p1.

Step 8: calculate the plaintext partition p_1

Step 9: Finally, put the two Plain text parts together to get the original text.

Once the Key generation, encryption, and decryption steps are finished, the security and protection of the patient data is maintained . We can see that the authentication and verification work well on the receiver side, showing that MAC and lattice-based cryptography are being used correctly.

5. Experimentation and Results:

In the experiments, the key size is chosen to be 128,256, and 512 bits. In order to assess and contrast the proposed system's performance evaluation, crystals-Kyber and crystals-Dilithium are utilized. In order to evaluate the suggested Hybrid MELMAC, we have taken three factors into account. Time to generate keys, time to encrypt, and time to decrypt is the three parameters that have been evaluated.

. These are defined as follows:

- The Time required to produce a pair of keys by means of a genetic algorithm is known as key generation time in the field of cryptography.
- The Time it takes for an encryption algorithm to encrypt data is known as the encryption time in cryptography.
- When data is encrypted, the time it takes to decode it using a decryption method and key is called decryption time.

The kind of encryption and decryption algorithm determines all of these things.

5.1 Key Generation Time:

Key generation times for Crystals-Kyber, Crystals-Dilithium, and the proposed MELMAC system are compared in Table 5.1 below. We provide keys with sizes of 128 bits, 256 bits, and 512 bits. The time it takes to generate a key is measured in milliseconds.

Table 5.1 Key Generation Time

Algorithms	**Key Generation Time(ms)**		
	128 bits	**256 bits**	**512 bits**
Crystals-Kyber	409	452	517
Crystals-Dilithium	331	361	408
MELMAC	217	247	283

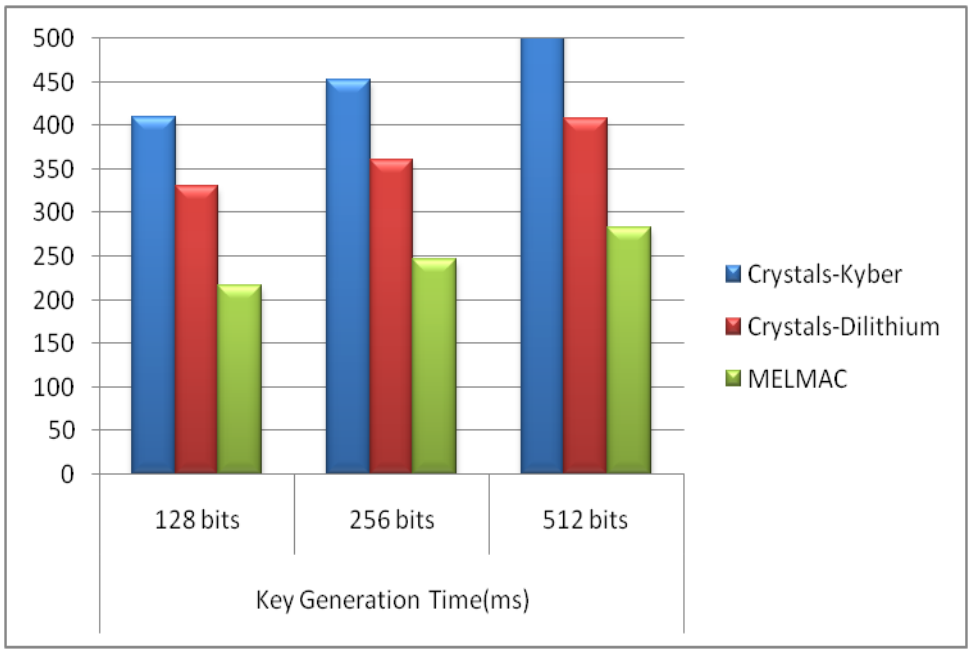

Figure 6. Results of Key Generation Time

Key size, in bits, is shown on the X-axis of the above figure. The key generation time, shown in milliseconds, is on the y-axis. The proposed system of MELMAC, crystals-Dilithium, and crystals-Kyber all have significant generation times displayed in Figure 6. Based on the results, the proposed strategy generates keys faster than existing algorithms. The suggested approach generates keys using quantum physics and a mathematical foundation based on lattices. The process of key generation takes less time.

5.2 Encryption Time:

The comparison of encryption times between crystals-Kyber, crystals-Dilithium, and MELMAC is shown in Figure 7 and Table 5.2. The X-axis here represents the key size, which is given in bits. The encryption time is shown on the y-axis in milliseconds.

Table 5.2 Encryption Time

Algorithms	**Encryption Time(ms)**		
	128 bits	**256 bits**	**512 bits**
Crystals-Kyber	398	412	474
Crystals-Dilithium	221	272	304
MELMAC	147	186	207

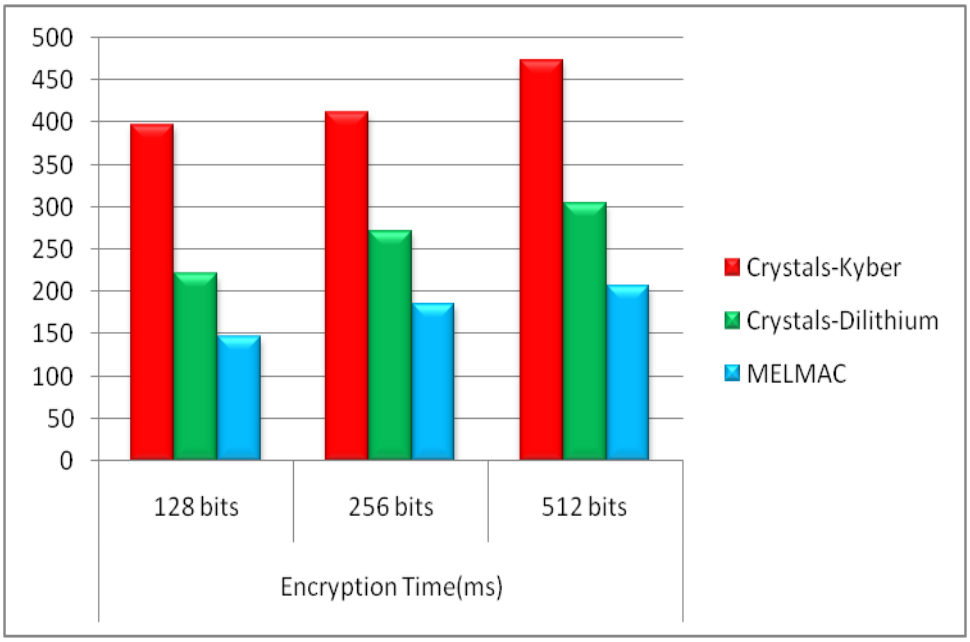

Figure 7. Results of Encryption Time

Three trials are carried out using keys ranging in size from 128 bits to 512 bits. The proposed hybrid approach has a faster encryption time compared to current techniques. The methods for plaintext partitioning are part of the suggested approach. Here, there are two sections of plaintext. Using key1 and quantum keys in a double-encryption fashion, the first section is secured. The value of key1 is used for encryption just once with the second portion of the plaintext. The process of encryption is split into two phases, which allows it to be executed more quickly. Encryption time is a function of both the availability of plaintext partition keys and the input used in the encryption process. The time component is crucial to the remote health tracking and treatment system. It takes less time to process this scheme. Evidence suggests the suggested method is an excellent match for secure WBAN transmission.

5.3 Decryption Time

Decryption time is measured in milliseconds, whereas key size is measured in bits. Secret key generation using Kyber is slower than with the suggested method. Table 5.3 and Figure 8 compare the current methods with the proposed ones.

Table 5.3 Decryption Time

Algorithms	Decryption Time(ms)		
	128 bits	**256 bits**	**512 bits**
Crystals-Kyber	487	526	605
Crystals-Dilithium	331	402	487
MELMAC	231	314	394

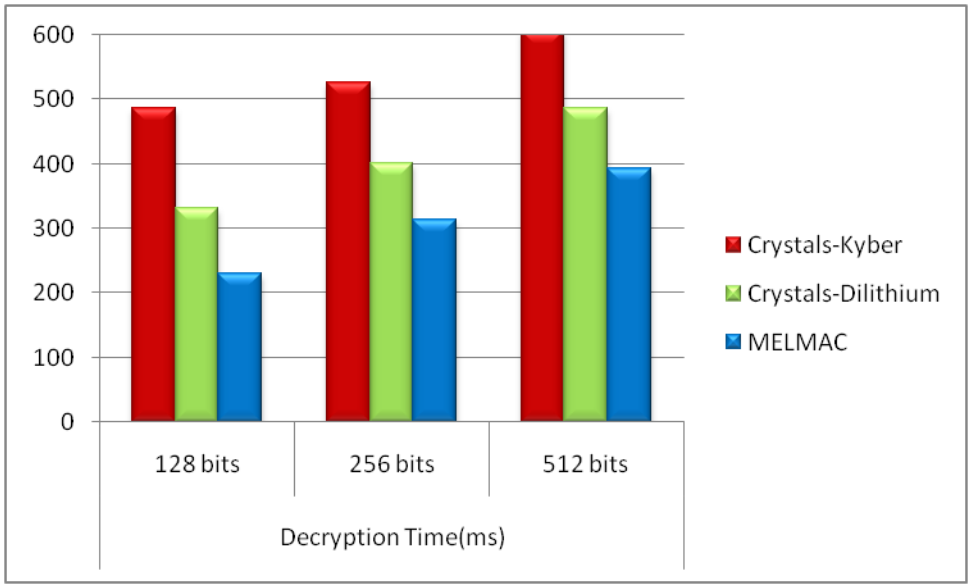

Figure 8. Results of Decryption Time

The mathematical functions form the basis of the key generation process in Kyber and Dilithium. Since these techniques are widely used, attackers can quickly crack the key creation procedures. The time required to generate keys by these algorithms will increase if they incorporate mathematical functions and user assumptions. The suggested strategy outperforms the state-of-the-art approaches in terms of decryption times.

6. Conclusion:

All of the main public key cryptosystems can be cracked using quantum techniques. It will be inevitable that they are entirely demolished. Thankfully, new cryptosystems can be built using newly-formulated hard problems. The development of efficient solutions, secure post-quantum cryptography methods, and resilient QKD protocols is crucial for the practical and safe implementation of quantum cryptography. Wireless body sensor networks rely on the MAC algorithm and Modified & Enhanced Lattice-based cryptography for authentication purposes. To make sure the transmission is secure, five procedures are followed. The patient must first register their identify with the body sensors. Secondly, the patient's registration information and data from their body sensors are encrypted before being sent to the receiver. Third, part1 and part2 are the two sections of the plaintext. Part 2's plaintext and Part 1's are both encrypted using modified and augmented lattice-based keys, and the fourth step is to use a quantum key for double encryption. Fifth, after decrypting parts 1 and 2, the text is concatenated in plain text. New algorithms for key generation, encryption, and decryption were developed in this proposed study using improved and updated lattice-based cryptography. To ensure the authenticity and

integrity of the messages, MELMAC combines two robust mechanisms. We employ quantum keys, also known as MELMAC-keys. The attackers cannot predict these keys. No outside parties are privy to the MELMAC encryption and decryption procedure. The authentication provided by this system is robust. When compared to other algorithms, MELMAC's time for key creation, encryption, and decryption is significantly lower.

References:

[1] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty- eighth annual ACM symposium on Theory of comput- ing*, pp. 212–219, 1996.

[2] Tasso, E´., De Feo, L., El Mrabet, N., & Pontie´, S. (2021, October). Resistance of isogeny-based cryptographic implementations to a fault attack. In International Workshop on Constructive Side-Channel Analy- sis and Secure Design (pp. 255-276). Springer, Cham

[3] M. K. a. G. L. a. A. L. a. M. Naya-Plasencia, Breaking Symmetric Cryptosystems using Quantum Period Finding, arXiv, 2016.

[4] Mehic, M.; Niemiec, M.; Rass, S.; Ma, J.; Peev, M.; Aguado, A.; Martin, V.; Schauer, S.; Poppe, A.; Pacher, C.; et al. "Quantum Key Distribution: A Networking Perspective". ACM Comput. Surv. 2020, 53, 1–41.

[5] Bertels, K.; Sarkar, A.; Hubregtsen, T.; Serrao, M.; Mouedenne, A.A.; Yadav, A.; Krol, A.; Ashraf, I.; Almudever, C.G. "Quantum Computer Architecture Toward Full-Stack Quantum Accelerators". IEEE Trans. Quantum Eng. 2020, 1, 1–17.

[6] D. J. Bernstein, "Introduction to Post-Quantum Cryptography," Springer, p. pp. 1–14, 2009.

[7] Pal, Soumen & Bhattacharya, Manojit & Lee, Sang-Soo & Chakraborty, Chiranjib. (2023). Quantum Computing in the Next-Generation Computational Biology Landscape: From Protein Folding to Molecular Dynamics. Molecular Biotechnology. 66. 1-16. 10.1007/s12033-023-00765-4.

[8] Majid Safari & Murat Uysal 2009, 'Relay-Assisted Quantum-Key Distribution Over Long Atmospheric Channels', Journal of Light Wave Technology, vol. 27, no. 20, pp. 4508-4515.

[9] Fei Gao, Su-Juan Qin, Fen-ZhuoGuo & Qiao-Yan Wen 2010, 'Dense-Coding Attack on Three-Party Quantum Key Distribution Protocols',IEEE Journal of Quantum Electronics, vol. X, no. X, pp. 1-6.

[10] Gan Gao 2010, 'Cryptanalysis of multiparty quantum secret sharing with collective eavesdropping-check', Journal Optics Communications,vol. 283, no.14, pp. 2997–3000.

[11] Ananda Rao, G, Srinivas, Y, VijayaSekhar, J & Pavan Kumar, CH 2011, 'Three Party Authentication Key Distributed Protocols Using Implicit and Explicit Quantum Cryptography', Indian Journal of Computer Science and Engineering, vol. 2, no. 2, pp. 143-145.

[12] Zhu Zhen-Chao, Zhang Yu-Qing & Fu An-Min 2011, 'Efficient quantum secret sharing scheme with two-particle entangled states',Chin. Phys. B, vol. 20, no. 4 .

[13] Zakaria Laboudi & Salim Chikhi 2012, 'Comparison of Genetic Algorithm and Quantum Genetic Algorithm', The International Arab Journal of Information Technology, vol. 9, no. 3.

[14] Rashad, MZ, Keshk, AE, El-Dosuky, MA & Kamal, MM 2014,'Genetic Cuckoo Optimization Algorithm (GCOA)',International Journal of Computer Applications, vol.90, no.3, pp.7-12.

[15] Rawya, Rizk, Yasmin & Alkady 2015, 'Two-phase hybrid cryptography algorithm for wireless sensor networks', Journal of Electrical Systems and Information Technology, vol. 2, no. 3, pp. 296-313.

[16] Jiang, Q, Khan, MK, Lu, X, Ma, J & He, D 2016, 'A privacy preserving three-factor authentication protocol for E-Health clouds', The Journal of Supercomputing, vol. 72, no. 10, pp. 3826-3849.

[17] Hala, Tawalbeh, Sonia, Hashish, Loai, Tawalbeh, Anwar & Aldairi 2017, 'Security in wireless sensor networks using lightweight cryptography', Journal of Information Assurance and Security, vol.12, no.2017, pp.118-123.

[18] Muhammad, Usman, Muhammad Rizwan, Asghar, Imran Shafique, Ansar Marwa & Qaraqe 2018, 'Security in wireless body area networks: From in-body to off body communications', IEEE Access, vol. 6, pp. 58064-58074.

[19] Ashish, Joshi, Amar, Kumar & Moha patra 2019, 'Authentication protocols for wireless body area networkwith key management approach', Journal of Discrete Mathematical Sciences& Cryptography,vol.22,no.2,pp.219-240.

[20] Sangwon, Shin, Kwanghee, Won & Sung Shin 2020, 'Size efficient preprocessed symmetric RSA for wireless body area network', Applied Computing Review, vol. 20, no. 1, pp. 1-15.

[21] Al-Batool, Al-Ghamdi, Ameenah, Al-Sulami, Asia Othman & Aljahdali 2020, 'On the security and confidentiality of quantum key distribution', Security and Privacy, vol. 3, no. 5, pp. 1-4.

[22] Nashwan, S 2021, 'AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment', Egyptian Informatics Journal, vol. 22, no. 7, pp. 15-26.

[23] Ghassan, Kbar, Wathiq & Mansoor 2021, 'Modified RSA using triple keys based encryption/decryption', Jordan Journal of Electrical Engineering,vol. 7, no. 1, pp. 1-14.

[24] Banerjee, U.; Ukyab, T.S.; Chandrakasan, A.P. "Sapphire: A Configurable Crypto-processor for Post-quantum Lattice-based Protocols". IACR Trans. Crypto. Hardw. Embed. Syst. 2022, 2022, 17–61.

[25] Nannipieri, P.; Matteo, S.D.; Zulberti, L.; Albicocchi, F.; Saponara, S.; Fanucci, L. A "RISC-V Post Quantum Cryptography Instruction Set Extension for Number Theoretic Transform to Speed-Up CRYSTALS Algorithms". IEEE Access 2023, 9, 150798–150808.

[26] Zhao, Y.; Xie, R.; Xin, G.; Han, J. A High-performance Domain-specific Processor with Matrix Extension of RISC-V for Module- LWE Applications. IEEE Trans. Circ. Syst. I Regul. Pap. (TCAS-I) 2023, 69, 2871–2884.

[27] Lee, J.; Kim, W.; Kim, S.; Kim, J.-H. Post-quantum Cryptography Coprocessor for RISC-V CPU Core. In Proceedings of the 2022 International Conference on Electronics, Information, and Communication (ICEIC), Jeju, Republic of Korea, 6–9 February 2023; pp. 1–2

[28] Nosouhi, M.R.; Shah, S.W.; Pan, L.; Zolotavkin, Y.; Nanda, A.; Gauravaram, P.; Doss, R. Weak-key Analysis for BIKE Post-quantum Key Encapsulation Mechanism. IEEE Trans. Inf. Forensics Secur. 2023, 18, 2160–2174.

[29] https://commons.wikimedia.org/wiki/ Message_Authentication_Code