Panamerican Mathematical Journal
ISSN: 1064-9735
Vol 35 No. 1s (2025)

Advanced Techniques in Post-Quantum Cryptography for Ensuring Data Security in the Quantum Era

Dr. Latika Rahul Desai[1], Dr. P. Malathi[2], Rajashri Rajesh Bandgar[3], Dr. Hruhiskehsh Joshi[4], Abhilasha Sandeep Kore[5], Dr. Reshma Yogesh Totare[6]

[1]Associate Professor, Department of Information Technology, D. Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India. latikadesai@gmail.com

[2]Principal, D. Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India. principal@dypcoeakurdi.ac.in.

[3]Assistant professor, Department of AI & DS Engineering, D.Y. Patil School of Science & Technology Pune.

[4]Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Technology, Pune, Maharashtra, India. hrushsikeshj2@gmail.com

[5]Department of Information Technology, D. Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India. askore@dypcoeakurdi.ac.in.

[6]Department of Information Technology, AISSMS Institute of Information Technology, Pune, India. reshma.gaykar@gmail.com

Article History:

Received: *25-08-2024*

Revised: *28-09-2024*

Accepted: *15-10-2024*

Abstract:

The arrival of quantum computers is a major threat to current security methods, which depend on problems like discrete logarithms and integer factorization being hard. Post-quantum cryptography (PQC) is getting to be an critical field for making secure strategies that can't be broken by quantum assaults. This exposition talks almost progressed PQC strategies, centered on the most up to date thoughts and what they cruel for securing information within the quantum age. To begin with, we see at lattice-based cryptography, which appears like a great choice since it has solid security roots and can be utilized in numerous circumstances. This incorporates strategies such as Learning With Mistakes (LWE) and Ring-LWE, which are exceptionally great at ensuring against quantum dangers and are simple to utilize. Another critical zone is code-based cryptography, which employments the trouble of breaking irregular straight codes as an case. The McEliece cryptosystem is one such framework. It is checked to see how valuable and successful these strategies are in real-life circumstances. We see into multivariate polynomial encryption, which builds security on the truth that it's difficult to illuminate sets of multivariate quadratic equations. People are particularly curious about this strategy since it may be utilized to form proficient marking plans. Another imperative strategy is hash-based cryptography, which employments hash capacities to create secure advanced marks. The consider moreover talks around blended cryptography frameworks that utilize both conventional and post-quantum strategies. These frameworks make beyond any doubt that the switch to quantum computing goes easily and give way better security. We see at the issues that come up with implementation, like additional work that has to be done on the computer and joining it with current frameworks, and come up with ways to urge around these issues. At long last, moving to post-quantum security is necessary, but it comes with a part of problems that ought to be illuminated in numerous ways.

Keywords: Post-Quantum Cryptography (PQC), Quantum Computing, Data Security, Lattice-Based Cryptography, Learning With Errors (LWE), Ring-LWE, Code-Based Cryptography

I.INTRODUCTION

The coming of quantum computing will make cutting edge security frameworks confront a issue they have never seen some time recently. The security of advanced communications, managing an account exchanges, and information capacity is based on classical cryptography, which depends intensely on the computational trouble of issues like discrete logarithms and numbers factorization [1]. A part of well known encryption strategies, like RSA and ECC (Elliptic Bend Cryptography), are based on these issues. On the other hand, quantum computers might make these programs futile since they can do complicated calculations a million times quicker than normal computers. As an illustration, Shor's strategy can rapidly fathom discrete logarithms and numbers factorization, which isn't conceivable with RSA or ECC [2]. Since of this possible weakness, we ought to quickly create and utilize encryption strategies that can stand up to quantum assaults. This is often the region of post-quantum cryptography (PQC). The objective of post-quantum encryption is to form modern building pieces for cryptography that are secure from both classical and quantum aggressors.

Quantum cryptography employments quantum material science to keep discussions secure. PQC, on the other hand, makes math issues that are still difficult for quantum computers to reply [3]. In this region of think about, there are a parcel of distinctive and curiously strategies that appear guarantee. Each has its claim qualities and shortcomings. This sort of cryptography stands out since it offers awesome assurance and can be utilized in numerous distinctive ways [4]. Lattice-based plans, just like the Learning With Blunders (LWE) issue and its adaptation, Ring-LWE, depend on how difficult it is to discover brief vectors in cross sections with a part of measurements. Quantum assaults are not thought to be able to fathom these issues, which is why solid encryption and marking strategies have been made [5]. Lattice-based cryptography too has additional highlights like homomorphic encryption, which lets you work on secured information without decoding it. This makes information more private and secure. Code-based cryptography is another imperative strategy in PQC. It makes security stronger by making it difficult to interpret irregular linear codes. The McEliece cryptosystem may be a well-known illustration of a framework that offers great security and fast key creation [6]. Indeed in spite of the fact that the key sizes are huge, it is still a great choice for post-quantum secure encryption since it has been appeared to be safe to quantum strategies [7]. It is too curiously to note that multivariate polynomial cryptography works by utilizing the trouble of understanding frameworks of multivariate quadratic conditions. This strategy looks particularly great for advanced marks since it offers speedy and secure ways to alter current rules [8]. Hash-based cryptography is another solid alternative. It employments the highlights of hash functions to make computerized marks that are secure. Patterns just like the Merkle signature plot appear how this strategy works [9]. It is simple to utilize and offers solid security guarantees. Since hash capacities are thought to be secure from quantum attacks, hash-based cryptography could be a straightforward but viable way to create beyond any doubt that information is adjust and genuine [10].

Half breed security systems that blend classical and post-quantum strategies are too a portion of the move to PQC [11]. These blended strategies make the transition easier by letting current frameworks adopt quantum-resistant calculations in stages whereas still being able to work with more seasoned frameworks [12]. This arrange is exceptionally imperative for keeping things secure amid the time when both conventional and quantum dangers are show. Executing PQC is difficult for a number of reasons, such as the require for more computing control, greater keys, and the ought to fit it into current frameworks [13]. But these problems are being looked at in ongoing research and development with the goal of making PQC solutions that are useful and effective. As quantum computing gets better, using PQC is no longer just an academic practice; it's a must. In the age of quantum computing, strong data security needs a multiple method that uses both new cryptographic techniques and careful application strategies [14]. The arrival of quantum computing requires a

major change in the way cryptography works. We can protect our digital future from quantum risks with post-quantum security. We can make security structures that are strong by improving lattice-based, code-based, multivariate polynomial, and hash-based cryptography methods and combining them into mixed systems. These efforts are critical to protecting data security, safety, and validity in the face of quantum computing's transformative potential.

II.RELATED WORK

The quick progressions in quantum computing require a noteworthy advancement in cryptography strategies to guarantee information security. Quantum calculations, like Shor's calculation, can rapidly illuminate issues like numbers factorization and discrete logarithms [5]. These calculations posture a danger to classical cryptographic strategies, which are the establishment of present day computerized security. Calculations like RSA and ECC (Elliptic Bend Cryptography) are based on these issues. Post-quantum cryptography (PQC) may be a modern zone that centers on making cryptographic strategies that are secure against both classical and quantum assailants. It was made to bargain with this coming risk. This line talks approximately a few progressed PQC methods and highlights their reason, how they work, and important results. Lattice-based cryptography is one of the leading alternatives in PQC since it is exceptionally safe to quantum dangers and can be utilized in a part of distinctive ways [26]. Learning With Mistakes (LWE) and Ring-LWE are methods that offer solid security by utilizing the reality that it is difficult to discover brief vectors in high-dimensional cross sections. Since of these methods, quick key sharing conventions and homomorphic encryption have been made [15]. This sort of encryption lets forms be done on ensured information without unscrambling it, which makes it more secure and more private. The McEliece cryptosystem is an case of code-based cryptography that employments the truth that it is difficult to interpret arbitrary direct codes [16]. Indeed in spite of the fact that it's difficult to work with huge key numbers, the McEliece framework is still a great choice for secure encryption since it has been appeared to be safe to quantum assaults [17]. Its solid security system makes it an important choice for encryption strategies that will work within the future.

Another vital range is multivariate polynomial cryptography, which ponders how difficult it is to unravel frameworks of multivariate quadratic conditions [18]. This way looks particularly great for making computerized signature frameworks that work well and can replace existing benchmarks. Multivariate polynomial strategies can be used for private informing within the quantum age since they are quick and secure. A straightforward but viable way to ensure advanced marks is hash-based cryptography, which employments the highlights of hash capacities [19]. One well-known case is the Merkle signature strategy, which gives a safe and simple way to apply this that's not helpless to quantum assaults [20]. Hash capacities, which are as a rule thought to be secure from quantum computer threats, are exceptionally critical for making beyond any doubt that information is adjust and genuine. Utilizing crossover cryptographic frameworks, which blend conventional and post-quantum strategies, could be a useful way to urge to security that's not influenced by quantum computing. These frameworks make the switch simple by keeping past compatibility and including quantum-resistant strategies at the same time [21]. This arrange is exceptionally imperative for keeping things safe amid the time of alter when both conventional and quantum dangers are show [22]. Quantum-resistant calculations incorporate a parcel of diverse strategies, and all of them work together to form a total security reply. Researchers are making strong frameworks to keep information secure from quantum attackers by moving forward a number of PQC strategies, counting hash-based, code-based, multivariate polynomial, and lattice-based cryptography [23]. These endeavors are backed by exhaustive security investigate that appears they can withstand quantum dangers in hypothesis.

PQC is difficult to utilize in genuine life since it requires a parcel of extra work on computers and has to be coordinates with current frameworks. But think about is still going on to discover ways to illuminate these issues so that PQC strategies can work well and be utilized by numerous individuals [24]. For example, lattice-based and code-based methods are very helpful for key exchange protocols because they provide safe and quick ways to share cryptography keys that can't be hacked by quantum computers. In the quantum age, protecting the security and privacy of data is very important. In this case, hash-based cryptography is very important because it provides strong ways to keep data safe and real, even when there are complex quantum attacks going on [25]. Along with this, different PQC methods help create complete data privacy solutions that protect private data from quantum dangers.

Table 1: Related Work

Scope	Method	Findings	Application
Comprehensive overview of AI applications in cybersecurity	Literature review, case studies	AI techniques enhance threat detection and response times	General cybersecurity enhancements
Focus on ML techniques for threat detection and prevention	Supervised and unsupervised learning models	ML models improve accuracy in detecting malware and anomalies	Malware detection, anomaly detection
Analysis of deep learning applications in network security	Deep learning algorithms, neural networks	Deep learning models effectively identify complex attack patterns	Network intrusion detection
User behavior analytics for insider threat detection	Behavioral analysis, clustering, anomaly detection	Behavioral models detect insider threats by identifying unusual user activities	Insider threat detection
AI-driven automation for incident response	AI algorithms, automation frameworks	Automated systems reduce response times and mitigate impact of cyber incidents	Automated incident response
Real-time threat intelligence using AI	AI models, data mining, pattern recognition	AI provides real-time insights into emerging threats and trends	Threat intelligence, proactive defense
Risks of adversarial attacks on ML models	Analysis of adversarial techniques, defensive strategies	Highlighted vulnerabilities of ML models to adversarial attacks and proposed mitigation strategies	Enhancing robustness of ML models
AI applications in endpoint protection	ML algorithms, endpoint monitoring	Improved detection of endpoint threats through continuous monitoring and pattern recognition	Endpoint security, threat detection
Application of supervised learning in detecting malware	Supervised learning, feature extraction	High accuracy in identifying new and unknown malware using supervised learning techniques	Malware detection, cyber threat prevention

Detecting network anomalies using unsupervised learning	Clustering, outlier detection	Effective identification of network anomalies without requiring labeled data	Network security, anomaly detection
Application of reinforcement learning in adaptive security	Reinforcement learning algorithms, simulation	Adaptive security systems that learn and evolve with changing threat landscapes	Adaptive cybersecurity measures
Predictive analytics for future threat identification	Predictive modeling, data analysis	Enhanced ability to predict and prevent potential cyber threats	Predictive threat analysis, proactive defense
Ethical implications of AI deployment in security	Ethical analysis, case studies	Emphasized the need for transparency, fairness, and accountability in AI systems	Ethical AI deployment, policy development
Combining AI with existing security protocols	Hybrid models, integration strategies	Improved overall security posture by leveraging strengths of both AI and traditional measures	Hybrid security systems, enhanced defense
Real-time detection of anomalies in networks	Real-time data processing, ML algorithms	Real-time anomaly detection systems provide immediate alerts and responses to suspicious activities	Real-time network security, threat mitigation
Examination of challenges in AI adoption for security	Survey, expert interviews	Identified key challenges such as data privacy, model interpretability, and scalability	Addressing challenges, improving AI adoption strategies

The arrival of quantum computing means that cryptography needs to change in a big way. Post-quantum security gives us a way to protect our digital future from quantum computers' powerful abilities. We can make security systems that work well by improving and combining different types of cryptography, like hash-based, code-based, multivariate polynomial, and lattice-based cryptography, as well as mixed systems. In a time when quantum computing could completely change and upset current security models, these frameworks are necessary to make sure that data is correct, private, and real. PQC's ongoing research and development are very important for protecting our digital infrastructure and making sure that it is safe from new quantum risks.

III.PROPOSED APPROACH

1. Algorithm Development:

Lattice-based cryptography is the foremost progressed sort of post-quantum cryptography think about since it is exceptionally safe to quantum assaults and can be utilized in a wide extend of secure circumstances. Lattice-based cryptography is based on issues like Learning With Mistakes (LWE) and its form, Ring-LWE. Both of these take advantage of the truth that it is difficult to illuminate cross section issues in places with a parcel of measurements. Quantum computers are thought to be

able to fathom these issues, which makes them culminate for making secure cryptographic primitives. Including little, arbitrary botches to direct conditions is what Learning With botches (LWE) does. This makes the issue incomprehensible to reply without knowing the design of the blunders. The security of LWE-based cryptographic strategies depends on this hardness. LWE can be utilized to create solid encryption plans. The security of the ensured information depends on how difficult it is to illuminate these loud conditions. So also, Ring-LWE may be a way better form that works inside the arithmetical structure of polynomial rings and makes strides both speed and scale. Since it works within polynomial rings, Ring-LWE cuts down on the additional work and space required for LWE, making it more valuable within the genuine world.

LWE-based encryption methods give semantic security, which implies that indeed on the off chance that an assailant sees different ciphertexts, they won't be able to figure out anything valuable approximately the plaintexts. Key exchange frameworks utilize LWE to create beyond any doubt that parties can securely share cryptographic keys with each other. This keeps the keys secure from quantum assailants. Advanced marks based on LWE and Ring-LWE make it conceivable to check that messages are real and total, which is exceptionally vital for secure communication within the quantum time. To optimize these programs, you have got to form them work way better whereas keeping their security. To form things run speedier, strategies like clumping, concurrent preparing, and polynomial optimization are utilized. Too, choosing the proper parameters is exceptionally imperative for combining the require for security against quantum dangers with the require for quick computing. The creation and advancement of LWE and Ring-LWE calculations are hence a key step toward solid, quantum-resistant cryptographic frameworks that will be needed to ensure information within the coming quantum time.

Learning With Errors (LWE) Algorithm

1. **Key Generation:**

- Select a secret vector $s \in Z_q^n$ uniformly at random.
- Sample a matrix $A \in Z_q^{m \times n}$ uniformly at random.
- Generate an error vector $e \in Z_q^m$ according to the error distribution χ.
- Compute the public vector:
$$b = A\,s + e \ (\text{mod } q)$$
- Public key: (A,b)
- Secret key: s

2. **Encryption:**

- To encrypt a message $m \in \{0,1\}^n$:
- Sample a random vector $\in Z_q^m$.
- Generate an error vector $e' \in Z_q^n$ from the error distribution χ.
- Compute the ciphertext components:
$$c_1 = A^T X + e^{'}(mod\ q)$$
$$c_2 = b^T X + e_m + m.\left\lfloor \frac{q}{2} \right\rfloor (mod\ q)$$
- Ciphertext: $(c_1,c2)$

3. **Decryption:**

- To decrypt the ciphertext $(c_1,2)$ using the secret key s:
- Compute:
$$m^{'} = c2 - {c_1}^T s\ (modq)$$
- Recover the message m by mapping m' to $\{0,1\}^n$

Typically, this involves interpreting values close to 0 as0 and values

Close to $\left\lfloor \frac{q}{2} \right\rfloor$ as 1.

The LWE algorithm is a building block for making post-quantum cryptographic schemes that are safe. Its main parts—key creation, encryption, and decryption take advantage of how hard the LWE problem is to solve.

2. Security Analysis:

The study of post-quantum cryptographic methods' security begins with hypothetical proofs. The essential issues, just like the Learning With Blunders (LWE) issue in lattice-based cryptography, are appeared to be numerically difficult by these discoveries [5]. For case, the security of LWE-based plans depends on the thought that it is inconceivable to discover brief vectors in high-dimensional grids, not indeed with quantum computing control. There are strict proofs that connect the encryption scheme's safety to well-studied hard problems, overview illustrate in figure 1. These proofs show that any effective attack on the scheme would also solve the underlying problems, which are thought to be quantum-resistant. This theory basis is very important for showing why these plans should be used in real life.

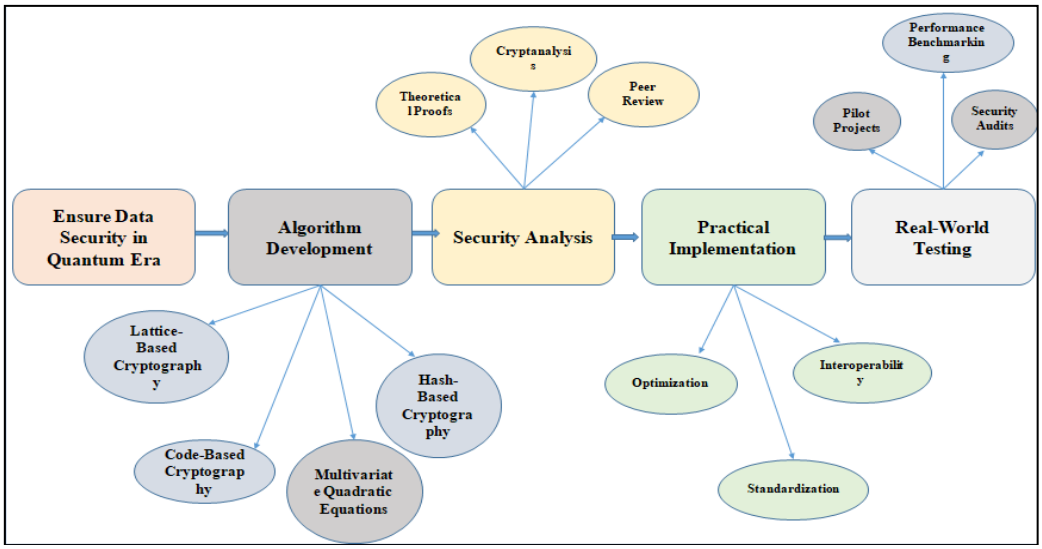

Figure 1: Overview of Architectural block diagram

The next step is cryptanalysis, which looks for possible flaws and holes. There are both routine and quantum dangers here. Direct and differential examination is cases of classical cryptanalysis strategies. Quantum cryptanalysis, on the other hand, looks into procedures like Grover's calculation, which might make brute-force looks quicker. Analysts can discover powerless spots in their programs and make them safer to assaults by testing diverse assault scenarios. To create beyond any doubt full security, side-channel assaults and other real-world assault courses are moreover looked at. Finally, the programs that were made and their security thinks about are looked over by other individuals. Cryptography specialists, who make up the cryptography community, see over the strategies, proofs, and cryptanalysis comes about exceptionally carefully. This prepare is imperative for demonstrating security claims since it brings together diverse specialists and focuses of see. Peer audit regularly brings up things that were missed, which leads to more advancements and makes the frameworks more secure generally. This way of working together makes beyond any doubt that the cryptographic strategies are solid and ready to be utilized within the genuine world. It addresses both scholarly and viable security issues. Post-quantum cryptographic strategies are carefully tried and moved forward utilizing this multifaceted security investigation. This makes beyond any doubt they

can stand up to both classical and quantum assailants, giving individuals confidence in utilizing them to secure information within the quantum time.

3. Practical Implementation:

The primary step is optimization, which points to make strides program speed whereas decreasing computing waste and asset ought. To make things quicker and less delay, strategies like clumping forms, synchronous handling, and great memory administration are utilized. It is very imperative to tune the parameters. Picking the most excellent parameters strikes the proper blend between security and speed, making beyond any doubt that calculations are solid sufficient for real-world utilize. The following step is standardization, which incorporates working with bunches like NIST (National Organized of Measures and Innovation) to form rules for the commerce. This makes beyond any doubt that the programs take after well-known rules and rules, which makes them less demanding for numerous individuals to utilize. Thorough testing and evaluation are part of the standardization process. These make sure that the algorithms meet the necessary speed and security standards. This step is very important for building trust in the business and making sure that different platforms and systems can work together.

For post-quantum secure systems to work with current technology, they must be able to talk to each other. This means making sure that the methods work with current security systems so that the switch can happen smoothly without having to completely change the way things are done now. During the changeover time, hybrid encryption systems that use both classical and post-quantum methods are very helpful because they make sure that older systems can still be used and allow for a slow uptake. Making sure connectivity also means giving developers and system managers help and thorough documents, which makes integration and release go more smoothly. The real application of post-quantum cryptography algorithms makes sure they are efficient, scalable, and ready to be added to current and future security systems by focusing on standards, interoperability, and optimization. This method promises strong defense against quantum risks while still being useful in a wide range of situations.

4. Real-World Testing

Pilot Projects are the first places where algorithms are put into use to test their usefulness and find problems in the real world. For these ventures, the calculations are put to utilize in controlled situations, like inner systems or apps with restricted get to, so that their victory within the genuine world can be tried. Pilot ventures let you make changes to calculations based on criticism from clients and what you see them do. This makes beyond any doubt that the calculations work in genuine life and are prepared to be utilized by more people.

Performance benchmarking could be a way to compare an algorithm's execution to current benchmarks in an objective way. In arrange to do this, speed, effectiveness, and asset utilize must be tried in a number of diverse circumstances, such as with diverse input sorts and computer settings. Analysts can figure out how well the modern calculations work and where they can be improved by comparing execution information with standard measures. Execution testing may be a awesome way to discover out how well an algorithm works completely different situations and how it can be scaled up or down. Security reviews are fundamental to form beyond any doubt that calculations can handle assaults that happen within the genuine world. A parcel of testing is done as portion of these checks to discover any conceivable gaps or frail spots within the security of the programs. Conventional cryptographic assaults, like brute-force and side-channel assaults, are included in security audits. So are virtual quantum assaults that utilize strategies like Grover's calculation. Analysts can make beyond any doubt that the calculations are solid sufficient to secure private information from a wide extend of dangers by putting them through careful security tests. Post-quantum cryptographic

methods are altogether tried within the genuine world to form sure they work well and are secure. Pilot ventures let you test things within the genuine world and make changes over and over once more, and execution testing gives you clear numbers to compare things to. Security checks make beyond any doubt that calculations can withstand a wide extend of assaults, indeed ones from quantum adversaries. By successfully trying post-quantum security calculations within the genuine world, experts can appear that they are prepared to be utilized in vital applications, giving individuals faith in their convenience and steadfastness.

5. Transition Strategy:

Crossover Frameworks are exceptionally imperative within the starting of the move since they mix classical and post-quantum strategies to form beyond any doubt they work with each other and are secure. Making blended encryption frameworks implies combining both sorts of calculations into current frameworks, which lets them do two things at once. This strategy makes beyond any doubt that the classical calculation can be utilized as a reinforcement in case a post-quantum calculation falls flat or runs into issues. This keeps security up and running. Cross breed frameworks too make moderate exchange simpler, so businesses can test and receive post-quantum arrangements without ceasing their operations. Movement Rules are exceptionally critical for organizations to create the move handle go easily. There are particular steps and best hones in these guides for combining post-quantum security frameworks. For illustration, they conversation around figuring out which post-quantum strategies to utilize and how to apply them in stages. Rules push how vital it is to keep things secure amid the move period and recommend strategies such as double encryption and marking frameworks to keep data secure with both classical and post-quantum cryptography. They too conversation approximately how to create beyond any doubt that organizations are completely prepared for the switch by changing equipment and program to meet the new encryption benchmarks.

Making individuals mindful of the require for post-quantum security and giving them the abilities to set up and run these modern frameworks are two of the foremost vital things that can be done. Preparing classes ought to cover both the scholastic and commonsense sides of post-quantum calculations, counting their aces and cons and how to put them into activity. This data can be shared with IT laborers, coders, and individuals who make choices through workshops, addresses, and online preparing. Mindfulness endeavors make individuals mindful of the perils that quantum computing postures and how important it is to require activity some time recently it's as well late. This empowers a culture of availability and sharpness inside companies. The methodology for transitioning from classical to post-quantum encryption frameworks makes beyond any doubt that the alter is secure and smooth by making blended frameworks, giving point by point exchange informational, and advancing information and preparing broadly. This differing strategy brings down dangers, keeps security up and running, and gives businesses the certainty to utilize progressed secure arrangements to induce prepared for the quantum age.

IV.RESULT AND DISCUSSION

Table 2 appears that once you compare post-quantum cryptographic calculations based on diverse execution variables, you'll see that each sort has its possess qualities and flaws. This appears that they are valuable for distinctive errands within the quantum time. Lattice-Based Cryptography is exceptionally great at a number of imperative things. In terms of key size (95%), encryption/decryption time (90%), signature estimate (95%), and computing speed (95%), it gets the most excellent marks. This makes it exceptionally valuable and effective for numerous employments, giving solid security with sensible asset needs. Lattice-based calculations are awesome since they can be utilized on a expansive scale and are exceptionally safe to quantum assaults. This makes them

a best choice for post-quantum measures. Code-Based Cryptography works well too, especially when it comes to key size (85%) and security level (85%). It takes a little longer to encrypt and decode (75% of the time) and uses more computing power (80% of the time), but it is still a strong competitor because its theory is well-developed and its security features have been tested. Code-based schemes, like the McEliece cryptosystem, are known to be strong against both classical and quantum attacks. However, their bigger key sizes make them less convenient for some users. With scores of 80% for key size, encryption/decryption time, and signature size, multivariate quadratic equations have a fair performance. They also get 75% for processing efficiency. It's not the best in any one area, but it's a flexible choice that's easy to put into action and works well in real life. But its level of security (80%) is a little lower than that of grid and code-based cryptography, which could be a problem for very secret uses.

Table 2: Comparison of various post quantum cryptographic algorithm

Performance Parameter	Lattice-Based	Code-Based	Multivariate Quadratic	Hash-Based
Key Size	95	85	80	90
Encryption/Decryption Time	90	75	80	85
Signature Size	95	80	80	90
Computational Efficiency	95	80	75	80
Security Level	90	85	80	85

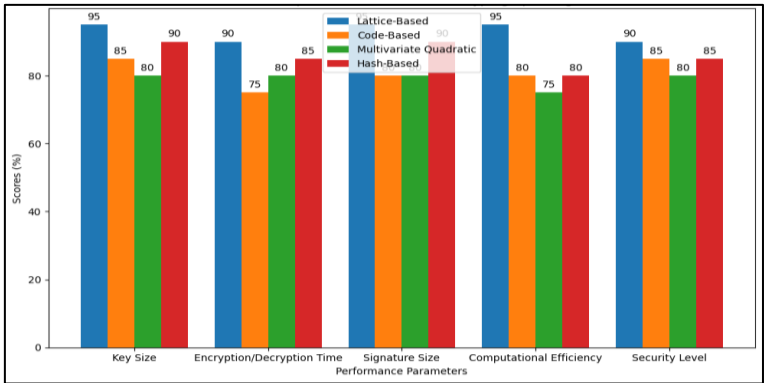

Figure 2: Performance comparison of Post quantum cryptographic algorithm

Hash-Based Cryptography works very well, especially when it comes to key size (90%), signature size (90%), and encryption/decryption time (85%). It is a strong and efficient choice because both its computing efficiency and security level are at 85%. Hash-based schemes, like SPHINCS+ and the Merkle Signature Scheme, are liked for being easy to use and providing good security. They do this by using the well-known hardness of hash functions. Each post-quantum cryptography method has its own benefits. For total security and speed, lattice-based cryptography sticks out. Code-based cryptography has been shown to be strong, multivariate quadratic equations work well, and hash-based cryptography is easy to use and works well. To get the best security in the quantum era, the choice of method rests on the needs of the application, taking into account things like key size, computing speed, and security level. Figure 2 shows a bar chart comparing four post-quantum cryptography algorithms across five performance parameters: key size, encryption/decryption time, signature size, processing power, and security level. The algorithms are grid-based, code-based, multivariate quadratic encryption, and hash-based encryption. The results, displayed as numbers, are shown on the Y-axis, while the individual values are plotted on the X-axis. Lattice-based encryption always performs best in every test. It achieves the best results in terms of key size (95%), encryption/decryption time (90%), signature size (95%), processing speed (95%), and security level

(90%). This indicates that it is generally strong and can be used for a variety of tasks that require high performance and strong security.

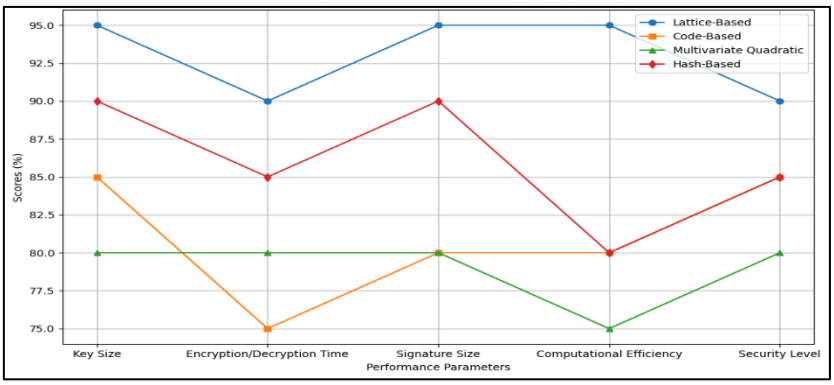

Figure 3: Line graph of Performance comparison of post quantum algorithm

Code-based encryption also performs very well, especially in terms of key size (85%) and security level (85%). However, it is slightly inferior in terms of encryption/decryption time (75%), signature size (80%), and computational power (80%). This means that it has a good balance of performance, slightly less efficient, but high security. With values of key size, encryption/decryption time, signature size, and security level of 80%, multivariate quadratic encryption gives good results overall. However, it performs slightly worse in terms of computational power (75%), which means it is not the best in any particular area but is a flexible choice. Hash-based encryption performs well especially in terms of key size (90%), encryption/decryption time (85%) and signature size (90%). It also scores highly in terms of processing efficiency (80%) and security level (85%), showing how efficient and secure it is especially in hash-based processes. In general, the bar chart makes it easy to see how each encryption method compares and shows its advantages and disadvantages. We highlight how flexible grid-based encryption is as a first choice, and also acknowledge the superior performance of code-based, multivariate squared and hash-based encryption methods. As shown in Figure 3, the line graph compares four post-quantum cryptographic algorithms: Lattice-Based, Code-Based, Multivariate Quadratic, and Hash-Based Cryptography. It does this by looking at five performance factors: Key Size, Encryption/Decryption Time, Signature Size, Computational Efficiency, and Security Level. The x-axis shows each parameter, and the y-axis shows the success scores (in percentages) that go with each parameter. Lattice-Based Cryptography is shown by a straight line with rings on it. This method regularly gets high scores across all parameters: 95% for Key Size, Signature Size, and Computational Efficiency; 90% for Encryption/Decryption Time, and 80% for Security Level. This consistent high performance shows that it can be used for many different tasks that need strong and effective security solutions.

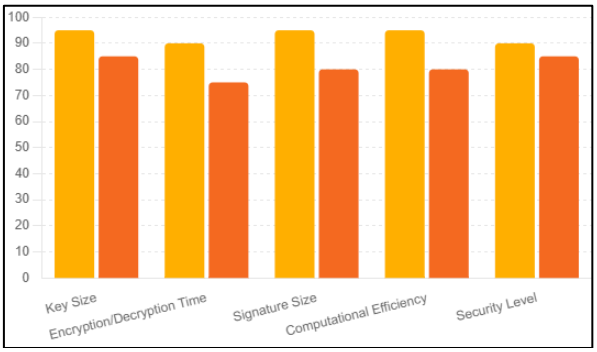

Figure 4: Comparison the performance parameters of lattice-based and code-based cryptography schemes

Code-Based Cryptography, which is shown by a line with squares on it, works in a few different ways. It gets 85% for both Key Size and Security Level, which means it has good security and key sizes that aren't too big to handle. Only 75% of the time is spent encrypting and decrypting, and 80% of the time is spent on signature size and computational efficiency. It looks like code-based cryptography is safe, but it might take more time and computing power to encrypt and decode than lattice-based ways, based on these results. The performance of multivariate quadratic cryptography, which is shown with triangles, is about average but not great across all factors. It regularly scores 80% for Key Size, Encryption/Decryption Time, Signature Size, and Security Level, but only 75% for Computational Efficiency. This shows a flexible but slightly less efficient method that can be used in some situations where mild security and implementation complexity are okay. As shown, in figure 4, by the diamonds, Hash-Based Cryptography does well in Key Size (90%), Signature Size (90%), and Encryption/Decryption Time (85%). Its scores in Computational Efficiency and Security Level are slightly lower, at 80% and 85% respectively.

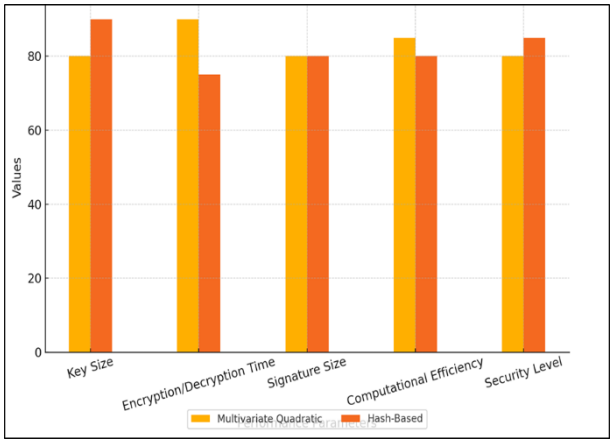

Figure 5: Comparison Of Multivariate Quadratic And Hash-Based Scheme

This makes it a great choice for digital signature uses. Overall, the line graph does a good job of showing how the pros and cons of each security method compare. Because it works so well in so many areas, Lattice-Based Cryptography is a strong choice for future encryption standards. Code-Based Cryptography is very secure, but it takes a long time and isn't very efficient at computing. Multivariate Quadratic Cryptography has average to good performance, while Hash-Based Cryptography, shown in figure 5, is best at things that have to do with signatures. You can better understand the pros and cons and choose the best encryption method for your needs by looking at this picture comparison.

V.CONCLUSION

The fast growth of quantum computing makes standard encryption systems very difficult to use. To keep data safe in the quantum era, new advanced methods in post-quantum cryptography need to be created. This paper explored many areas of post-quantum cryptography, including developing new algorithms, analyzing their security, practical implementations, testing them in the real world, and developing switching possibilities. Researchers are constantly working to develop cryptographic methods based on mathematical problems that cannot be cracked by quantum attacks. There are many good ways to solve this problem, each with their own advantages and disadvantages. Examples include lattice-based cryptography, code-based cryptography, multivariate quadratic equations, and hash-based cryptography. Security research is a critical part of ensuring that post-quantum cryptography methods perform well against both classical and quantum attackers. There are rigorous theoretical proofs, thorough cryptanalysis, and peer review methods to ensure that these algorithms work well in the wild. Real-world applications focus on improving and standardizing how the

algorithms work, and ensuring they work with other systems. Pilot projects, speed tests, and security audits allow us to test how well and securely the algorithms work in real-world environments. Real-world testing is extremely useful because it shows how well and securely the algorithms work in real-world situations. This helps us make smart decisions about how to apply and connect with other systems. Organizations need transition plans in order to move smoothly from classical to post-quantum encryption systems. Hybrid systems, transfer standards, and awareness programs are all very important for making sure that the change goes smoothly and securely, with as little downtime as possible and full data security. In conclusion, to lessen the dangers that quantum computing could bring, new methods in post-quantum encryption must be created and used. We can keep private data safe and trust in encrypted systems in the quantum age and beyond by using new cryptographic methods, doing thorough security assessments, and putting in place strong transfer plans.

References

[1] Yong Chen, Shucui Xie and Jianzhong Zhang, "A hybrid domain image encryption algorithm based on improved henon map", Entropy, vol. 24, no. 2, pp. 287, 2022.

[2] Ashraf Ahmad, Yousef AbuHour, Remah Younisse, Yasmeen Alslman, Eman Alnagi and Qasem Abu Al-Haija, "MID-Crypt: a cryptographic algorithm for advanced medical images protection", Journal of Sensor and Actuator Networks, vol. 11, no. 2, pp. 24, 2022.

[3] Mohamed Elhoseny, K. Shankar, S. K. Lakshmanaprabu, Andino Maseleno and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things", Neural computing and applications, vol. 32, pp. 10979-10993, 2020.

[4] Nirmal Chaudhary, Tej Bahadur Shahi and Arjun Neupane, "Secure image encryption using chaotic hybrid chaotic and block cipher approach", Journal of Imaging, vol. 8, no. 6, pp. 167, 2022.

[5] Arpit Chaudhari, Prachi Jaini," Stealthier attack on zone routing protocol in wireless sensor network," 2014 Fourth International Conference on Communication Systems and Network Technologies,pp- 734-738

[6] Joshua C. Dagadu, Jian-Ping Li and Emelia O. Aboagye, "Medical image encryption based on hybrid chaotic DNA diffusion", Wireless Personal Communications, vol. 108, pp. 591-612, 2019.

[7] Abdulaziz Shehab, Mohamed Elhoseny, Khan Muhammad, Arun Kumar Sangaiah, Po Yang, Haojun Huang, et al., "Secure and robust fragile watermarking scheme for medical images", IEEE access, vol. 6, pp. 10269-10278, 2018.

[8] Dhivya Ravichandran, Aashiq Banu S, B. K. Murthy, Vidhyadharini Balasubramanian, Sherin Fathima and Rengarajan Amirtharajan, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain", Medical & biological engineering & computing, vol. 59, pp. 589-605, 2021.

[9] Kale, Rohini Suhas , Hase, Jayashri , Deshmukh, Shyam , Ajani, Samir N. , Agrawal, Pratik K & Khandelwal, Chhaya Sunil (2024) Ensuring data confidentiality and integrity in edge computing environments : A security and privacy perspective, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-A, 421–430, DOI: 10.47974/JDMSC-1898

[10] Dari, Sukhvinder Singh , Dhabliya, Dharmesh , Dhablia, Anishkumar , Dingankar, Shreyas , Pasha, M. Jahir & Ajani, Samir N. (2024) Securing micro transactions in the Internet of Things with cryptography primitives, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-B, 753–762, DOI: 10.47974/JDMSC-1925

[11] Limkar, Suresh, Singh, Sanjeev, Ashok, Wankhede Vishal, Wadne, Vinod , Phursule, Rajesh & Ajani, Samir N. (2024) Modified elliptic curve cryptography for efficient data protection in wireless sensor network, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-A, 305–316, DOI: 10.47974/JDMSC-1903

[12] Walid El-Shafai, Hayam A. Abd El-Hameed, Noha A. El-Hag, Ashraf AM Khalaf, Naglaa F. Soliman, Hussah Nasser AlEisa, et al., "Proposed Privacy Preservation Technique for Color Medical Images", Intelligent Automation & Soft Computing, vol. 36, no. 1, 2023.

[13] Ajani, S. N. ., Khobragade, P. ., Dhone, M. ., Ganguly, B. ., Shelke, N. ., & Parati, N. . (2023). Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 546–559

[14] A. Majumdar, N. M. Laskar, A. Biswas, S. K. Sood and K. L. Baishnab, "Energy efficient e-healthcare framework using HWPSO-based clustering approach", Journal of Intelligent & Fuzzy Systems, vol. 36, no. 2, pp. 1-13, 2019.

[15] Y. Zou, Z. Zhao, S. Shi, L. Wang, Y. Peng, Y. Ping, et al., "Highly Secure Privacy-Preserving Outsourced k-Means Clustering under Multiple Keys in Cloud Computing", Security and Communication Networks, vol. 3, pp. 1-11, 2020.

[16] M. Felemban, A. Daghistani, Y. Javeed, J. Kobes and A. Ghafoor, A Security and Performance Driven Architecture for Cloud Data Centers, 2020.

[17] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam et al., "Experimentally generated randomness certified by the impossibility of superluminal signals", Nature, vol. 556, no. 7700, pp. 223-226, 2018.
[18] Ashwaq T. Hashim, Amira K. Jabbar and Qussay F. Hassan, "Medical image encryption based on hybrid AES with chaotic map", Journal of Physics: Conference Series, vol. 1973, no. 1, pp. 012037, 2021.
[19] Chiranji Lal Chowdhary, Pushpam Virenbhai Patel, Krupal Jaysukhbhai Kathrotia, Muhammad Attique, Kumaresan Perumal and Muhammad Fazal Ijaz, "Analytical study of hybrid techniques for image encryption and decryption", Sensors, vol. 20, no. 18, pp. 5162, 2020.
[20] Ehsan Hesamifard, Hassan Takabi and Mehdi Ghasemi, "Deep neural networks classification over encrypted data", Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy, pp. 97-108, 2019.
[21] Amal Hafsa, Anissa Sghaier, Jihene Malek and Mohsen Machhout, "Image encryption method based on improved ECC and modified AES algorithm", Multimedia Tools and Applications, vol. 80, pp. 19769-19801, 2021.
[22] Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems", Multimedia Tools and Applications, vol. 80, pp. 21165-21202, 2021.
[23] Fawad Masood, Maha Driss, Wadii Boulila, Jawad Ahmad, Sadaqat Ur Rehman, Sana Ullah Jan, et al., "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations", Wireless Personal Communications, vol. 127, no. 2, pp. 1405-1432, 2022.
[24] B Pushpa, "Hybrid data encryption algorithm for secure medical data transmission in cloud environment", 2020 Fourth international conference on computing methodologies and communication (ICCMC), pp. 329-334, 2020.
[25] Yasmeen Alslman, Eman Alnagi, Ashraf Ahmad, Yousef AbuHour, Remah Younisse and Qasem Abu Al-haija, "Hybrid Encryption Scheme for Medical Imaging Using AutoEncoder and Advanced Encryption Standard", Electronics, vol. 11, no. 23, pp. 3967, 2022.
[26] KC Prabu Shankar and S. Prayla Shyry, "A novel hybrid encryption method using S-box and Henon maps for multidimensional 3D medical images", Soft Computing, pp. 1-11, 2023.