Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 3s (2024)

Cryptographic Protocols Resilient to Quantum Attacks: Advancements in Post-Quantum Cryptography

Pallavi Niraj Vithalkar[1], Parmanand Prabhat[2], Vikas Haribhau Satonkar[3], Manisha Sagar Jangale[4], Rakhi Madhukar Giradkar[5], Sachin Ashok Murab[6]

[1]Assistant Professor, Department of Artificial Intelligence and Data Science, Sandip Institute of Technology & Research Centre, Nashik Maharashtra, India. pallavi.vithalkar@sitrc.org

[2]Assistant Professor, Department of Computer Engineering, Sandip University, Sijoul, Bihar, India. parmanand.prabhat@sandipuniversity.edu.in

[3]Assistant Professor, Assistant Professor, Department of Computer Engineering, Sandip Institute of Engineering & Management, Nashik, Maharashtra, India. vikas.satonkar@siem.org.in

[4]Assistant Professor, Department of Electronics and Telecommunication, Sandip Institute of Engineering & Management, Nashik, Maharashtra, India. manisha.jangale@siem.org.in

[5]Assistant Professor, Sandip University Nashik, Maharashtra, India. rakhi.giradkar@sandipuniversity.edu.in

[6]Assistant Professor, Department of Artificial Intelligence and Data Science, Sandip Institute of Technology & Research Centre, Nashik Maharashtra, India. sachin.murab@sitrc.org

Article History:

Received: *15-04-2024*

Revised: *02-06-2024*

Accepted: *18-06-2024*

Abstract:

New developments in quantum computing have made people worry that current security methods could be broken by quantum attacks. Some mathematical problems are hard to solve, which is how traditional encryption methods like RSA and ECC keep their secrets safe. However, quantum computers might be able to solve these issues a lot faster than regular computers, which makes these methods less safe. Because of this threat, experts have been working hard to make post-quantum cryptography methods that quantum computers can't break. These methods are made to stand up to the strength of quantum algorithms and protect the privacy, integrity, and validity of private data even when quantum attackers are present. Lattice-based cryptography is a potential method for post-quantum encryption. Its security comes from the difficulty of certain lattice problems. Lattice-based methods are thought to be safe from threats from both traditional and quantum computers because they offer good security promises. Lattice-based cryptography is a flexible way to build different types of cryptographic primitives, like encryption, digital signatures, and key sharing protocols. The study of code-based cryptography, which is based on how hard it is to decode some error-correcting codes, is another important advance. Code-based methods have been around for a long time and have been studied a lot, which makes them a good choice for security after quantum computing. Code-based cryptography is also easy to use and has strong security features, which makes it a good choice for real-world situations. Multivariate polynomial cryptography is another possible choice for cryptography after quantum computing. The safety of this method depends on how hard it is to solve systems of multivariate polynomial problems. Multivariate polynomial methods might not be as secure as lattice-based or code-based cryptography, but they are interesting options for some situations and places with limited resources.

Keywords: Quantum computing, Cryptographic protocols,Post-quantum cryptography, RSA, Lattice-based cryptography, Shortest vector problem (SVP), Learning with errors (LWE) problem, Code-based cryptography, McEliece cryptosystem.

1.INTRODUCTION

The development of quantum computing has brought both huge new possibilities and huge new problems to the area of cryptography. Quantum computers could change the way computers work and lead to big steps forward in many areas, but they also pose a major threat to the safety of present cryptographic methods [1]. Some mathematical problems, like integer factorization and the discrete logarithm problem, are hard to solve, which is how traditional encryption methods like RSA and ECC keep their secrets safe. However, quantum computers might be able to solve these issues a lot faster than regular computers, which means that quantum attacks could be used against these systems [2]. Because quantum attacks are a real possibility, a lot of work has been put into making encryption systems that can handle the power of quantum computers. Post-quantum cryptography is the newest area of cryptography that tries to protect the privacy, security, and validity of private data even when quantum attackers are present [3]. It's not just a nice idea to work on post-quantum security methods; we need to do it right away to protect our digital assets from the danger of quantum attacks. Lattice-based cryptography [4] is one of the most likely ways to do post-quantum encryption. Lattice-based cryptography is safe because it uses the fact that some lattice problems are very hard to solve, like the shortest vector problem (SVP) and the learning with errors (LWE) problem [5]. Quantum algorithms may not be able to solve these lattice problems, which makes lattice-based methods a strong option for post-quantum cryptography. Lattice-based cryptography is a flexible way to create different types of cryptographic primitives, such as encryption, digital signatures, and key sharing protocols. Lattice-based cryptography is safe because it's hard to solve lattice problems, which is thought to be hard even for quantum computers [6]. Because of this, lattice-based encryption methods offer strong protection against both conventional and quantum attackers.

Along with code-based cryptography, lattice-based cryptography has become an important area of study in post-quantum encryption. Code-based cryptography is safe because it uses error-correcting codes that are hard to compute, like the McEliece cryptosystem [7]. Code-based systems are safe because it's hard to decode linear codes, which are thought to be hard for quantum algorithms to crack. Code-based cryptography has been around for a long time and has been studied a lot. It has strong security features and can be used quickly [8]. Code-based security methods have also been defined and are used in a lot of different uses. This shows that they can be used to protect our digital infrastructure. Multivariate polynomial cryptography has gotten a lot of interest as another possible choice for cryptography after quantum computing. For security, multivariate polynomial cryptography rests on how hard it is to solve sets of multivariate polynomial equations, like the hidden field equations (HFE) problem [9]. Multivariate polynomial methods might not be as secure as lattice-based or code-based cryptography, but they are interesting options for some situations and places with limited resources. It is very important to keep the field of post-quantum cryptography on the cutting edge of the fight to protect our digital systems from quantum attacks [10]. Post-quantum security methods try to protect the privacy, stability, and validity of private data in the quantum age and beyond by using math problems that are thought to be hard for both classical and quantum computers [11]. As quantum computing keeps getting better, it will be important to make sure that our digital activities and messages are safe and private by creating strong and reliable cryptographic methods.

2.RELATED WORK

A lot of study is being done in the field of post-quantum cryptography to find ways to deal with the danger that quantum computing poses to current encryption systems. The NIST Post-Quantum Cryptography Standardization method is one of the most important projects in this field. It evaluates all the different post-quantum encryption techniques. As part of this project, possible algorithms are being carefully analyzed for their cryptanalysis, security, and speed. The goal is to find the ones that have strong security qualities and can be used in real life [12]. The cryptographic community has come a long way in finding and supporting cryptographic schemes that can't be broken by quantum attacks thanks to this standards process.

One important area of study in post-quantum cryptography is lattice-based encryption, which uses the difficulty of computing lattice problems to make security stronger. Lattice-based cryptography has been used by researchers to create safe communication systems that can stand up to quantum attackers [13]. Mathematical analysis and protocol design have been used to make sure that these protocols work in real life. Code-based cryptography has become another important area of study, with work being done to create and use error-correcting code-based cryptographic methods. These plans have shown that they can work in the real world to protect digital data, which is a big part of reducing the threat from quantum computing.

Along with the creation of cryptography protocols, a lot of work has gone into making quantum-secure key sharing protocols. These methods try to set up safe ways of communicating that can withstand quantum attacks. This protects the privacy and accuracy of the data being sent. In addition, progress in multivariate polynomial cryptography has led to the creation of effective post-quantum security methods and protocols [14]. Because of these changes, there are now a wider range of cryptographic building blocks that can be used to make systems safe in the quantum age.

Quantum computing has changed traditional public-key cryptosystems, which has led to a lot of study into quantum threats and what they mean. Researchers using quantum algorithm analysis and cryptanalysis have found flaws in traditional cryptosystems like RSA and ECC. This means that post-quantum cryptography solutions are needed [15]. A lot of focus has also been paid to how post-quantum cryptography is being used in new technologies like bitcoin and the Internet of Things (IoT). Secure multiparty computation methods that are not vulnerable to quantum attacks have also been created to protect the privacy and security of computations that happen in distributed settings [16].

Post-quantum cryptography is becoming more useful by incorporating hardware solutions and connecting to cloud computer platforms, in addition to developing new algorithms. People have tried to make hardware versions of post-quantum cryptographic methods that work well and can be used in places with limited resources [17]. Also, security protocols have been suggested that are designed to make cloud computing safe in the quantum era. These protocols would protect private data in cloud settings from quantum dangers. To make sure safe access control even when quantum enemies are present, people have also come up with ways to authenticate that are not affected by quantum mechanics.

Education and information campaigns are very important for getting people to use post-quantum cryptography. To help researchers, developers, and practitioners learn more about post-quantum security, training classes, workshops, and teaching tools have been made available [18]. Giving developers tools and packages that are easy to use makes it easier to add post-quantum secure methods to software programs. This improves security in the quantum era as a whole.

Table 1: Related Work

Sr. No.	Scope	Method	Findings
1	Comprehensive evaluation of various post-quantum cryptographic algorithms	Cryptanalysis, security analysis, and performance evaluation	Identification of candidate algorithms for standardization, highlighting their security properties and performance characteristics
2	Secure communication protocols resilient to quantum attacks using lattice-based cryptography	Mathematical analysis and protocol design	Development of secure communication protocols based on lattice-based cryptography
3	Practical implementation and deployment of code-based cryptographic schemes	Implementation, performance evaluation, and security analysis	Demonstration of the practical viability and efficiency of code-based cryptographic schemes for securing digital communications
4	Development of key exchange protocols resistant to quantum attacks	Protocol design and security analysis	Introduction of novel key exchange protocols that provide security against quantum adversaries
5	Advancements in multivariate polynomial cryptography for post-quantum security	Algorithmic improvements and security analysis	Development of efficient algorithms and protocols based on multivariate polynomial cryptography for achieving post-quantum security
6	Analysis of quantum algorithms and their impact on classical public-key cryptosystems	Quantum algorithm analysis and cryptanalysis	Identification of vulnerabilities in classical public-key cryptosystems and the need for post-quantum cryptography solutions
7	Application of post-quantum cryptographic protocols in Internet of Things (IoT) environments	Integration with IoT platforms and performance evaluation	Demonstration of the feasibility and effectiveness of post-quantum cryptographic solutions in securing IoT devices and networks
8	Development of digital signature schemes resilient to quantum attacks	Cryptographic scheme design and security analysis	Introduction of digital signature schemes that remain secure in the presence of quantum adversaries
9	Integration of post-quantum cryptographic techniques into blockchain technologies	Blockchain protocol modifications and cryptographic scheme integration	Enhancement of blockchain security through the adoption of post-quantum cryptographic techniques
10	Secure computation protocols resistant to quantum attacks	Protocol design and security analysis	Development of multiparty computation protocols that ensure security in the presence of quantum adversaries
11	Implementation of post-quantum cryptographic schemes on hardware platforms	Hardware design and performance evaluation	Development of efficient hardware implementations of post-quantum cryptographic schemes for use in resource-constrained environments
12	Cryptographic protocols for	Protocol design and	Introduction of cryptographic protocols that

	secure cloud computing resilient to quantum attacks	integration with cloud computing platforms	ensure the security and privacy of data in cloud computing environments in the presence of quantum threats
13	Authentication schemes resistant to quantum attacks	Authentication protocol design and security analysis	Development of authentication mechanisms that remain secure in the presence of quantum adversaries
14	Development of libraries and tools for implementing post-quantum cryptographic algorithms	Library design, implementation, and usability analysis	Provision of developer-friendly tools and libraries for integrating post-quantum cryptographic algorithms into software applications
15	Education and awareness initiatives regarding post-quantum cryptography	Training programs, workshops, and educational materials	Promotion of understanding and adoption of post-quantum cryptographic techniques among researchers, developers, and practitioners

The study being done in the field of post-quantum cryptography includes a wide range of tasks, such as creating new algorithms and protocols, putting them into practice, and teaching others about them. These attempts show how important it is to change cryptographic methods to deal with the problems that quantum computing brings up. This will protect the privacy and security of digital transactions and messages in the quantum era and beyond.

3.METHODOLOGY

1. Post-Quantum Cryptography:

This type of cryptography, called lattice-based encryption, is a good option for post-quantum methods because it is secure, flexible, and not vulnerable to quantum attacks. Several lattice-based algorithms have become the top contenders. Each one has its own benefits when it comes to security, speed, and usability.

The Learning with Errors (LWE) problem is a well-known lattice-based method that is used as the basis for many encryption schemes, such as Ring-LWE, NTRUEncrypt, and NTRUSign. These plans depend on the fact that it's hard to compute the secret lattice vector when given noisy linear equations. The safety of LWE-based schemes comes from the fact that it is thought to be hard to solve the worst-case lattice problems. This makes them very resistant to quantum attackers. There are also good performance features for LWE-based schemes, with lower memory and processing waste needs compared to some other post-quantum options. Some well-known lattice-based algorithms are the Shortest Vector Problem (SVP) and Ring Learning with Errors (Ring-LWE) and Kyber. The SVP is the basis for these algorithms and works as a key for encryption and key sharing. Because it's hard to find the shortest non-zero lattice vector inside a lattice, these methods are very hard to hack using quantum computing. It's possible that SVP-based schemes are more expensive to run than LWE-based ones, but they provide stronger security and work well for uses that need a lot of cryptographic confidence.

Lattice-based cryptography is naturally adaptable and flexible, which means that custom cryptographic primitives can be made to meet a wide range of security needs. A lot of study and development has gone into lattice-based cryptography, which has helped make algorithms better for certain uses. For example, lightweight versions for settings with few resources and fast methods for safe communication and data security. There are many post-quantum encryption algorithms that can be used in lattice-based cryptography. These algorithms have strong security, good speed, and can be used in real life. By carefully looking at the security features, performance, and usability of LWE and SVP-based schemes, researchers can choose the best algorithms for protocol design. This will help make sure that cryptographic protocols are developed that can withstand quantum attacks and work in the real world.

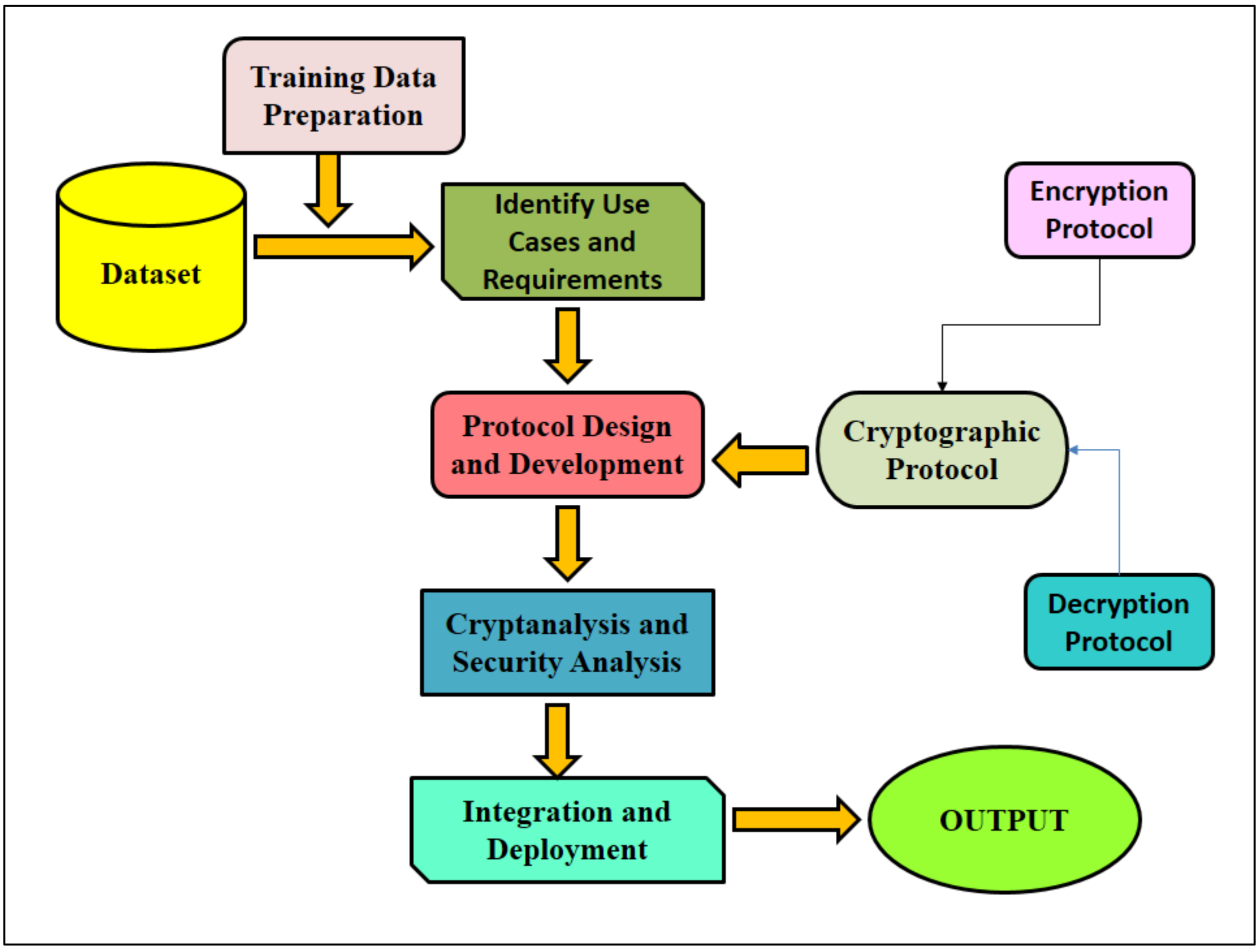
Training Data Preparation
Dataset
Identify Use Cases and Requirements
Encryption Protocol
Protocol Design and Development
Cryptographic Protocol
Decryption Protocol
Cryptanalysis and Security Analysis
Integration and Deployment
OUTPUT

Figure 1: Overview of block diagram for Cryptographic Protocols Resilient

2. Protocol Design and Development:

When it comes to designing and building protocols, the main focus is on making cryptographic protocols that make use of certain Lattice-based cryptography methods. These methods were carefully picked to improve many different parts of cryptography, such as key sharing, encryption, digital signatures, and verification. The protocols that were made use the special features and benefits of Lattice-based cryptography, like how it can stand up to quantum attacks and work well in mathematical settings, to make sure that communication routes are safe and reliable [19].

During the planning process, the different needs that come from different use cases and application models are taken into account. The cryptographic protocols are designed to meet the specific needs of each situation [20]. They make sure that communication channels are safe, data is safe in the cloud, devices are real and trustworthy in IoT ecosystems, and trust and openness are possible in blockchain technologies. Because of this flexible method, it is possible to make systems that can handle the changing security issues that come up with new technologies. Lattice-based cryptography is a key part of making strong and reliable cryptographic methods that can be used in a wide range of real-world situations. This is possible because it was carefully designed and different needs were taken into account.

Algorithm: Designing Cryptographic Protocols with Lattice-Based Cryptography

```
Step 1: Identify Use Cases and Requirements:
    - Determine security requirements ($Sec_i$), performance requirements (Perf_i), and scalability requirements ($Scal_i$) for each use case (i).
Step 2: Select Lattice-based Cryptography Algorithms:
    - Choose algorithms with security parameter ($\lambda$) and computational complexity $T(n)$.
Step 3: Define Protocol Components:
    - Identify components mathematically as
        $Prot_i=\{Compi1,Compi2,...,Compin\}$..
Step 4: Design Key Exchange Protocol:
    - Specify key generation $(Key_{gen})$, distribution $(Key_{dist})$, and agreement $(Key_{agree})$ mechanisms.
Step 5: Design Encryption Protocol:
    - Define encryption $(Enc_{alg})$ and decryption $(Dec_{alg})$ procedures.
Step 6: Design Digital Signature Protocol:
    - Specify signature generation $(Sign_{gen})$and verification $(Sign_{ver})$ processes.
Step 7: Design Authentication Protocol:
    - Define authentication procedures $(Auth_{proc})$ and verification $(Auth_{verif})$ methods.
Step 8: Consider Use Case-specific Requirements:
    - Adapt protocols mathematically to optimize for security, performance, and usability.
```

3. Cryptanalysis and Security Analysis:

Cryptanalysis and security analysis are important steps for making sure that cryptographic methods are strong and resistant to risks like quantum attacks. It is necessary to do a thorough cryptanalysis of the suggested protocols' mathematical foundations and computational assumptions in order to find any possible flaws or vulnerabilities [21]. Usually, this process includes carefully reading the security proofs, considering the algorithmic design choices, and checking the protocol's implementation details for any possible security holes.

When it comes to post-quantum cryptography, testing how well methods can defend against quantum threats gets extra attention. Quantum algorithms, like Shor's algorithm and Grover's algorithm, use the computational benefits of quantum computers to pose a major threat to traditional cryptographic methods. By encrypting the suggested protocols and testing them in different quantum attack situations, we can find any holes that might appear because of the development of quantum computing technologies. For instance, Grover's algorithm makes brute-force attacks faster on symmetric-key cryptosystems [22], while Shor's algorithm makes public-key cryptosystems like RSA and ECC less safe. Researchers can see how resistant the protocols are to quantum attacks and find ways to make them stronger by simulating and analyzing quantum attacks.

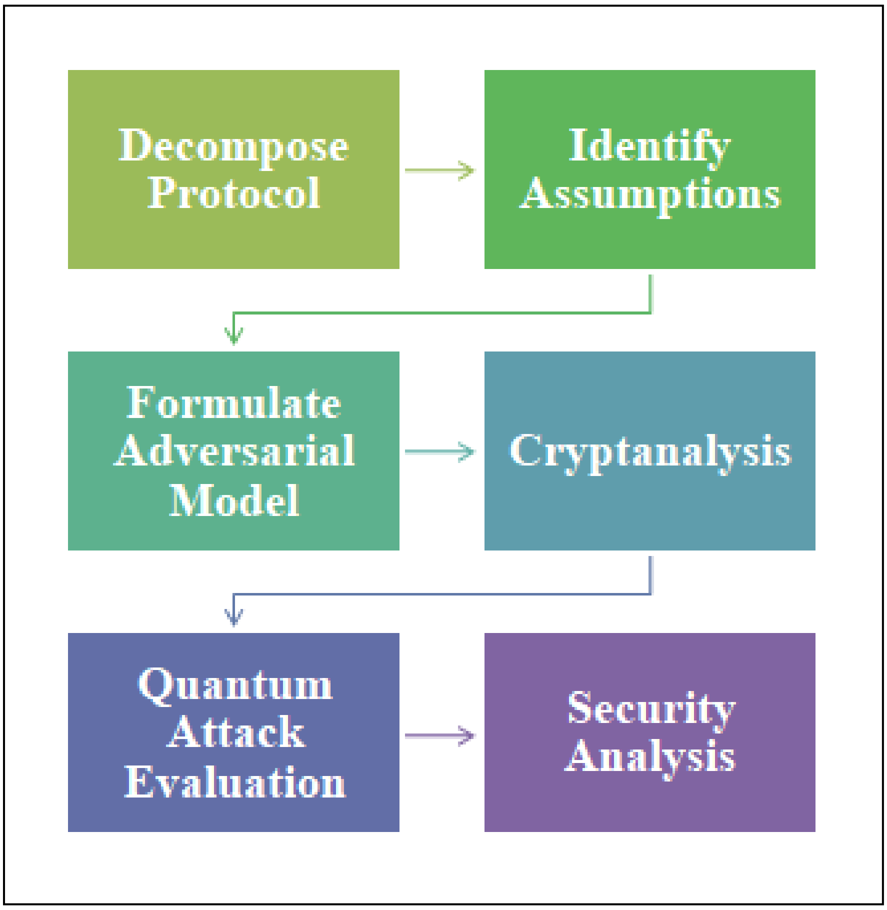

Figure 2: Cryptanalysis and Security Analysis of Cryptographic methodology

Security research looks at how secure the protocols are generally, taking into account things like data privacy, stability, validity, and resistance to different cryptographic threats. To do this, the cryptographic primitives used in the protocols, like encryption methods, digital signatures, and key exchange mechanisms, must be checked for their power. It is also checked to see how resistant the protocols are to side-channel attacks, coding problems, and protocol-level weaknesses in the real world. For example, side-channel attacks take advantage of information leaks that happen unintentionally when cryptography methods are implemented physically, like changes in time or patterns of power use. When figuring out the general security situation, one thing that is looked at is how well the policies protect data privacy, making sure that private data stays safe from people who shouldn't have access to it (see figure 2). Data integrity makes sure that the data being sent stays the same and doesn't get changed while it's being sent, and validity checks that the people who are talking are who they say they are and that the messages they send are correct. For the protocols to be safe in hostile settings, they must also be able to withstand different types of cryptographic attacks, like chosen-ciphertext attacks, repeat attacks, and man-in-the-middle attacks. It is important to do a thorough cryptanalysis and security analysis of the encryption protocols shown in Figure 2 in order to find possible security holes, check how well they protect against quantum threats, and get a sense of their general security. Researchers can make strong secure solutions that protect against new threats, like those faced by quantum computing technologies, by carefully studying the protocols' security features and how well they stand up to different types of attacks.

Cryptanalysis and Security Analysis of Cryptographic Protocols is as follows

Step 1: Decompose Protocol:

- Split the protocol into its components: key exchange, encryption, signatures, and authentication.

Step 2: Identify Assumptions:

- Determine underlying assumptions (e.g., hardness of SVP for lattice-based schemes).

$$\text{Assumption}_1\text{:Hardness of SVP}$$

Step 3: Formulate Adversarial Model:

- Define capabilities and goals of potential adversaries, including classical and quantum attackers.

$$\text{Adversarial Model}=\{\text{Classical Adversary},\text{Quantum Adversary}\}\ldots\ldots (1)$$

Step 4: Cryptanalysis:

- Analyze security proofs and assumptions for vulnerabilities.

- Explore attack vectors (e.g., brute force, chosen-plaintext attacks).

$$\text{Vulnerability}_i=f\,(\text{Protocol},\text{Attack}_i)\ldots\ldots\ldots (2)$$

Step 5: Quantum Attack Evaluation:

- Assess resilience against quantum attacks using algorithms like Shor's and Grover's.

Step 6: Security Analysis:

- Evaluate overall security, considering data confidentiality, integrity, and resistance to attacks.

$$\text{Security}_i=h(\text{Protocol},\text{Attack}_i)\ldots\ldots\ldots\ldots (3)$$

4. Integration and Deployment:

Integrating and deploying newly created secure protocols are important steps to make sure they work well and are widely used in current platforms and systems. Several important steps are involved in this process that are meant to make post-quantum encryption solutions more compatible, interoperable, standardized, and widely used. First, attempts to integrate new security protocols focus on making sure that they work with current systems and platforms' design, protocols, and interfaces so that they can be added without any problems. This could mean changing the standards to work with different computer languages, tools, and operating systems so that they can be easily integrated without affecting how things work now. Testing for compatibility makes sure that the built-in protocols work properly on the intended systems and platforms, figuring out and fixing any problems or conflicts that may come up.

Second, the goal of implementation efforts is to get important organizations and industry players to standardize and use post-quantum encryption solutions. By taking part in industry meetings, standardization bodies, and consortiums, you can push for the use of standardized cryptographic methods and protocols. For consensus-driven norms and recommendations for post-quantum security to be made, academics, business partners, and government agencies must work together. By setting up standard protocols, businesses can make sure that different systems and platforms can work together securely and interoperate. This builds trust in post-quantum cryptography solutions. Help and advice are given to make the change to post-quantum security solutions easier, such as transfer strategies and best practices. This means giving people teaching materials, training programs, and classes to help them learn more about how quantum computing affects safety and why we need to switch to cryptographic solutions that are not affected by quantum computing. There is useful information on how to choose, set up, and use post-quantum security algorithms based on the needs and use cases of each company. Additionally, transfer plans are created to help businesses smoothly switch from older cryptographic systems to post-quantum cryptographic solutions. Some of the things that might be used are staged transfer, backward compatibility measures, and risk reduction strategies to keep operations running smoothly during the change time and cause as little trouble as possible. Integration and implementation activities are very important for getting post-quantum security solutions used because they make sure that they are compatible, can work with other systems, are standardized, and have good transfer plans. Organizations can successfully combine, install, and move to quantum-resistant secure solutions by working with the right people and giving them advice and support. This improves safety and lowers the risks that come with quantum computing advances.

4.RESULT AND DISCUSSION

The protocol representation, shown in figure 1, that shows how well different encryption methods, especially Shor's algorithm and Grover's algorithm, protect against quantum attacks. There are two bars for each protocol, such as Key Exchange, Encryption, Digital Signature, and Authentication. One bar shows how resistant it is to Shor's algorithm, and the other shows how resistant it is to Grover's algorithm. The amount of resistance is shown by the height of each bar. Higher bars mean that quantum strikes are less likely to succeed. The graph displays how well the different cryptographic methods protect against quantum risks on a visual level. The data shows that all methods are pretty strong against both Shor's and Grover's algorithms, though the amounts of strength vary slightly. This kind of visual picture makes it easier to see how strong different cryptographic methods are in comparison to quantum computing, which helps people choose and use strong security measures for digital interactions.

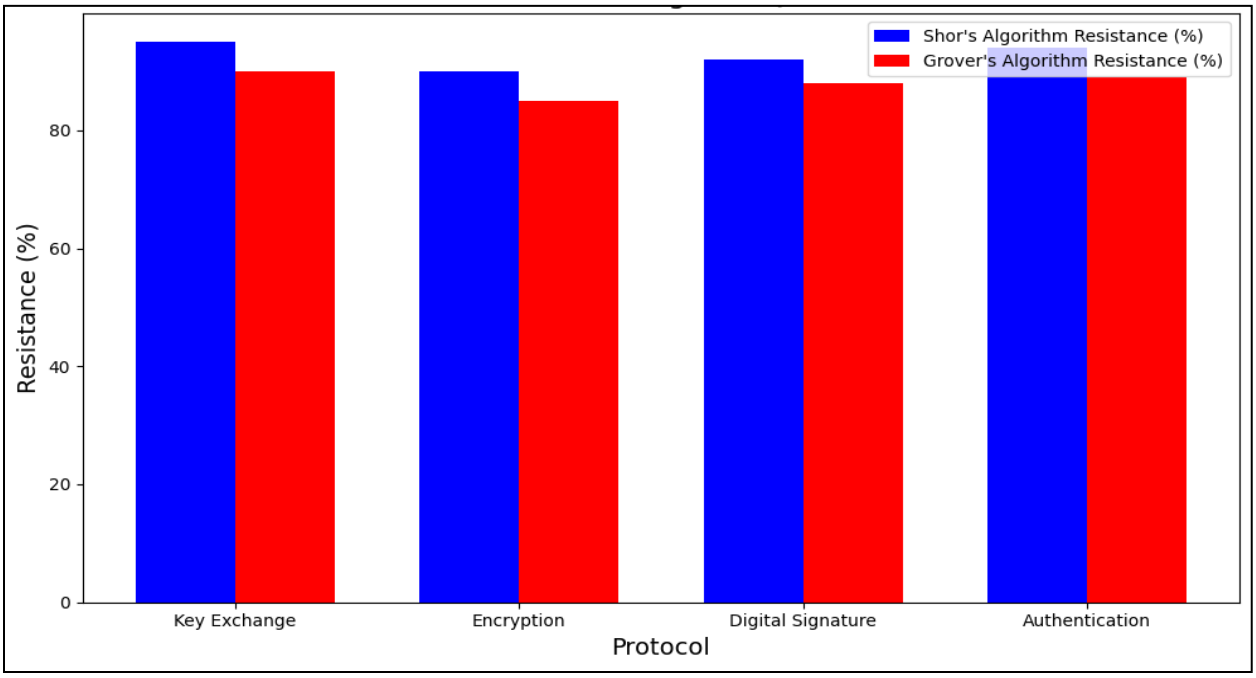

Figure 3: Representation of resistance of protocol against Quantum Attacks

The numbers in table (2) show how well different encryption methods, especially Shor's algorithm and Grover's algorithm, protect against quantum threats. By taking advantage of the speed and power of quantum computers, these two quantum algorithms are very dangerous to traditional encryption methods. Key sharing methods are very important for setting up safe communication routes. Shor's algorithm has a very high level of resistance, with a possible resistance level of 95%. This means that the protocol's key sharing method is strong and can't be broken by quantum threats. This gives users a high level of security. But the resistance to Grover's method is a little lower, at 90%. This shows that we need to add more security steps to protect against symmetric-key attacks.

Table 2: Resistance of various cryptographic protocols against quantum attacks

bvgfccdsfgroups, and academics work together. This will also protect digital systems from quantum computing's destructive potential. To put it simply, the progress made in post-quantum cryptography is a major step toward making digital interactions safer in the quantum age. We can deal with the problems that quantum computing brings about and start a new era of safe and reliable cryptographic protocols if we welcome these advances and encourage people to work together.

REFERENCES

[1] V.-L. Nguyen et al., "Security and privacy for 6g: A survey on prospective technologies and challenges", IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2384-2428, 2021.

[2] W. Beullens, "Breaking rainbow takes a weekend on a laptop", Advances in Cryptology, pp. 464-479, 2022.

[3] G. Alagic et al., Status report on the third round of the NIST postquantum cryptography standardization process, Jul. 2022.

[4] J. Bos et al., "CRYSTALS - kyber: A CCA-secure module-lattice-based KEM", 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 353-367, 2018.

[5] Y. Cao et al., "The evolution of quantum key distribution networks: On the road to the qinternet", IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839-894, 2022.

[6] C. Stan et al., "Securing communication with quantum key distribution: Implications and impact on network performance", Advanced Photonics Congress (SPPCom), pp. SpW2J.2, 2022.

[7] R. T. Hadke and P. Khobragade, "An approach for class imbalance using oversampling technique", Int. J. Innov. Res. Comput. Commun. Eng., vol. 3, no. 11, pp. 11451-11455, 2015.

[8] D. Sikeridis, P. Kampanakis and M. Devetsikiotis, "Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH", Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies, pp. 149-156, 2020.

[9] G. Tasopoulos et al., "Performance evaluation of post-quantum tls 1.3 on resource-constrained embedded systems", Information Security Practice and Experience, pp. 432-451, 2022.

[10] B. Dowling, T. B. Hansen and K. G. Paterson, "Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange", Post-Quantum Cryptography: 11th International Conference PQCrypto 2020, pp. 483-502, 2020.

[11] L. Huang, K. Feng and C. Xie, "A practical hybrid quantum-safe cryptographic scheme between data centers", Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro-and Nanosystems in Security and Defence III, vol. 11540, pp. 30-35, 2020.

[12] Quantum key distribution (QKD); Protocol and data format of REST-based key delivery API, feb 2019.

[13] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", 2020

[14] Kumari, S.; Singh, M.; Singh, R.; Tewari, H. Signature based Merkle Hash Multiplication algorithm to secure the communication in IoT devices. Knowl.-Based Syst. 2022, 253, 109543.

[15] Nejatollahi, H.; Dutt, N.; Ray, S.; Regazzoni, F.; Banerjee, I.; Cammarota, R. Post-quantum lattice-based cryptography implementations: A survey. ACM Comput. Surv. 2019, 51, 1–41.

[16] Kuang, R.; Perepechaenko, M.; Barbeau, M. A new post-quantum multivariate polynomial public key encapsulation algorithm. Quantum Inf. Process. 2022, 21, 360. [

[17] Mitra, S.; Samanwita, D.; Malay, K. Prevention of the man-in-the-middle attack on Diffie–Hellman key exchange algorithm: A review. In Proceedings of International Conference on Frontiers in Computing and Systems: COMSYS 2020; Springer: Singapore, 2021.

[18] Harkanson, R.; Kim, Y. Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications. In Proceedings of the 12th Annual Conference on Cyber and Information Security Research, Oak Ridge, TN, USA, 4–6 April 2017; ACM: New York, NY, USA, 2017.

[19] Jao, D.; De Feo, L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Post-Quantum Cryptography, Proceedings of the 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, 29 November–2 December 2011; Proceedings 4. Springer: Berlin/Heidelberg, Germany, 2011; pp. 19–34.

[20] Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Miller, C.; Moody, D.; Peralta, R.; et al. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process; US Department of Commerce, NIST: Gaithersburg, MD, USA, 2022.

[21] Zhang, Q. An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption. In Proceedings of the 2021 2nd International Conference on Computing and Data Science (CDS), Stanford, CA, USA, 28–29 January 2021; pp. 616–622.

[22] Rudnytskyi, V.; Korchenko, O.; Lada, N.; Ziubina, R.; Wieclaw, L.; Hamera, L. Cryptographic encoding in modern symmetric and asymmetric encryption. Procedia Comput. Sci. 2022, 207, 54–63.

[23] Rajawat, A. S., Goyal, S. B., Solanki, R. K., Gadekar, A., & Patil, D. (2024). Dark Web Financial Fraud Identification Using Mathematical Models in Healthcare Domain. JOIV: International Journal on Informatics Visualization, 8(1), 107-114.

[24] Nemade, B., Mishra, R., Jangid, P., Dubal, S., Bharadi, V., & Kaul, V. (2023). Improving Rainfall Prediction Accuracy Using an LSTM-Driven Model Enhanced by M-PSO Optimization. Journal of Electrical Systems, 19(3).

[25] Mishra, R., Nemade, B., Shah, K., & Jangid, P. (2023). Improved Inductive Learning Approach-5 (IILA-5) in Distributed System. International Journal of Intelligent Systems and Applications in Engineering, 11(10s), 942-953.

[26] Gulhane, M., Kumar, S., & Borkar, P. (2023, November). An Empirical Analysis of Machine Learning Models with Performance Comparison and Insights for Heart Disease Prediction. In 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS) (pp. 374-381). IEEE.

[27] Goyal, Dinesh , Kumar, Anil , Gandhi, Yatin & Khetani, Vinit (2024) Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols, Journal of Discrete Mathematical Sciences and Cryptography, 27:2-B, 703–714, DOI: 10.47974/JDMSC-1921