



Quantum Computing: A Threat to Cryptography

Lavanyan T¹, Selvi S²

¹III-B.Sc., Computer Science - 'B', PSG College of Arts & Science, Coimbatore-14

² Associate Professor, Department of Computer Science, PSG College of Arts & Science, Coimbatore-14

ABSTRACT:

Quantum computing is poised to revolutionize the world of computational science, introducing unparalleled processing capabilities. However, this technological leap poses significant challenges to modern cryptographic practices. Many encryption methods that currently secure global communications are vulnerable to attacks by quantum algorithms. This paper examines the nature of quantum computing, its impact on cryptographic systems, and the ongoing development of quantum-resistant cryptographic methods to counteract this emerging threat.

Keywords: Quantum Computing, Cryptography threats, Cybersecurity solutions, Quantum Algorithms.

1. Introduction:

The advent of the digital age has made cryptography an essential tool for securing communications, financial transactions, and sensitive data. Current cryptographic systems depend heavily on mathematical problems that are computationally difficult for classical computers to solve. Quantum computers use their quantum bits, also known as "Qubits," to store and manipulate the information, in contrast to traditional classical computers, which are based on conventional computing and utilize binary bits 0 and 1 separately. Quantum computing[1], with its ability to perform certain calculations exponentially faster than classical machines, threatens to upend these systems. This journal explores the implications of quantum computing and highlighting the cryptography[2,4,6] vulnerabilities and gives potential solutions for threat protection.

2. Understanding Quantum Computing:

Quantum computers operate based on principles of quantum mechanics, such as superposition, entanglement, and quantum interference. Unlike classical bits that exist as either 0 or 1, quantum bits (qubits) can represent 0, 1, or both simultaneously through superposition. This capability allows quantum computers to perform multiple calculations at once, vastly increasing their computational power for specific problems. Quantum entanglement, another unique feature, enables qubits to interact in ways that significantly enhance processing capabilities, which are able to finish the computations[3] with the problems that would take years by the super computer at present.

2.1 Quantum Algorithms

Quantum computing's[7,9] potential impact on cryptography[8] stems from algorithms that exploit its unique properties and here are some of the important Quantum algorithms that are given below:

2.1.1 Shor's Algorithm

Shor's Algorithm was proposed by Peter Shor in 1994, this algorithm is a cornerstone of quantum computing's threat to cryptography. It efficiently factors large integers and computes discrete logarithms, both of which underpin the security of public-key cryptosystems such as RSA, DSA, and ECC. Shor's Algorithm operates exponentially faster than the best-known classical algorithms for these tasks, enabling the decryption of encrypted data protected by these methods once large-scale quantum computers are available.

Classical background: The difficulty of factoring large integers underpins the security of many cryptographic systems. Classical algorithms like trial division, Pollard's rho algorithm, or the quadratic sieve grow exponentially in complexity with the size of N, making them impractical for very large numbers. Shor's algorithm leverages the unique properties of quantum mechanics to solve this problem efficiently.

Quantum Insights:

The efficiency of Shor's algorithm arises from its use of **quantum parallelism** and **period finding**, which is the core computational task.

Period Finding Problem

Given a function $f(x) = a^x \bmod N$ (where a is a randomly chosen integer coprime to N), the algorithm aims to find the period r of $f(x)$, i.e., the smallest positive integer such that:

$$f(x+r) = f(x) \text{ for all } x.$$

Once the period r is found, it is possible to compute the factors of N .

Implications:

Shor's algorithm poses a significant threat to classical public-key cryptosystems like RSA, which rely on the assumption that factoring large integers is computationally infeasible. A sufficiently powerful quantum computer could break RSA encryption in a matter of seconds.

2.1.2 Grover's Algorithm

Grover's Algorithm was developed by Lov Grover in 1996, this algorithm enhances brute-force search capabilities by providing a quadratic speedup. While it does not completely compromise symmetric cryptography [10,11], it effectively reduces the security of symmetric key algorithms, such as AES and DES, by halving the key length required to maintain the same level of security.

For example, an AES-128 system would have an effective security level equivalent to AES-64 against Grover's Algorithm.

Steps in Grover's Algorithm

[1] Initialization:

- a. Prepare an n -qubit register (where $N=2^n$) in the $|0\rangle$ state.
- b. Apply the Hadamard transform to create a uniform superposition.

[2] Grover Iteration (repeated $O(\sqrt{N})$ times):

- a. Apply the oracle to mark the solution states.
- b. Apply the diffusion operator to amplify the probability of the solution states.

[3] Measurement: After sufficient iterations, measure the quantum state to obtain the target solution with high probability.

2.1.3 Quantum Fourier Transform (QFT)

The Quantum Fourier Transform (QFT) is a crucial algorithm in quantum computing, providing a quantum equivalent of the classical discrete Fourier transform (DFT). It plays a key role in many quantum algorithms, such as Shor's algorithm for factoring and solving the discrete logarithm problem.

The QFT maps a quantum state from the computational basis to a superposition state in the Fourier basis. Given an n -qubit input state $|x\rangle$, the QFT transforms it into a quantum state $|\psi\rangle$. This transformation is the quantum analog of the discrete Fourier transform, which is widely used in signal processing. The QFT follows a circuit methodology which typically involves:

- a. Hadamard Gates (H): These initialize superpositions for each qubit.
- b. Controlled Phase Gates: These introduce relative phase shifts between qubits based on their binary representations.
- c. Swaps (optional): To reverse the order of qubits if required, as the QFT output is in bit-reversed order. For a 3-qubit system, the circuit diagram would look like this:
 - a. Apply a Hadamard gate to the first qubit.
 - b. Apply controlled-phase gates to entangle the first qubit with others.
 - c. Repeat for the remaining qubits, applying Hadamard gates and controlled-phase gates sequentially.
 - d. Optionally, reverse the qubit order at the end.

2.1.4 Variational Quantum Algorithms

Variational Quantum Algorithms (VQAs) are hybrid quantum-classical algorithms designed to leverage the strengths of both quantum and classical computing. They are particularly promising for solving complex optimization problems, simulating quantum systems, and tackling machine learning tasks on near-term quantum devices, which are characterized by limited qubits and noise. This includes algorithms, such as the Variational Quantum Eigensolver (VQE) and Quantum Approximate Optimization Algorithm (QAOA), leverage the hybrid capabilities of quantum and classical computing.

i. Variational Quantum Eigensolver (VQE):

The Variational Quantum Eigensolver (VQE) is a hybrid quantum-classical algorithm designed to approximate the ground state energy of a quantum system. It is particularly useful for problems in quantum chemistry and materials science.

ii. **Quantum Approximate Optimization Algorithm (QAOA):**

The Quantum Approximate Optimization Algorithm (QAOA) is a variational algorithm designed to solve combinatorial optimization problems by mapping them onto a quantum system.

Both VQE and QAOA showcase the versatility of variational algorithms, while not specifically designed for cryptanalysis, they have potential applications in optimization problems related to cryptography each tailored to distinct problem domains.

2.1.5 Quantum Annealing

Quantum annealing is a heuristic approach used to solve combinatorial optimization problems. It works by finding the minimum energy configuration of a system, represented as a mathematical optimization problem, using principles of quantum mechanics. Though not as universally powerful as gate-based quantum algorithms, quantum annealing has been explored for cryptographic applications such as solving [12] constraint satisfaction problems and hash function inversions.

The Quantum Annealing works following the steps such as, formulating the problem, encoding the problem, initialization (starting state), adiabatic evolution, Quantum Tunneling, final state (solution).

Quantum annealing is implemented in hardware by companies like **D-Wave Systems**, which designs quantum processors specifically for annealing. While not universal quantum computers, these devices are effective for specific optimization problems.

3. Cryptography in the Face of Quantum Computing:

3.1 Public-Key Cryptography:

- a. Public key cryptography[7], also known as asymmetric cryptography, uses a pair of keys: a public key and a private key. The public key is shared openly and can be used by anyone to encrypt data, while the private key is kept secret and is used to decrypt the data. This approach enables secure communication over insecure channels and underpins many protocols used in internet security, such as SSL/TLS and digital signatures.
- b. For example, in RSA (Rivest-Shamir-Adleman), a popular public key cryptography algorithm, the security relies on the difficulty of factoring large numbers. If someone wants to send a secure message, they encrypt it using the recipient's public key. Only the recipient, who possesses the private key, can decrypt the message. Similarly, in Elliptic Curve Cryptography [10,14](ECC), security is based on the difficulty of solving the elliptic curve discrete logarithm problem, making it more efficient than RSA for smaller key sizes.
- c. However, quantum computers running Shor's algorithm can efficiently factor large numbers or solve discrete logarithm problems, effectively breaking RSA and ECC. For example, a sufficiently powerful quantum computer could decrypt an RSA-encrypted message by factorizing its public modulus into its prime factors.

3.2 Symmetric Cryptography:

- a. Symmetric cryptography uses a single key for both encryption and decryption. It is widely used for secure data transmission and storage due to its simplicity and efficiency. Examples of symmetric encryption algorithms include the Advanced Encryption Standard (AES), Data Encryption Standard (DES), and ChaCha20.
- b. A real-world example of symmetric cryptography is the use of AES in securing Wi-Fi networks (WPA2 and WPA3 protocols). In financial systems, ChaCha20 is often used for securing online transactions due to its speed and reliability.
- c. Unlike public key cryptography, symmetric cryptography is considered more resistant to quantum attacks. While Grover's algorithm can theoretically reduce the effective key length by half, increasing the key size can mitigate this threat. For instance, AES-128 (providing 128 bits of security)[10] could be effectively reduced to 64 bits of security under Grover's attack. Transitioning to AES-256 would ensure quantum resilience by maintaining an effective security level of 128 bits.

3.3 Hash Functions:

- i. Hash functions are cryptographic algorithms that transform input data of arbitrary size into a fixed-size output, called a hash or digest. These

functions are designed to be fast, deterministic, and collision-resistant, meaning it should be computationally infeasible to find two different inputs that produce the same hash. Hash functions are widely used in digital signatures, password storage, and data integrity checks.

ii. For instance, SHA-256, part of the Secure Hash Algorithm (SHA) family, is commonly used in blockchain technology. Bitcoin uses SHA-256 for mining and transaction validation. If quantum computers achieve practical application, Grover's algorithm could weaken SHA-256 by speeding up the search for collisions. Similarly, systems storing passwords hashed with MD5 or SHA-1 (already deemed weak due to classical collision attacks) would face even greater risks.

- iii. To counteract this, transitioning to hash functions with larger output sizes, such as SHA-3 or Blake2, is essential. For example, moving from

SHA-256 to SHA-512 would double the output size and increase quantum resistance.

The rise of quantum computing is both a challenge and an opportunity. By proactively adopting quantum-resistant technologies, we can safeguard digital systems against the threats posed by this transformative technology.

4. Post-Quantum Cryptography:

To address these challenges, researchers are developing cryptographic algorithms resistant to quantum attacks, collectively known as post-quantum cryptography. These methods rely on mathematical problems not susceptible to known quantum algorithms. Prominent approaches include:

- **Lattice-Based Cryptography**

Lattice-based cryptography is an area of cryptographic research that leverages the hardness of problems related to lattice structures in mathematics. A lattice is a regular arrangement of points in space, typically described as the set of all integer linear combinations of a set of basis vectors. The difficulty of solving certain problems in lattice theory forms the foundation for various cryptographic schemes, many of which are believed to be secure against attacks from quantum computers.

A lattice is a discrete set of points in n -dimensional space, defined by a set of basis vectors. The important problems in lattice-based cryptography are often based on the difficulty of solving problems involving these lattices. Some of the central problems include:

- i. **Shortest Vector Problem (SVP):** Finding the shortest non-zero vector in a lattice.
- ii. **Closest Vector Problem (CVP):** Finding the closest vector to a given target point in the lattice.
- iii. **Learning With Errors (LWE):** A problem where the goal is to solve a system of linear equations, but with small random noise added to the equations. LWE is believed to be hard even for quantum computers.

These problems are computationally intensive even for quantum computers making lattice-based cryptography a promising alternative to traditional cryptography [17,18], which may be vulnerable to quantum attacks. Algorithms like NTRUEncrypt and Kyber exemplify lattice-based cryptography, offering both encryption and key exchange capabilities.

- **Code-Based Cryptography**

Code-based cryptography utilizes the difficulty of decoding random linear codes. These codes are mathematical objects that are widely used in error-correcting codes, which are designed to detect and correct errors in data transmission. In code-based cryptography, the security of the system relies on the difficulty of decoding a general linear code, a problem that is believed to be hard even for quantum computers.

The Goppa code is one of the most commonly used families of codes in code-based cryptography. The Decoding Problem for Goppa Codes is known to be hard to solve efficiently, even with access to powerful computational resources, which makes it a strong candidate for cryptographic applications.

Code-Based Cryptographic Schemes:

Code-based cryptography has been primarily used for **public key encryption** and **digital signatures**. Some of the most well-known schemes are:

i. McEliece Public Key Encryption (1978): The McEliece cryptosystem is one of the earliest and most well-known code-based encryption schemes. It is based on the hardness of decoding a general linear code, and the scheme uses a large binary Goppa code.

- a. In McEliece, the public key consists of an encoding of a Goppa code, and the private key is used for decoding. The system is resistant to quantum attacks because the decoding problem is hard even for quantum computers.
- b. Despite McEliece's security, its public key size is relatively large, which has been a practical concern. However, it remains one of the promising candidates for post-quantum cryptography.

- [2] **Niederreiter Cryptosystem (1986):** The Niederreiter cryptosystem is closely related to McEliece but uses a different structure for the public key. It is based on the syndrome decoding problem, which is also believed to be hard to solve. The Niederreiter system is a variant of McEliece and is also quantum-resistant.
- [3] **Code-Based Digital Signatures:** Code-based cryptography also supports digital signature schemes, such as the Tcheremynski-Karlin and BLISS (Bimodal Lattice Signature Scheme). These signature schemes provide strong security guarantees and are designed to be resistant to quantum computer attacks.
- [4] **Code-Based Key Exchange Protocols:** Some research has focused on creating key exchange protocols based on code-based cryptography. These protocols allow two parties to securely exchange keys using error-correcting codes.

Multivariate Cryptography

Multivariate Public Key Cryptography is a class of cryptographic systems that are based on multivariate polynomial equations over finite fields. These cryptographic schemes use the hardness of solving systems of multivariate polynomial equations as their security foundation. Multivariate cryptography is one of the promising candidates for post-quantum cryptography because the underlying problems are believed to be difficult even for quantum computers.

In multivariate cryptography, the security of the cryptographic system is based on the computational difficulty of solving a system of multivariate polynomial equations. The basic idea is to create a set of polynomial equations with several variables, and the challenge is to solve for the variables given a set of equations, which is computationally hard.

The polynomial equations are typically defined over finite fields (i.e., sets of numbers with a finite number of elements), and the system is designed in such a way that finding the solutions to these equations is hard for classical and quantum computers.

Hash-Based Cryptography

Hash-based cryptography refers to cryptographic systems that rely on hash functions to provide security. These systems are typically used in digital signatures and message authentication codes (MACs). Hash-based cryptographic schemes are particularly attractive for post-quantum cryptography, as they are based on hash functions, which are believed to remain secure even in the presence of quantum computers.

Hash-Based Cryptographic Systems:

The main cryptographic applications of hash functions are in digital signatures and public key authentication. In hash-based cryptography, security is often derived from the difficulty of finding collisions in hash functions or exploiting weaknesses in the construction of hash-based systems.

Two key areas where hash functions play a central role in cryptography are:

Digital Signatures: Hash-based digital signatures use a cryptographic hash function to sign a message. The message is first hashed, and the signature is applied to the hash of the message. This allows for the verification of both the integrity of the message and the authenticity of the signature.

Message Authentication Codes (MACs): A MAC is used to ensure the integrity and authenticity of a message. It typically involves combining a cryptographic hash function with a secret key to produce a MAC. The receiver, who knows the secret key, can use the hash function to verify that the message has not been tampered with.

Hash-Based Signature Schemes:

One of the most significant areas of hash-based cryptography is hash-based digital signature schemes. These schemes use hash functions and rely on the difficulty of finding collisions to provide secure, efficient signatures.

- i. **Merkle Signature Scheme (MSS):** The Merkle Signature Scheme (MSS) is a family of hash-based signature schemes based on Merkle trees. Merkle trees are binary trees where each leaf node represents the hash of a message, and each internal node is the hash of its child nodes. The root of the Merkle tree is a compact representation of all the messages.
- ii. **XMSS (eXtended Merkle Signature Scheme):** XMSS is an improvement over the Merkle Signature Scheme and provides stateful hash-based signatures. It uses a sequence of hash-based signatures, with each signature being based on a different set of hash functions. XMSS is designed to be secure and efficient, especially for systems that need to handle large numbers of signatures.
- iii. **LMS (Leighton-Micali Signature Scheme):** LMS is another hash-based digital signature scheme that uses a tree of hash functions for efficient signature generation and verification. It is particularly designed for high security and is used in environments where large-scale signing is needed, such as blockchain and distributed ledgers.
- iv. **SPHINCS+ (Stateless Practical Hash-based Signatures):** SPHINCS+ is a stateful and stateless hybrid signature scheme that offers quantum-resilience by relying entirely on hash functions. Unlike the traditional RSA and ECC-based schemes, SPHINCS+ uses a tree structure and combines several hash-based schemes into one, ensuring that a break in one scheme does not compromise the entire system.

Hash-based signature schemes are quantum-resistant because they rely on the security of hash functions, which are not vulnerable to quantum algorithms like Shor's algorithm (which breaks RSA and ECC). Since no efficient quantum algorithm is known for finding collisions in cryptographically secure hash functions, hash-based cryptography offers a strong foundation for post-quantum cryptography.

Isogeny-Based Cryptography

Isogeny-based cryptography is a branch of cryptography that uses the mathematical concept of isogenies between elliptic curves as the foundation for cryptographic protocols. An isogeny is a special type of mathematical map between elliptic curves that preserves the group structure of the curves. The security of isogeny-based cryptographic systems is based on the hardness of finding an isogeny between two given elliptic curves, a problem that is believed to be difficult, even for quantum computers.

Isogeny-based cryptography has gained significant attention in the post-quantum cryptography field due to its potential resistance to attacks by quantum computers. The main advantage of isogeny-based systems is that they rely on the algebraic structure of elliptic curves and isogenies, which are not affected by Shor's algorithm (the quantum algorithm that efficiently solves integer factorization and discrete logarithm problems).

Isogeny-Based Cryptographic Systems:

Isogeny-based cryptography has led to the development of several cryptographic protocols, with key exchange and digital signatures being two of the main applications.

Supersingular Isogeny Diffie-Hellman (SIDH): The Supersingular Isogeny Diffie-Hellman (SIDH) protocol is a key exchange protocol

based on supersingular elliptic curves and isogenies between them. It is one of the most well-known cryptographic protocols based on isogenies and is designed to be secure against quantum computers.

Supersingular Isogeny Key Exchange (SIKE): SIKE is a key exchange protocol based on SIDH but optimized for practical implementation. It is a post-quantum cryptographic protocol designed for secure communication in the presence of quantum adversaries.

Isogeny-Based Digital Signatures: While key exchange protocols like SIDH and SIKE are more widely studied, researchers have also explored isogeny-based digital signature schemes. These schemes aim to create secure signatures using isogenies between elliptic curves.

• NIST Standardization Efforts

The National Institute of Standards and Technology (NIST) has been spearheading efforts to standardize post-quantum cryptographic algorithms. In its ongoing competition, several candidate algorithms have advanced to the final stages, including Kyber (lattice-based), Dilithium (lattice-based), and SPHINCS+ (hash-based). These algorithms are being evaluated for their security, efficiency, and implementation feasibility.

Challenges in Transition to Quantum-Resilient Cryptography:

The challenges in shift to post-quantum cryptography presents several obstacles that are given below:

I. Scalability:

Many quantum-resistant algorithms require more computational resources, potentially slowing down existing systems. For example, lattice-based cryptography often demands greater storage for keys and ciphertext, which can strain devices with limited memory.

II. Interoperability:

Ensuring that new cryptographic standards integrate seamlessly with legacy systems is a daunting task. Organizations relying on older encryption systems may face compatibility issues, necessitating extensive software and hardware upgrades.

III. Adoption Timeline:

Encouraging organizations to adopt quantum-resistant solutions before large-scale quantum computers become practical is a race against time. Many enterprises may delay transitions due to the high costs and perceived complexity of implementation, leaving systems vulnerable.

IV. Global Coordination:

Facilitating international cooperation to establish consistent standards and practices is essential. The absence of unified guidelines could lead to fragmented security protocols, increasing vulnerabilities across interconnected systems.

V. Testing and Validation:

New algorithms must undergo rigorous testing to ensure they are resistant not only to quantum attacks but also to classical vulnerabilities. Ensuring thorough validation across diverse environments can be resource-intensive and time-consuming.

VI. Economic and Organizational Resistance:

Transitioning to post-quantum cryptography involves significant investment in new infrastructure and training. Small and medium-sized enterprises, in particular, may lack the resources to prioritize such upgrades, leaving a gap in global readiness.

5. Strategic Directions for Quantum-Safe Cryptographic Systems:

The rise of quantum computing necessitates proactive measures to safeguard data security. Governments, industries, and academic institutions must collaborate to:

Accelerate Research and Development:

Advancements in hardware and software tools for post-quantum cryptography can expedite the creation of more efficient algorithms. For example, exploring hybrid systems that combine classical and quantum-resistant methods can provide interim solutions during the transition period.

Implement Layered Security Approaches:

Organizations can adopt multi-layered security strategies that combine quantum-resistant algorithms with existing protocols. This redundancy ensures continued protection even if one layer is compromised.

Invest in Infrastructure:

Governments and private entities must allocate resources for the development of scalable, cost-effective solutions that are accessible to businesses of all sizes. Cloud-based platforms offering post-quantum cryptographic services could reduce the barriers to adoption.

Encourage Standardization and Collaboration:

International bodies like NIST and ISO should intensify efforts to standardize algorithms and protocols. Unified standards enable global interoperability and reduce the risks associated with fragmented implementations.

Pilot Programs and Early Adoption Initiatives:

Large organizations and government agencies can lead by example, implementing post-quantum cryptography in critical systems. These pilot programs can provide valuable insights and best practices for broader adoption.

Monitor Quantum Computing Progress:

Establishing dedicated task forces to track advancements in quantum computing ensures preparedness. Early detection of breakthroughs in quantum hardware can guide timely updates to cryptographic strategies.

6. Conclusion:

Quantum computing is both a technological marvel and a formidable challenge to the security of modern cryptographic systems. While quantum algorithms like Shor's and Grover's expose vulnerabilities in current encryption methods, the development of post-quantum cryptography provides a pathway to secure the digital world against this emerging threat. Proactive adoption of quantum-resistant algorithms is essential to ensuring the integrity of global communications in the quantum era.

REFERENCES:

- [1] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
- [2] [S. Selvi](#) & [M. Gobi](#) , Hyper Elliptic Curve Based Homomorphic Encryption Scheme for Cloud Data Security, International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018(ICICI 2018) -6
- [3] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography: The case for large-scale preparedness. Communications of the ACM, 60(2), 70-79.
- [4] S. Selvi, "An efficient hybrid cryptography model for cloud data security," International Journal of Computer Science and Information Security (IJCSIS), vol. 15, no. 5, 2017
- [5] Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
- [6] S. Selvi, and R. Ganesan, "A Secured Cloud System using Hyper Elliptic Curve Cryptography", International Journal of Scientific & Engineering Research, Vol. 6, No.1, 2015
- [7] Foundational textbook explaining quantum mechanics principles for computation. Arute, F., et al. (2019). "Quantum supremacy using a programmable superconducting processor." *Nature*, 574(7779), 505-510.
- [8] Selvi, S., and R. Sridevi. "Efficient Scheduling Mechanisms for Secured Cloud Data Environment.", International Journal of Recent Technology and Engineering (IJRTE), 8, Issue-2S11, 2019

-
- [9] Landmark paper demonstrating quantum supremacy with Google's Sycamore processor. Preskill, J. (2018). "Quantum computing in the NISQ era and beyond." *Quantum*, 2, 79.
- [10] S.Selvi, M.Gobi , 'Improving Cloud Data Security using Hyper Elliptical Curve Cryptography & Steganography' International Journal for Scientific Research & Development| Vol. 5, Issue 04, 2017 | ISSN (online):2321-0613.
- [11] Discusses the challenges and potential of noisy intermediate-scale quantum (NISQ) devices. Peikert, C. (2016). "A decade of lattice cryptography." *Foundations and Trends® in Theoretical Computer Science*, 10(4), 283-424.
- [12] Reviews lattice-based cryptography extensively, a leading candidate for post-quantum systems. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). "Post-quantum key exchange—A new hope." *Proceedings of the 25th USENIX Security Symposium*.
- [13] Introduces "NewHope," a lattice-based key exchange protocol for quantum resistance. Mosca, M. (2018). "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security & Privacy*, 16(5), 38-41.
- [14] Examines quantum computing's potential impact on blockchain technologies and cryptocurrencies. National Security Agency (NSA). (2022). *Quantum Computing and the Cryptographic Transition*.
- [15] S. Selvi, K. Aggarwal, R. Pandurangan, V. P. Vijayan, A. Ali and K. Anuradha, "Enhancing the accuracy of target detection in remote video surveillance analytics through federated learning", *Opt. Quantum Electron.*, vol. 56, no. 2, pp. 185, 2024.
- [16] R. Hemalatha and S. Selvi, "Improving security of visual cryptography by contrast sensitivity function", *Vidyabharati International Interdisciplinary Research Journal*, Special Issue on Recent Research Trends in Management, Science and Technology, pp. 1322-1330, 2021
- [17] Progressing Biometric Security Concern with Blowfish Algorithm R.Sridevi, S.Selvi , *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* ISSN: 2278-3075, Volume-8, Issue- 9S2, July 2019
- [18] Hemalatha Rangaswamy, Selvi Sellappan , "Robust Collusion Avoidance-Secure Signific VC Scheme", *International Journal of Intelligent Engineering & Systems*, 2022