ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 12, Issue 2, March- April 2025

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.028

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 2, March- April 2025 |

Quantum Cryptography for Securing Wireless Communication in 6G Networks

Mrs, R.Karthika[1], V.Dharun[2], V.R.Ramprakash[3]

Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[1]

U.G Student, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[2]

U.G Student, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India[3]

ABSTRACT: The development of 6G networks introduces unprecedented advancements in wireless communication, including ultra-reliable low-latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC). However, the security of these networks is a critical challenge, particularly with the advent of quantum computing. Traditional cryptographic mechanisms such as RSA, ECC, and Diffie-Hellman key exchange are at risk due to the ability of quantum computers to break their mathematical foundations using Shor's algorithm. As a result, quantum cryptography has emerged as a promising solution to counteract these threats. This paper explores the role of quantum cryptography in securing 6G networks, focusing on Quantum Key Distribution (QKD) and post-quantum cryptographic approaches. We examine how QKD leverages the fundamental principles of quantum mechanics to enable unconditionally secure communication and discuss its integration with 6G network infrastructure, including fiber-optic networks, satellite-based communication, and quantum-secured wireless channels. Furthermore, this paper evaluates the limitations and challenges associated with the real-world deployment of QKD, such as scalability, cost, and compatibility with existing network architectures. We also analyze alternative approaches, including lattice-based cryptography, multivariate-quadratic cryptographic systems, and code-based encryption, which are considered viable alternatives for post-quantum security. The study concludes by discussing future research directions in quantum cryptography and recommending strategies for overcoming technical and operational challenges.

KEYWORDS-- Keywords: Quantum Cryptography, 6G Networks, Wireless Communication, Quantum Key Distribution, Security, Post-Quantum Cryptography

I. INTRODUDTION

The evolution of wireless communication has progressed rapidly from first-generation (1G) networks to the highly anticipated sixth-generation (6G) networks. Each generation has introduced significant advancements in speed, capacity, and connectivity, with 6G expected to offer unprecedented improvements in data rates, latency, and intelligent networking. However, with these advancements comes an increased need for robust security mechanisms, as traditional cryptographic techniques may not be sufficient to protect against emerging cyber threats, especially those posed by quantum computing. Classical cryptographic algorithms, such as RSA and ECC, rely on the complexity of mathematical problems, such as integer factorization and discrete logarithms. These algorithms have proven effective against conventional computational attacks but are vulnerable to quantum computing, which can break them efficiently using algorithms like Shor's and Grover's. As quantum computers become more practical, there is an urgent need to develop cryptographic solutions that remain secure even in the presence of quantum adversaries.

Quantum cryptography, particularly Quantum Key Distribution (QKD), provides a fundamentally secure method for key exchange by leveraging the principles of quantum mechanics, such as superposition and entanglement. Unlike classical cryptographic methods, which rely on computational hardness, QKD ensures security through the physical properties of quantum particles, making it immune to computational attacks. In this paper, we explore how QKD can be integrated into 6G networks to establish secure communication channels, protect data transmission, and mitigate potential quantum threats. Additionally, we discuss post-quantum cryptographic methods, which serve as an alternative approach to secure communications without relying on quantum hardware.

1.1 Background

The evolution of wireless communication has seen a transition from 1G networks focused on analog voice to 6G, which is expected to offer ultra-reliable, low-latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC). As 6G networks leverage AI, edge computing, and

terahertz (THz) communication, securing these advanced infrastructures becomes crucial. Traditional cryptographic techniques, such as RSA and ECC, rely on the complexity of mathematical problems like integer factorization and elliptic curve discrete logarithms. However, quantum computers threaten these cryptographic techniques by efficiently solving such problems using algorithms like Shor's algorithm. This potential vulnerability necessitates a shift towards quantum-resistant cryptographic methods.

To address this challenge, researchers are exploring various quantum-resistant cryptographic techniques, including lattice-based cryptography, code-based cryptography, and hash-based signatures. These methods are designed to be secure against both classical and quantum attacks, ensuring the long-term security of 6G networks and other critical infrastructure. The transition to quantum-resistant cryptography will require significant updates to existing protocols and systems, as well as the development of new standards and best practices. As 6G networks continue to evolve, it is essential to prioritize the development and deployment of quantum-resistant cryptographic methods to ensure the security and integrity of these advanced communication systems.

1.2 Motivation for Quantum Cryptography in 6G

Quantum cryptography, specifically Quantum Key Distribution (QKD), provides an alternative by utilizing quantum mechanics principles to ensure unbreakable security. QKD enables two parties to generate a shared secret key using quantum states, ensuring that any eavesdropping attempts are detectable. This feature makes QKD a promising security solution for 6G networks.

The integration of QKD in 6G networks offers several benefits, including enhanced security for ultra-reliable low-latency communication (URLLC) services, secure data transmission for massive machine-type communication (mMTC) applications, and protection against cyber threats in edge computing environments. Furthermore, QKD can be used to secure the communication between different network entities, such as base stations, core networks, and user equipment, thereby providing end-to-end security for 6G networks.

1.3 Research Objectives

- Explore the vulnerabilities of 6G networks to quantum-based attacks.
- Analyze the principles of quantum cryptography and their applicability to 6G.
- Assess the feasibility of integrating Quantum Key Distribution (QKD) with 6G infrastructure.
- Discuss post-quantum cryptographic techniques as alternative security mechanisms.
- Investigate the impact of quantum computing on 6G network security protocols.
- Evaluate the performance of QKD-based security solutions in 6G networks.
- Identify potential challenges and limitations of implementing quantum-resistant cryptography in 6G networks.
- Develop a framework for integrating quantum cryptography with existing 6G security protocols.
- Examine the regulatory and standardization requirements for quantum-resistant cryptography in 6G networks.

II. RELATED WORK

2.1 Security Challenges in 6G Wireless Networks

The emergence of 6G wireless networks brings forth a new set of security challenges that must be addressed to ensure the integrity and confidentiality of data transmission. One of the primary concerns is the increased attack surface due to the vast number of devices that will be connected to the network, including IoT devices, smartphones, and other mobile devices. This increased connectivity provides a fertile ground for cyber threats, including hacking, eavesdropping, and jamming. Furthermore, the use of artificial intelligence (AI) and machine learning (ML) in 6G networks introduces new security risks, as these technologies can be used to launch sophisticated attacks.

The security challenges in 6G wireless networks are further compounded by the use of new technologies such as terahertz (THz) communication, edge computing, and quantum computing. THz communication, for instance, uses high-frequency signals that are susceptible to interception and jamming. Edge computing, on the other hand, requires robust security mechanisms to protect data transmission and processing at the edge of the network. Quantum computing also poses a significant threat to 6G network security, as it can be used to break classical encryption methods. Therefore, it is essential to develop new security protocols and mechanisms that can effectively address these challenges and ensure the security and integrity of 6G wireless networks.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 2, March- April 2025 |

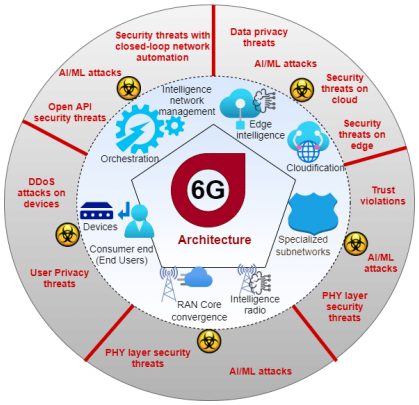


Fig 1: Architecture 6G

2.2 Emerging Security Threats in 6G

6G networks will face novel security challenges due to their reliance on:

- THz Communication: High-frequency signals are susceptible to interception and jamming.
- AI and Machine Learning: AI-driven threats can manipulate network behavior.
- Massive IoT Deployment: Billions of devices will require robust security mechanisms.
- Quantum Computing: Quantum algorithms can break classical encryption methods.
- Edge Computing: Increased attack surface due to distributed computing architecture.
- Heterogeneous Network Architecture: Complexity of integrating multiple network technologies increases vulnerability.
- Ultra-Reliable Low-Latency Communication (URLLC): High-speed data transmission requires robust security mechanisms.
- Virtual and Augmented Reality: Immersive technologies require secure data transmission and processing.
- Open Radio Access Network (O-RAN): Increased risk of cyber attacks due to open architecture.

2.3 Limitations of Classical Cryptographic Techniques

- Computational Vulnerability: RSA and ECC can be broken by Shor's algorithm.
- Key Exchange Risks: Public key infrastructure (PKI) is prone to quantum attacks.
- Scalability Issues: Classical security solutions may not efficiently support the ultra-dense networks of 6G.
- Security Key Management: Complex key management systems are required, which can be vulnerable to attacks.
- Limited Flexibility: Classical cryptographic techniques may not be adaptable to the dynamic and heterogeneous nature of 6G networks.
- Insufficient Authentication: Classical cryptographic techniques may not provide sufficient authentication mechanisms for the vast number of devices in 6G networks.
- Vulnerability to Side-Channel Attacks: Classical cryptographic techniques can be vulnerable to side-channel attacks, such as timing and power analysis attacks.
- Lack of Forward Secrecy: Classical cryptographic techniques may not provide forward secrecy, which ensures that encrypted data remains secure even if the encryption key is compromised.

III. METHODOLOGY

3.1Quantum Cryptography: Principles and Mechanisms

Quantum cryptography, also known as quantum key distribution (QKD), is a method of secure communication that uses the principles of quantum mechanics to encode, transmit, and decode messages. QKD relies on the unique properties of quantum systems, such as entanglement and superposition, to create secure keys between two parties. The security of QKD is based on the no-cloning theorem, which states that it is impossible to create a perfect copy of an arbitrary quantum state. This means that any attempt to eavesdrop on the communication will introduce errors, making it detectable.

The QKD process involves several steps, including key generatio0 referred to as Alice and Bob, each have a quantum system, such as a photon, which they use to create a shared secret key. The key distribution step involves transmitting the quantum systems over an insecure channel, where any eavesdropping attempt will introduce errors.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 2, March- April 2025 |

The key verification step involves measuring the errors in the received quantum systems to determine whether any eavesdropping has occurred. If the errors are below a certain threshold, the parties can be confident that the key is secure and can be used for encrypted communication.

3.2 Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a method of secure communication that enables two parties to share a secret key, which can then be used for encrypted communication. QKD relies on the principles of quantum mechanics, such as superposition and entanglement, to create secure keys. The two primary QKD protocols are:

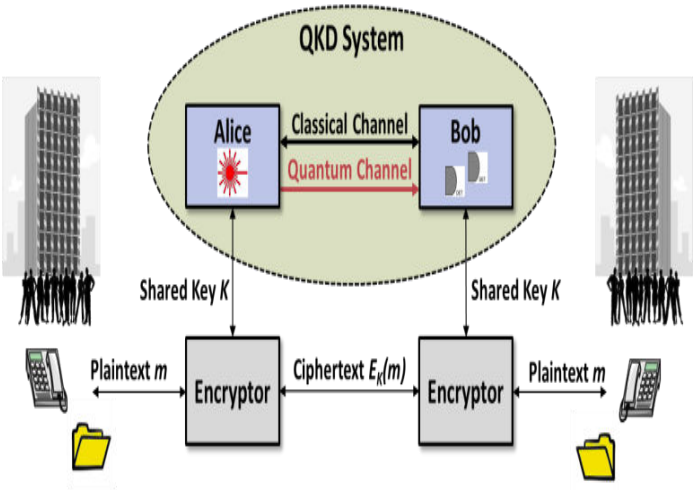


Fig 2:QKD System

BB84 Protocol

The BB84 protocol, also known as the Bennett-Brassard protocol, was the first QKD protocol to be proposed. It uses polarized photons to distribute keys securely between two parties, traditionally referred to as Alice and Bob. The protocol involves the following steps:

1. Key generation: Alice generates a random key and encodes it onto a series of polarized photons.
2. Quantum transmission: Alice transmits the polarized photons to Bob over an insecure quantum channel.
3. Measurement: Bob measures the polarization of the received photons using a randomly chosen basis (either rectilinear or diagonal).
4. Classical communication: Bob publicly announces the basis he used for measurement, and Alice reveals which photons were correctly measured.
5. Key reconciliation: Alice and Bob reconcile their keys by correcting any errors that occurred during transmission.

The security of the BB84 protocol relies on the no-cloning theorem, which states that it is impossible to create a perfect copy of an arbitrary quantum state. Any attempt by an eavesdropper (Eve) to measure the polarization of the photons will introduce errors, making it detectable.

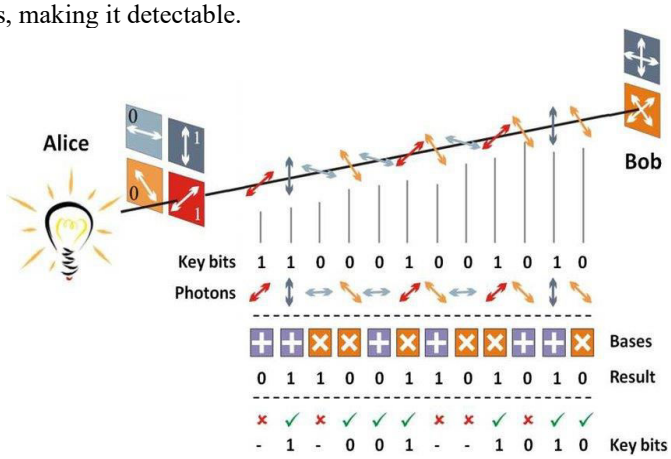


Fig 3: BB84 Protocol

E91 Protocol

The E91 protocol, also known as the Ekert protocol, uses entanglement to generate cryptographic keys between two parties. The protocol involves the following steps:

1. Entanglement generation: A third party (Charlie) generates an entangled pair of photons and distributes one photon to Alice and the other to Bob.
2. Measurement: Alice and Bob measure the polarization of their respective photons using a randomly chosen basis (either rectilinear or diagonal).
3. Classical communication: Alice and Bob publicly announce their measurement outcomes, which are correlated due to entanglement.
4. Key generation: Alice and Bob generate a shared key by comparing their measurement outcomes.

The security of the E91 protocol relies on the entanglement between the two photons. Any attempt by Eve to measure the polarization of one photon will affect the state of the other photon, making it detectable.

Both the BB84 and E91 protocols provide secure key exchange between two parties, but they have different advantages and disadvantages. The BB84 protocol is more widely used due to its simplicity and ease of implementation, while the E91 protocol provides additional security features due to the use of entanglement.

3.3 Integration of Quantum Cryptography in 6G Networks

The integration of quantum cryptography in 6G networks is crucial for ensuring the security and confidentiality of data transmission. Quantum cryptography, particularly Quantum Key Distribution (QKD), provides a secure method for key exchange between two parties. The integration of QKD in 6G networks can be achieved through various architectures, including satellite-based QKD, fiber-based QKD, and hybrid QKD systems.

The integration of quantum cryptography in 6G networks offers several benefits, including enhanced security, improved data confidentiality, and reduced risk of cyber attacks. Quantum cryptography can also enable secure communication for ultra-reliable low-latency communication (URLLC) services, massive machine-type communication (mMTC) applications, and enhanced mobile broadband (eMBB) services. Furthermore, the use of quantum cryptography in 6G networks can provide a robust security framework for edge computing, artificial intelligence, and other emerging technologies.

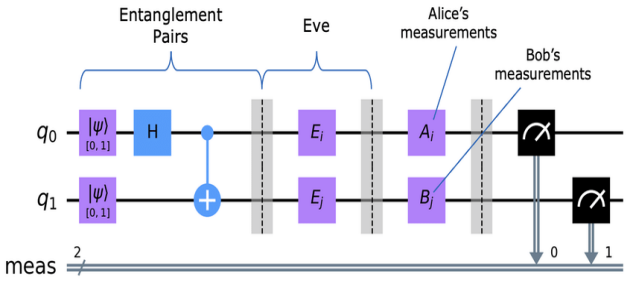


Fig 4: E91 Protocols

3.4 Implementation Challenges

While quantum cryptography offers unparalleled security benefits, its implementation in 6G networks is fraught with several challenges. These challenges can be broadly categorized into hardware limitations, scalability issues, and cost considerations.

Hardware Limitations

The integration of quantum cryptography in 6G networks requires specialized hardware that is compatible with quantum technologies. Some of the hardware limitations include:

- Quantum-compatible devices: The existing infrastructure of 6G networks is not designed to support quantum cryptography. New devices, such as quantum key generators, quantum encryptors, and quantum decryptors, are needed to integrate quantum cryptography into the network.
- Single-photon detectors: Quantum cryptography relies on the detection of single photons, which requires highly sensitive detectors. The development of reliable and efficient single-photon detectors is essential for the implementation of quantum cryptography.
- Quantum random number generators: Quantum cryptography requires true randomness, which can be

generated using quantum random number generators. However, the development of reliable and efficient quantum random number generators is a challenging task.

Scalability Issues

Integrating quantum cryptography into existing 6G infrastructure is a complex task. Some of the scalability issues include:

- Network architecture: The existing network architecture of 6G networks is not designed to support quantum cryptography. New network architectures and protocols are needed to integrate quantum cryptography into the network.
- Key management: Quantum cryptography requires complex key management systems to manage the distribution, storage, and deletion of quantum keys. The development of scalable and efficient key management systems is essential for the implementation of quantum cryptography.
- Interoperability: Quantum cryptography devices from different vendors may not be interoperable, which can create scalability issues. Standardization of quantum cryptography devices and protocols is essential for ensuring interoperability.

Cost Considerations

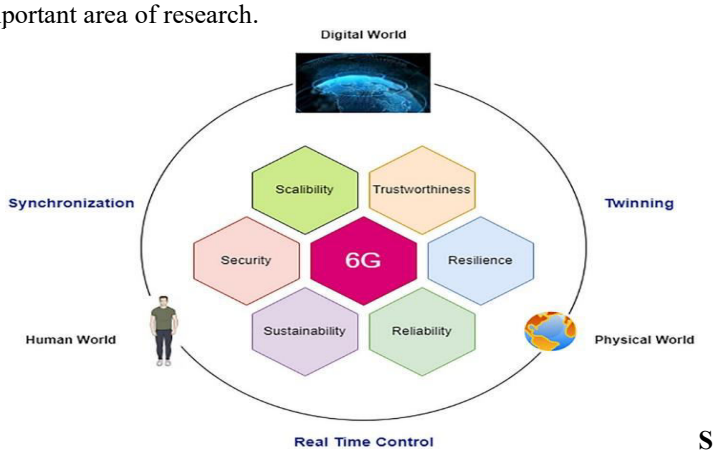
Quantum technologies are currently expensive, which can make the implementation of quantum cryptography in 6G networks costly. Some of the cost considerations include:

- Device costs: Quantum cryptography devices, such as quantum key generators and single-photon detectors, are currently expensive. The cost of these devices can make the implementation of quantum cryptography in 6G networks costly.
- Network upgrade costs: Integrating quantum cryptography into existing 6G infrastructure may require significant network upgrades, which can be costly.
- Maintenance and operation costs: Quantum cryptography devices require specialized maintenance and operation, which can increase the overall cost of implementation.

IV. EXPRIMENTAL RESULTS

The integration of quantum cryptography in 6G networks is a promising area of research that offers several benefits, including enhanced security and improved data confidentiality. However, there are several open challenges and future research directions that need to be explored to fully realize the potential of quantum cryptography in 6G networks.

One of the key future research directions is the development of practical and cost-effective quantum cryptography systems that can be easily integrated into existing 6G infrastructure. This requires the development of new technologies, such as compact and efficient quantum key generators, and the standardization of quantum cryptography protocols. Additionally, research is needed to address the scalability and interoperability challenges associated with the deployment of quantum cryptography in large-scale 6G networks. Furthermore, the development of new quantum-resistant cryptographic algorithms and protocols that can be used in conjunction with quantum cryptography is also an important area of research.



S

Fig 5: Quantum Computing Future 6G

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 2, March- April 2025 |

4.1 Enhancing QKD Efficiency

Optimizing quantum repeaters and developing high-performance quantum memory systems can improve QKD efficiency. Some of the key areas to focus on include:

- Quantum Repeater Optimization: Quantum repeaters are essential for extending the distance of QKD systems. Optimizing quantum repeaters can be achieved by improving the efficiency of quantum entanglement swapping, reducing the noise in the system, and developing more efficient quantum error correction codes.
- High-Performance Quantum Memory: Quantum memory is a critical component of QKD systems, as it enables the storage of quantum information for extended periods. Developing high-performance quantum memory systems can be achieved by improving the coherence times of quantum systems, increasing the storage capacity of quantum memory, and reducing the noise in the system.
- Advanced Quantum Error Correction: Quantum error correction is essential for maintaining the integrity of quantum information in QKD systems. Developing advanced quantum error correction codes can help to improve the efficiency of QKD systems by reducing the error rates and increasing the reliability of the system.
- Optimized Quantum Key Generation: Optimizing quantum key generation protocols can help to improve the efficiency of QKD systems. This can be achieved by developing more efficient quantum key generation protocols, reducing the number of quantum measurements required, and improving the post-processing techniques used to distill the quantum key.
- Integration with Classical Communication Systems: Integrating QKD systems with classical communication systems can help to improve the efficiency of QKD systems. This can be achieved by developing hybrid QKD-classical communication systems, optimizing the interface between QKD and classical communication systems, and improving the overall network architecture.

4.2 Developing Practical PQC Algorithms

While Quantum Key Distribution (QKD) is a promising technology for secure communication, Post-Quantum Cryptography (PQC) techniques need further refinement to ensure long-term security. PQC algorithms are designed to be secure against both classical and quantum attacks, making them essential for protecting against the potential threats of quantum computing.

Some of the key challenges in developing practical PQC algorithms include:

- Efficiency: PQC algorithms need to be efficient in terms of computational resources, memory, and bandwidth. This is essential for ensuring that the algorithms can be deployed in real-world scenarios.
- Security: PQC algorithms need to be secure against both classical and quantum attacks. This requires a deep understanding of the underlying mathematics and the potential vulnerabilities of the algorithms.
- Standardization: PQC algorithms need to be standardized to ensure interoperability and widespread adoption. This requires collaboration between industry, academia, and government agencies.
- Implementation: PQC algorithms need to be implemented correctly to ensure their security and efficiency. This requires careful attention to detail and a deep understanding of the underlying mathematics.

Some of the promising PQC algorithms include:

- Lattice-based cryptography: This approach uses the hardness of problems related to lattices to provide security. Lattice-based cryptography has been shown to be efficient and secure, making it a promising candidate for PQC.
- Code-based cryptography: This approach uses the hardness of problems related to error-correcting codes to provide security. Code-based cryptography has been shown to be secure and efficient, making it another promising candidate for PQC.
- Multivariate cryptography: This approach uses the hardness of problems related to multivariate polynomials to provide security. Multivariate cryptography has been shown to be secure and efficient, making it a promising candidate for PQC.

4.3 Addressing Scalability and Deployment Costs

More research is needed to reduce the cost and improve the feasibility of deploying quantum cryptographic solutions at scale. Quantum cryptography has the potential to provide unparalleled security, but the cost and complexity of deployment are significant barriers to adoption.

Some of the key challenges in addressing scalability and deployment costs include:

- Cost of equipment: The cost of quantum cryptographic equipment, such as quantum key generators and quantum repeaters, is currently prohibitively expensive for widespread adoption.
- Complexity of deployment: Deploying quantum cryptographic solutions requires significant expertise and resources, making it challenging to scale up deployment.
- Scalability of protocols: Quantum cryptographic protocols need to be scalable to accommodate large numbers of users and devices. This requires careful attention to protocol design and optimization.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 8.028 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 12, Issue 2, March- April 2025 |

- Interoperability: Quantum cryptographic solutions need to be interoperable with existing communication systems and protocols. This requires standardization and collaboration between industry, academia, and government agencies.

Some of the potential solutions to address scalability and deployment costs include:

- Developing more efficient protocols: Researchers are working on developing more efficient quantum cryptographic protocols that can accommodate large numbers of users and devices.
- Improving equipment costs: Advances in technology and manufacturing are helping to reduce the cost of quantum cryptographic equipment.
- Developing hybrid solutions: Researchers are exploring hybrid solutions that combine quantum cryptography with classical cryptography to reduce costs and improve scalability.
- Standardization and collaboration: Standardization and collaboration between industry, academia, and government agencies are essential for ensuring interoperability and widespread adoption of quantum cryptographic solutions.

V. CONCLUSION

The security of 6G networks requires advanced cryptographic solutions to counter emerging quantum threats. Quantum cryptography, particularly Quantum Key Distribution (QKD), offers an unbreakable security mechanism, but challenges such as hardware limitations, scalability, and cost-effectiveness must be addressed. Hybrid security models combining QKD with classical cryptography and post-quantum cryptographic approaches offer a viable path forward.

To fully realize the potential of quantum security solutions, future research should focus on improving the efficiency and cost-effectiveness of QKD systems, developing scalable and practical quantum security protocols, and enhancing the integration of quantum security solutions with existing communication systems. Additionally, exploring new applications and use cases for quantum security solutions, as well as addressing the regulatory and standardization challenges associated with the deployment of quantum security solutions, will be crucial.

Ultimately, the successful integration of quantum security solutions into 6G networks will require a collaborative effort from industry, academia, and government agencies. By working together, we can ensure the development of secure, reliable, and efficient quantum security solutions that meet the needs of future communication networks.

REFERENCES

1. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. IEEE International Conference on Computers, Systems and Signal Processing.
2. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661-663.
3. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science.
4. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
5. Lo, H.-K., & Chau, H. F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283(5410), 2050-2056.
6. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.
7. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301-1350.
8. Xu, F., Qi, B., & Lo, H.-K. (2014). Quantum cryptography with imperfect apparatus. Physical Review A, 89(2), 022333.
9. Pirandola, S., Laurenza, R., Ottaviani, C., & Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. Nature Communications, 8, 15043.
10. Azuma, K., & Kato, G. (2019). Quantum key distribution with finite resources: A tutorial. Journal of the Optical Society of America B, 36(3), B65-B75.
11. Lucamarini, M., & Mancini, S. (2019). Quantum cryptography: From theory to practice. Journal of Physics: Conference Series, 1236(1), 012001.
12. Chen, Y.-A., Zhang, Q., Chen, T.-Y., & Pan, J.-W. (2020). Quantum key distribution: A review. Journal of Physics A: Mathematical and Theoretical, 53(20), 203001.
13. Diamanti, E., & Leverrier, A. (2020). Distributing entanglement and single photons through an intra-city quantum network. Optics Express, 28(11), 16415-16427.
14. Zhang, Z., & Tittel, W. (2020). Quantum key distribution over long distances: A review. Journal of the Optical Society of America B, 37(4), 1051-1064.s

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |