Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 06, June - 2025

Classical Cryptography to Quantum Cryptography

Suhani Wadhwa
Department of Information Technology
Indira Gandhi Delhi Technical University for Women, Delhi, India

1. INTRODUCTION

This is the third wave of the digital age and cryptography is the science and backbone of secure communication. Everything from your public database to sensitive information needs to be protected from any potential eves dropping and threats. The rapid research and growth in quantum computing seems very fascinating but it can be a big threat to the current quantum cryptographic algorithms like RSA.

RSA cryptography relies on a public-private key pair, where the public key consists of an exponent e and a modulus $N = p \times q$, with p and q being large prime numbers. The private key is derived using these primes and modular arithmetic. The security of RSA is based on the difficulty of factoring N into p and q, a problem that classical computers struggle to solve efficiently. However, quantum computers, using Shor's algorithm, can factor N exponentially faster, posing a significant threat to modern cryptographic security.

Quantum key distribution uses Quantum mechanical concepts such as entanglement to ensure secure communication and to make sure there is no attempt to eavesdrop or intercept the communication system. Unlike classical encryption, QKD provides information-theoretic security, making it resistant to both classical and quantum adversaries.

This paper provides a literature review of the QKD, protocols like BB84 and modern QKD systems like the DI-QKD system. It examines the key principles, experimental progress, scalability, future scope and challenges. It also identifies current problems that are open to further future research.

While QKD has advanced a lot in theory and experiments, putting it into real-world use still has challenges. This review explores the gap between its theoretical security and practical limitations, discussing existing research and future steps to make QKD more secure and scalable for real-world applications.

2. BACKGROUND ON QUANTUM CRYPTOGRAPHY

2.1 Evolution of Cryptography

Earlier cryptographic methods include Caesar Cipher and Vigenère Cipher.

Caesar Cipher involved shifting of alphabets, the number of times the alphabets were shifted was the key. For example, if a plain text of "Hi" was supposed to be sent, then the cryptographic text might be "Kl" and the key would be 3. As there are only 25 possible shifts, It was easy to get the key.

Vigenère Cipher used a key to vary the shifts in words. For example, a word "Hello" using the key "key" would be encrypted as "Keyke". This was a more secure approach as compared to Caesar cipher but could still be easily broken using modern cryptographic methods.

Modern cryptographic systems have revolved around methods like RSA and ECC. RSA relies on the complexity of the factor problem and ECC leverages the computational hardness of solving certain logarithmic problems.

Quantum computers can make these problems very easy to solve hence posing a threat to modern cryptography as mentioned in studies like "Quantum Computation and Shor's Algorithm" by Peter W. Shor (1997) which talks about Shor algorithm simplifying the factor problem.

The emergence of Quantum cryptography started by the BB84 protocol as stated in the 1984 paper by Bennett and Brassard. Later on Artur Ekurt's 91 protocol also played a key role in enhancing the quantum cryptographic methods.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 06, June - 2025

2.2 Key Quantum Principles

(A) Superposition: The superposition principle in quantum physics allows qubits to exist in a superposition state of both 0 and 1 at the same time unlike the classical bits which can only exist as 0 or 1 at a given point in time.

(B) Entanglement: Entanglement is the state of two photons being correlated to each other despite the distance between them. Change in state of any one of the photons can lead to the change in other.

(C) No Cloning theorem: This theorem states that nobody can make a perfect copy of an unknown quantum state. This was proven by Wootters and Zurek in 1982.

2.3 Early QKD Protocols

The BB84 protocol uses polarized photos for its cryptographic communication. We assume that Alice wants to send information Bob, she chooses any one polarized bases and encodes each bit using that polarized base. Similarly, Bob measures the photons using any random base of his choice. Once this is done, Alice and Bob publicly compare their bases, if they observe any errors, they can conclude an interception was made thanks to the superposition principle.
Papers and studies like the one done by Scarani et al in 2009 shows the feasibility of implementation of the BB84 protocol and ensures secure communication upto a distance of 100kms.

2.4 Modern QKD Systems

The DI-QKD (Device independent quantum key distribution system) as the name suggests removes the need to rely on the internal workings of a quantum system increasing the security as it is completely based on the statistical outcomes of the quantum measurements.
This system works on violations of Bell's inequality which was first introduced in the 1991 paper "Quantum cryptography based on Bell's theorem" written by Artur Ekert. This paper discussed how Bell's theorem and quantum cryptography can go hand in hand laying foundations for secure communication. In this process, a quantum source first produces entangles particles which are sent to two parties Alice and Bob. They both then choose random measurement settings to test for Bell's violations or CSHS inequality. Using this, they can confirm the presence of interception and can produce to use a secure key. This way, the internal workings of a quantum system will play no role in the security of the communication process. One of the earliest implementations of this process was done by B. Hensen in 2015 where he performed Loop-hole free Bell equality violation of two electron spins separated by a distance of 1.3kms. This turned to be a key-milestone in proving the practicality of using DI-QKD.

3. APPLICATIONS OF QUANTUM CRYPTOGRAPHY

3.1 Quantum Networks

Quantum Networks is one of the most prominent applications of Quantum cryptography as it helps in secure communication over long distances.

One of the most ground breaking work done in this field was the Micius satellite launched by China in 2016. It demonstrated secure QKD transmission over 1200 kms. This was published in 'Science' by Yin et al.

3.2 Financial Security Systems

Banks and financial institutions are implementing QKD in their daily tasks to facilitate safe transactions in an easier way than what is being used today. For example, the Swiss company ID Quantique has partnered with multiple financial firms to incorporate QKD for high security data transmission.

3.3 Healthcare and Medical Data security

Given the increasing number of breaches in the medical sector, QKD can help with safeguarding sensitive medical information of patients. Studies such as the one done by Lo et al in nature photonics highlight how it can enhance data protection in telemedicine networks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 06, June - 2025

3.4 Government and Defence use cases

Government and defence organizations are using QKD to secure diplomatic communication Research by Peev et al published in New journal of physics states the same. In 2007, a QKD-secured video conference was successfully conducted between Vienna and Bratislava, demonstrating the potential of QKD in diplomatic security.

4. CHALLENGES AND FUTURE DIRECTIONS

4.1 Practical implementation challenges

Scalability issues

While QKD has been successfully demonstrated on a smaller scale like laboratories, its implementation on a larger and global scale still remains a challenge that physicists are looking to tackle. This would require extensive infrastructure including quantum repeaters, entanglement distribution mechanisms, and fault-tolerant quantum hardware.

Distance Limitations

Fiber-optics cables face distance loss due to the weakening in signals with increasing distance. Due to the no cloning theorem studied in quantum computing, these signals can't be amplified and copied unlike the classical signals and hence covering large distances still remain a challenge in this field of study. Even though twin field QKD proposed by Lucamarini in 2018 has shown promise in extending secure transmission beyond 500 kms, further enhancements are still pending.

Hardware vulnerabilities and side-channel attack

QKD in practicality is unbreakable but limitations in our current resources have shown vulnerability in practical implementations. Imperfections in quantum devices, such as photon source inconsistencies and detector inefficiencies, create security loopholes that attackers can exploit.

4.2 Practical implementation challenges

Post Quantum cryptography (PQC) and Hybrid Systems

This focuses on building classical cryptography algorithms resistant to quantum attacks. This hybrid approach includes systems that integrate both the PQC and QKD for enhanced security in real world applications. (Mosca et al., IEEE Security & Privacy, 2018).

Quantum repeaters and Long-distance QKD

Quantum repeaters allow entanglement swapping allowing signals to travel a much larger distance. These are established at distant nodes without physically sending an entangled qubit the entire distance.

Advancements in Satellite-based QKD

Satellite QKD can act as a replacement for fiber optics transmission as these can travel over thousands of kilometres. Efficiency and cost effectiveness are the two areas where future research is going to be concentrating on as far as Satellite-based QKD goes.

5. CONCLUSION

Quantum cryptography has proven to be a ground breaking discovery in modern science. It has proven to be a replacement for traditional cryptographic practices which can be easily broken. Through methods like BB84 and E91, QKD theoretically proves to be unbreakable as it uses quantum phenomena like superposition and entanglement. As this review states, QKD has already found a practical use in areas like finance, government and cloud computing.

That being said, challenges still exist in these quantum cryptographic systems. Large distances, hardware imperfections and side channel leakage are some of the issues that still need to be tackled. Quantum repeaters, post-quantum cryptography (PQC), and satellite-based QKD are some areas are being researched to tackle the said issues.

Governments, industry, and scientists need to join forces to narrow the difference between theoretical security and practical implementation. By breaking down the present barriers, quantum cryptography can rewrite secure communication by making long-term data privacy feasible at a time when quantum computers undermine traditional forms of encryption.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 06, June - 2025

REFERENCES

[1] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997.
[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179, 1984.
[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters, vol. 67, no. 6, pp. 661–663, 1991.
[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Reviews of Modern Physics, vol. 81, no. 3, pp. 1301–1350, 2009.
[5] B. Hensen et al., "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," Nature, vol. 526, pp. 682–686, 2015.
[6] J. Yin et al., "Satellite-based entanglement distribution over 1200 kilometers," Science, vol. 356, no. 6343, pp. 1140–1144, 2017.
[7] ID Quantique, "Quantum-Safe Security for the Financial Industry," [Online]. Available: https://www.idquantique.com.
[8] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Nature Photonics, vol. 8, pp. 595–604, 2014.
[9] M. Peev et al., "The SECOQC quantum key distribution network in Vienna," New Journal of Physics, vol. 11, p. 075001, 2009.
[10] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature, vol. 557, pp. 400–403, 2018.
[11] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018.