A Survey on Improving Cyber Security Encryption Methods using Quantum Computing

Deepa Barethiya ; Priti Zanzad ; Nishad Kamlekar
Dept. of Master in Computer Application, GHRCEM, Nagpur, India

Abstract
This paper inspects the evolutionary impression of quantum computing on cybersecurity encryption techniques. Quantum computing shows both ultimate and opportunities inside the area of cybersecurity. classical encryption techniques, which depend on complex mathematical issues for security, are highly vulnerable to quantum algorithms like as Shor's and Grover's algorithms, which can proficiently split these encryption plans. Although, quantum computing also simplifies the growth of advanced encryption methods, as well as Quantum Key Distribution (QKD) and post-quantum cryptographic algorithms, which provide enhanced security opposed to quantum threats. In this paper author discusses the impact of quantum computing on encryption, reviews ongoing study into quantum-resistant cryptographic methods and policies for applying quantum-safe security frameworks to ensure powerful data encryption.

Keywords: Quantum computing, encryption, cybersecurity, quantum key distribution, post-quantum cryptography.

1. Introduction

Quantum computing is become visible field that influence the concepts of quantum mechanics to process information in elementally distinct ways from traditional computers. Unlike traditional bits, which can show either a 0 or a 1, quantum bits, or qubits, can live in a position of superposition, meaning they can represent both 0 and 1concurrently. This property, across with quantum involvement, permits quantum computers to present some calculations much more effectively than traditional computers. For example, quantum computing has the power to transfiguring areas like cryptography, material science, and complex system modeling [18]. The appearance of quantum computing shows pattern shift in the landscape of infrastructure security. Quantum computing's remarkable suggestions penetrate every layer of our digital infrastructure, releasing a shadow of uncertainty over the realm of cyber security [13].

2. Literature Review

In the domain of cybersecurity, encryption techniques are necessary for protecting data integrity and confidentiality. Encryption changes readable data to an unreadable format using algorithms and keys, assuring that only permissible parties can access the original information. Encryption can be classified into two primary types that are, symmetric and asymmetric encryption. In symmetric encryption it utilizes the same key for both encryption and decryption process of data, creating an efficient but requiring secure key distribution. Common symmetric encryption algorithms consist the Advanced Encryption Standard (AES) and Data Encryption Standard (DES). Asymmetric encryption, also called as public-key encryption, utilizes a pair of keys—a public key for encryption and a private key for decryption—increasing security during data transmission over unsecured channels. Remarkable asymmetric encryption algorithms include RSA and Elliptic Curve Cryptography (ECC) [19]. Cybersecurity is the avoidance of any damage to electronic communication systems and services and the protection of information involved along with containing integrity, availability,

DOI: https://doi.org/10.5281/zenodo.15463011

confidentiality, authentication and non-repudiation [16].

The appearance of quantum computing poses important challenges to present encryption techniques. Quantum algorithms, like Shor's algorithm, can successfully solve problems such as integer factorization, which supports the security of mostly used encryption methods like RSA. This potential threatens the effectiveness of traditional encryption techniques, requiring the evolution of quantum-resistant cryptographic methods to ensure data security in a post-quantum world [20]. In today's dynamic digital world, cybersecurity is a guard against increasing number of threats that come with technological advancements. Cybersecurity protocols are essential in the current era because most digital systems, like distributed file systems, NoSQL databases, and Network-Attached Storage (NAS), are used to store largeamounts of data [1].

Quantum computers leverage the principles of superposition and entanglement to perform difficult calculations at an exponentially faster rate as compared to traditional computers [2]. This computational power poses a fast risk to traditional encryption systems but also introduces new security patterns. This paper aims to shows this dual side, highlighting vulnerabilities in present encryption standards and developing the potential of quantum-resistant cryptographic techniques.

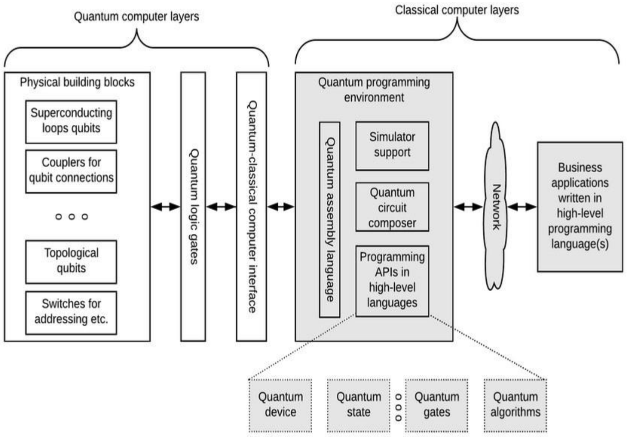
Quantum computer layers
Classical computer layers
Physical building blocks
Superconducting loops qubits
Couplers for qubit connections
Topological qubits
Switches for addressing etc.
Quantum logic gates
Quantum-classical computer interface
Quantum programming environment
Quantum assembly language
Simulator support
Quantum circuit composer
Programming APIs in high-level languages
Network
Business applications written in high-level programming language(s)
Quantum device
Quantum state
Quantum gates
Quantum algorithms

Fig-1: Architecture of Quantum Computing Platform [11]

3. Traditional Encryption And Quantum Threats

Modern cryptographic systems depend on problems that are computationally complex for traditional computers to solve. For instance, RSA encryption is depended on the complexity of integer factorization, while ECC based on the complexity of the discrete logarithm problem. However, the introduction of quantum computing basically changes this landscape. Shor's algorithm, a quantum algorithm, can easily factor large integers, effectively breaking RSA encryption [3]. Likewise, Grover's algorithm can increase brute-force attacks on symmetric encryption systems, decreasing the effective security of AES keys. Research shows that with the advent of a sufficiently large quantum computer, present encryption techniques could be compromised in a matter of hours [4]. This highlights the intense requirement for quantum-resistant cryptographic solutions.

4. Quantum Key Distribution (Qkd)

Quantum Key Distribution (QKD) is a revolutionary security technique that uses quantum techniques to improve secure communication. QKD operates on the basis that measuring a quantum state improves its properties, through enabling the detection of any spy attempts. The BB84 protocol, introduced by Bennett and Brassard in 1984, is the most broadly utilize QKD protocol [5]. QKD ensures that any blocking of quantum keys is instantly noticeable, thereby creating secure communication channels feasible. This method represents an important step towards quantum-secure encryption systems and is being actively explored in different research and industrial applications.

5. Post-Quantum Cryptography (Pqc)

Post Quantum Cryptography is the area of cryptography in which encryption algorithms are created which are secure from an adversary with quantum computers [7]. The main point of post-quantum cryptography (also known quantum-resistant cryptography) is to create cryptographic

DOI: https://doi.org/10.5281/zenodo.15463011

systems that are secure oppose to both quantum as well as classical computers, and can interoperate with available communications protocols and networks [4]. Quantum Cryptography is the review of new cryptosystems which cannot be break by both quantum and traditional computers. The cryptosystems are classified into several families depend on the essential problem upon which the security is renowned. These essential problems are believed to be impossible by both traditional and quantum computers. The major families are lattice-based cryptography, isogeny-based cryptography, non-commutative cryptography, code-based cryptography, hash-based digital signatures, and multi-factor cryptography [7].

6. Quantum Secret Sharing And Secure Communications

Quantum Secrete Sharing (QSS) is the outcome of merging the principles of quantum mechanics with secret information distributing. It allows a sender to exchange a secret among receivers, and the receivers can then collectively recover the secret when the requirement arises. To increase the practicality of these quantum protocols, revolutionary idea of Quantum Anonymous Secret sharing (QASS) is advanced. To our knowledge, sharing quantum information is also an essential branch of quantum secret sharing, and has the same essential status as sharing traditional information. Its important advantage is the ability to achieve direct sharing of quantum information, which is particularly essential for quantum computing and quantum communication networks. [8]. QSS leverages the principles of quantum entanglement to gain heightened security in multi-party communication environments, creating it an essential component of future cryptographic systems.

7. Practical Implementations And Challenges

Quantum computations are physically realized via the time-progress of quantum systems steered by analog control signals. As quantum information is preserved in regular amplitudes and phases, these control signals must be carefully chosen to achieve expected result [9]. Several Governments and organizations are investing highly in quantum-resistant security infrastructures. Companies like Google, IBM, and have been actively evolving quantum computing solutions, while researchers work on hybrid cryptographic models that integrate traditional and quantum security. Although, the practical implementation of quantum cryptographic methods comes with challenges:

- High-end technology: Quantum computing methods remains costly and not accessible for widespread deployment.
- Vulnerability to noise: Quantum systems are extremely vulnerable to environmental disturbances, requiring error-correction mechanisms.
- Quantum network infrastructure: Creating a secure quantum communication network requires significant advancements in quantum networking techniques [10].

Government agencies and defense departments supervise difficult and different data, making them primary purpose for strong quantum-based attacks. As a preventive process, governments are searching quantum-safe frameworks, like as hybrid cryptographic systems adding both PQC and traditional encryption for a gradual change [15].

8. Future Directions

With the ongoing development of quantum computers, the threat of decrypting vulnerable data encrypted using standard techniques develops significantly. This approaching threat highlights the need for the development of quantum-resistant encryption methods [11].

The development of cybersecurity in the quantum age is a portrayal of ongoing modification and transformation. As digital methods have expert, so too have the techniques and practices created to preserve digital assets from unauthorized access and cyber threats. This process from past to present underscores the flexible interplay between technological innovation and cybersecurity approaches, particularly in the face of the quantum

DOI: https://doi.org/10.5281/zenodo.15463011

computing revolution [14]. As quantum methods continue to develop, the pursuit of practical quantum computing uses and the conclusion of current challenges become crucial for understanding the full power of quantum computation. Continued research in quantum hardware focuses to address ongoing disadvantages and push the limits of quantum computing capacities. Enhancing qubit coherence times, decreasing error rates, enhancing qubit connectivity are main objectives. Improvements in materials science, engineering, and innovative quantum architectures donate to the continue evolution of more robust quantum processors [12]. As quantum computing proceeds to develop, the requirement for quantum-resistant cryptographic solutions turns into increasingly difficult. Organizations must proactively change to post-quantum cryptographic algorithms and detect inquantum-secure communication methods. Quantum computing (QC) is a develop and increasingly growing domain. QC can potentially decrypt RSA and ECC algorithms, influencing almost 100% of encrypted Internet traffic. Businesses around the world are spilling in resources to additional QC knowledge and practices. [17].

9. Conclusion

In overview, the formation of quantum computing into cybersecurity offers a combination of challenges and opportunities. To direct this progressive era, it is essential to proactively gain quantum-resistant cryptographic cures, encourage collaborative research, handle ethical concerns, and create comprehensive regulatory frameworks. The future of cybersecurity in the quantum age will base on continuous evolution and a shared commitment to responsible approaches. By staying attentive and working together, it can utilize the potential of quantum methods to enhance digital security while diminishing the risks they introduce

9. References

[1] Abid Mehmood (Member, IEEE), Arslan Shafique, Moatsum Alawida, and Abdul Nasir Khan. Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques". 19 February 2024.

[2] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2010.

[3] L. K. Grover, "A fast quantum mechanical algorithm for database search," Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996, pp. 212-219.

[4] National Institute of Standards and Technology, "Post-Quantum Cryptography: NIST PQC Project," 04-Mar-2025. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography

[5] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, 1984, pp. 175-179.

[6] National Security Agency (NSA), "Quantum-Resistant Cryptography Recommendations," . Available: https://www.nsa.gov

[7] Ritik Bavdekar · Eashan Jayant Chopde · Ashutosh Bhatia · Kamlesh Tiwari, Sandeep Joshua Daniel · Atul, "Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research.

[8] Guo-Dong Li, Wen-Chuan Cheng, Qing-Le Wang, Long Cheng, Ying Mao, and Heng-Yue Jia, "Quantum Secret Sharing Enhanced: Utilizing W States for Anonymous and Secure Communication.

[9] Google AI, "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, pp. 505-510, 2019.

[10] IBM Research, "Building a Quantum-Safe Cryptographic Future".https://research.ibm.com/blog/new-quantum-safe-standards-NIST

[11] S. Singh and D. Kumar, "Enhancing Cyber Security Using Quantum Computing and Artificial Intelligence: A Review," June 3, 2024.

[12] O. A. Ajala, C. A. Arinze, O. C. Ofodile, C. C. Okoye, and A. I. Daraojimba, "Exploring and

DOI: https://doi.org/10.5281/zenodo.15463011

reviewing the potential of quantum computing in enhancing cybersecurity encryption methods," Magna Scientia Advanced Research and Reviews, vol. 10, no. 01, pp. 321–329, 2024.

[13] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure," Apr. 16, 2024.

[14] Enoch Oluwademilade Sodiya , Uchenna Joseph Umoga , Olukunle Oladipupo Amoo and Akoh Atadoga , Quantum computing and its potential impact on U.S. cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets, 2024, 18(02), 049–064.

[15] S. Khan, P. Krishnamoorthy, M.Goswami, F. M. Rakhimjonovna, S. A. Mohammed, and D. Menaga, "Quantum Computing and Its Implications for Cybersecurity: A Comprehensive Review of Emerging Threats and Defenses," vol. 1232–1248, 2024.

[16] A. Vaishnavi and S. Pillai, "Cybersecurity in the Quantum Era—A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods," 1964 (2021) 042002.

[17] Fazal Raheman, The Future of Cybersecurity in the Age of Quantum Computers . 16 November 2022.

[18] IBM Research, "What is QuantumComputing?" https://www.ibm.com/think/topics/quantum-computing.

[19] Splunk, "Data Encryption Methods & Types". https://www.splunk.com/en_us/blog/learn/data-encryption-methods-types.html.

[20] IBM Research, "How Quantum Computing Will Impact Cybersecurity."https://www.ibm.com/think/topics/ quantum-computing.

DOI: https://doi.org/10.5281/zenodo.15463011