OPEN ACCESS Freely available online

IJBSI International Journal of Business Studies and Innovation

ISSN 2737-5331
Volume 4, Issue 3
https://ijbsi.iikii.com.sg/
International Journal of Business Studies and Innovation

Technical Paper

Encryption and Decryption Technology for Quantum Computing

Yooan Lee[1]*, Taeyun Nam[2], and Sanghyeok Yune[3]

[1] Gyeonggi Global School; Goyang 10407, Korea
[2] Saint John's High School; Shrewsbury 01545 USA; taeyun0403@gmail.com
[3] FAYSTON Preparatory; Yongin 16802, Korea; 25yune.sanghyok@faystonsuji.org

* Corrrespondence; aidenlee321@icloud.com

Received: Sep 10, 2024; **Revised:** Oct 10, 2024; **Accepted:** Oct 13, 2024; **Published:** Oct 30, 2024

Abstract: We review the development of quantum computing and its corresponding encryption technology in this technical paper. As quantum computing is developing, a new paradigm of encryption technology is required as existing technologies cannot secure data and communication against quantum attacks. Through a literature review, the status and direction of further development of related technologies are explored to provide a basis for improving the present encryption technology for quantum computing. There is still room for development which necessitates the collaboration of stakeholders in a global network. More advanced algorithms and cryptography are mandatory for using quantum computing which will bring revolutionary technological advancement. Based on this report, the following study to improve the present algorithm is planned to apply them to diverse areas.

Keywords: Cryptography, Encryption, Decryption, Quantum Computing, Algorithm, Blockchain

1. Introduction

Quantum computing provides a revolutionary paradigm shift in computation and processing information based on quantum mechanics. Quantum computers use quantum bits or qubits of data while conventional computers use bits (0 or 1). Qubits can be superpositioned, meaning that they represent both 0 and 1 simultaneously. This is the key concept of quantum computing which enables the process of the enormous data. (Di Meglio et al., 2024; Subramanian et al., 2024). Quantum computing was proposed in the 1980s by Richard Feynman and David Deutsch. Feynman (1982) proposed the concept of quantum computing that simulates quantum systems. Shor (1994) developed an algorithm for quantum computing that factored large numbers exponentially faster than the best-known algorithms then, proving the potential of a quantum computer to revolutionize computing technologies including cryptography. Presently, quantum computing is researched extensively by numerous researchers and companies including IBM, Google, and Microsoft, along with startups. It is expected that quantum computing can be applied in cryptography, logistics and finance, drug discovery, and machine learning. These areas need revolutionary computational models for enhanced data analysis, solving complex problems, and complex simulation (Caltech, 2024; Flöther, 2023; Pixelplex, 2024). Quantum computing presents threats and opportunities for existing computer technologies. Among them, widely-used encryption using Rivest–Shamir–Adleman (RSA) can be easily broken as a quantum computer. Shor (1997) already showed that quantum computers could break RSA. Thus, post-quantum cryptography needs to be developed by creating algorithms that are secure against such quantum computer's ability.

Encryption and decryption are essential to secure data in the digital era. Encryption converts plaintext data into ciphertext using algorithms and keys, while decryption reverses this process, transforming ciphertext back into readable plaintext. Encryption has a long history, dating back to the Caesar cipher. With the Data Encryption Standard (DES) and the RSA algorithm, modern cryptography introduced public key cryptography in the 1970s. The emergence of the Internet has required more sophisticated algorithms including the Advanced Encryption Standard (AES) and elliptic-curve cryptography (ECC) for secure communication (Thales, 2024; National Academies of Science, Engineering, and Medicine, 2018).

As digital technologies are ubiquitous, the demand for robust encryption technologies is still increasing. Therefore, it is mandatory to develop quantum-resistant algorithms. In this article, we review the status and development of encryption technologies for quantum computing, which provides a basis to conduct related research.

2. Existing Encryption Technology

The purpose of encryption and decryption is to secure digital communication. Symmetric and asymmetric encryption are the basis of data protection, confidentiality, integrity, and authenticity. Encryption and decryption are performed using robust algorithms and cryptographic standards.

In encryption, plaintexts (readable data) are converted into ciphertexts (unreadable data) using an algorithm and a key to create confidentiality which allows only authorized parties or personnel to access the original data. In the conversion, each component of the plaintext is replaced with others. For example, in Caesar's cipher, each letter is shifted to a certain number of places in the alphabet order. In the Rail Fence cipher, the positions of components in the plaintext are changed according to a certain rule (Stallings, 2017). In confusion and diffusion, the relationship between the ciphertext and the encryption key is created as complex as possible. Thus, when changing one letter in the plaintext, many become changed in the ciphertext. Also, the influence of one symbol in the plaintext is exerted over ciphertext symbols to hide patterns, which makes the statistical analysis of ciphertext less useful (Shannon, 1949).

In symmetric-key encryption, the same key is used for both encryption and decryption to encrypt large data sets with secure key distribution efficiently. AES is used for secure key exchanges and digital signatures in symmetric-key encryption. In AES, a public and a private key are used for encryption and decryption, respectively. In decryption, ciphertext is converted back into plaintext using a decryption algorithm and a key. The original data is recovered by authorized users. In key-based decryption, symmetric and asymmetric key systems. While the same key used in encryption must be used for decryption in symmetric key systems, the private key must be kept secure in asymmetric-key systems. In key-based decryption, security depends on the key secret, and the holder of the private key can decrypt encrypted messages with the public key. In encryption and decryption, integrity and authentication are required. With integrity, the message is assured of its originality in transmission. Hash functions and checksums are also used other than encryption to keep integrity. Authentication refers to the verification of the identity of the user. Digital signatures created using asymmetric cryptography are mainly used for authentication (Kurose and Ross, 2016).

AES is the most widely used symmetric encryption algorithm and it was standardized by the National Institute of Standards and Technology (NIST) in 2001. It supports key sizes of 128, 192, and 256 bits to balance between security and performance. DES was an earlier standard with a 56-bit key length. However, DES is an insecure method nowadays. 3DES is, then, to improve security. In 3DES, the DES algorithm is applied three times with different keys at the same time. Symmetric-key cryptography is used in data storage, network security, and secure communications protocols such as Secure Sockets Layer (SSL)/ Transport Layer Security (TLS). SSL/TLS encrypts communications between a client and server, usually between web browsers and website applications. SSL encryption is more modern and secure while TLS encryption protects data on the Internet or a computer network (Daemen and Rijmen, 2002).

In asymmetric cryptography, RSA is used for secure data transmission as a public-key cryptosystem. ECC provides the same level of security as RSA but employs smaller key sizes. Thus, ECC is more efficient for mobile and embedded systems. Asymmetric cryptography is widely used in SSL/TLS, email encryption, and digital signatures (Rivest, et al., 1978; Koblitz, 1987). In hash functions of asymmetric cryptography, a fixed-size hash value is defined from input data of arbitrary size. Hash functions are used for data verification and password hashing. For has functions, Secure Hash Algorithms 2 and 3 (SHA-2 and SHA-3) are used. SHA-2 includes variants of SHA-256 and SHA-512, while SHA-3 is the latest standard. Hash functions are used in digital signatures, certificates, and blockchain technology (Eastlake and Hansen, 2011).

3. Encryption Technology for Quantum Computing

Quantum computers make current encryption methods obsolete, posing significant security risks. Therefore, it is needed to develop quantum-resistant encryption technologies to protect sensitive information on finance, healthcare, and national security.
Quantum Key Distribution (QKD) is a promising quantum cryptographic method. QKD is based on quantum mechanics to safely allocate encryption keys. Protocols such as BB84 are used based on the no-cloning theorem and quantum entanglement to ensure secure key exchange by detecting malicious attempts. The most popular protocol, BB84, was developed by Bennett and Brassard (1984). QKD prevents intercepts or copying of the quantum states to avoid the transmission of the the key. QKD is applied in secure communications of the financial industry and government networks. Companies such as ID Quantique and Toshiba have already developed commercial QKD systems. The security of QKD relies on how well it detects eavesdropping attempts, which are identified with quantum state disturbances. The use of QKD is limited by distance. It also requires specific hardware. However, no known quantum algorithm can break QKD without being detected, which makes QKD a prominent candidate (Lai et al., 2008; Toshiba, 2024; Sundar, 2024).

Quantum-resistant cryptography includes lattice-based, hash-based, code-based, and multivariate polynomial cryptography. NIST is currently standardizing Quantum-resistant cryptographic algorithms to replace present public-key cryptosystems such as

RSA and ECC, which can be decrypted by quantum computers This cryptography enables the development of protocols that resist quantum attacks.

Lattice-based cryptography uses cryptographic algorithms based on the hardness of lattice problems. Lattice problems are resistant to attacks by quantum computers. Lattice-based cryptography allows for functionalities, including public-key encryption, digital signatures, and homomorphic encryption. Lattice-based cryptography is considered a cryptography standard for quantum computing by the National Institute of Standards and Technology (NIST) (Schneier, 2024; Yu, 2021). Lattice-based cryptography is resistant to quantum attacks as quantum algorithms that can solve lattice problems faster than classical computers are not created yet. However, the efficiency and long-term security of lattice-based cryptography need to be enhanced for widespread use (Sabani et al., 2023; Asif, 2021).

Code-based cryptography employs error-correcting codes. The most studied scheme is the McEliece cryptosystem which withstands cryptanalytic attacks. Code-based cryptography is also part of NIST's post-quantum cryptography standards and is evaluated for its efficiency and security. The size of code-based cryptography is larger than others, which influences the performance of a system. Thus, it is necessary to reduce the size and optimize code-based cryptography for widespread use (Singh, 2022).

Quantum computing can be a threat to existing encryption methods. Therefore, research and development in quantum-resistant encryption technologies are mandatory for secure communication. QKD and various post-quantum cryptography are promising in terms of security against quantum attacks. Continuous research is mandatory to solve practical problems and make relevant technologies remain secure as quantum computing is expected to develop continuously. The outcomes of the continuous research on encryption technology against the attacks of quantum computers are expected to be obtained soon. Such outcomes include robust quantum-resistant algorithms, widespread adoption of QKD, and innovative cryptographic protocols (Kirsch, 2015; Baseri et al., 2024; Anderson, 2024; Savage, 2023).

Such research results on encryption for quantum computing can enhance cybersecurity by strengthening the security framework for the digital economy and be the basis for the formulation of cryptographic standards. Advanced technologies based on the research outcome contribute to secure communication and technological innovation through the development of new cryptographic methods and quantum technologies. While the development of quantum computing poses challenges and opportunities for cryptography technology, continuous research and development of encryption are needed regarding the security threats from the use of quantum computing (Baseri et al., 2024; Ahmed, 2024).

4. Future Development of Quantum Computing and Encryption Technology

The development of quantum computing and encryption technology provides implications for computing, data security, and cryptography. Quantum computing allows for unprecedented computing speed to solve complex and specific problems faster than conventional computers. Such advantages require error correction and stability in computing as the quantum computer is susceptible to noise and errors. Error correction technology is important to sustain the stability and reliability of quantum computations. For effective error correction, surface codes and topological qubits are researched extensively. In quantum computing, it is not easy to use more qubits without losing coherence. Thus, superconducting qubits, trapped ions, and topological qubits are being developed for a large quantum computer (Arute et al., 2019; Preskill, 2018; Fowler et al., 2012; IBM, 2023). Algorithms must be developed for quantum computing depending on various demands. Shor's and Grover's algorithms are the fundamental ones but new algorithms are demanded and existing algorithms must be ones for diverse applications. With such algorithms, quantum networks need to be developed to connect multiple quantum computers to form a quantum internet for secure communication using QKD and other protocols (Wehner et al, 2018; Pirandola, 2020). As mentioned above, post-quantum cryptography is necessary to mitigate the risks of using RSA and ECC such as QKD and homomorphic encryption algorithms. Such algorithms are mandatory to secure the security of blockchain technology as it is vulnerable to quantum attacks (Aggarwal et al., 2018). As data privacy concerns increase, multi-party computation and differential privacy also need to be developed for effective data protection. With quantum computing, many existing encryption algorithms can be cracked, so it is necessary to develop cryptographic algorithms that are resistant to quantum computing attacks. In the future, it will be important to standardize and promote these quantum-resistant encryption algorithms. In addition to post-quantum cryptography, other cryptographic protocols and technologies may emerge such as homomorphic encryption to allow computation on encrypted data and zero-knowledge proofs to ensure data privacy. These technologies are expected to improve data privacy and security. QKD is a secure communication technology based on the principle of quantum mechanics for the absolute security of information. In the future, QKD technology is likely to be commercialized and play an important role in secure communications at the national and enterprise levels. As technology evolves, encryption technology will become more widespread and standardized to keep personal and business data safe which requires the popularization and standardization of encryption technology.

Quantum computing and encryption technology are intertwined driving innovations of each other. As quantum computing matures, new encryption technology must be developed to ensure data security. Innovations in encryption technology help secure communications on the quantum network. It is necessary to establish a global collaborating scheme between academia and industry to utilize the potential of quantum computing (Dwork and Roth, 2014).

Author Contributions: Conceptualization, Y. Lee and T. Nam.; investigation, Y. Lee, T. Nam and S. Yune; writing—original draft preparation, Y. Lee and S. Yune.; writing—review and editing, Y. Lee and T. Nam;

Funding: This research did not receive external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Aggarwal, D.; Brennen, G. K., Lee, T., & Santhaet, M. (2018). Quantum attacks on Bitcoin, and how to protect against them. *Ledger*, *3*, 41–62. http://dx.doi.org/10.5195/LEDGER.2018.127.
2. Ahmed, U., Sipola, T., & Hautamäki, J. (2024). Cyber Protection Applications of Quantum Computing: A Review. *Proceedings of the 23rd European Conference on Cyber Warfare and Security*, *23(1)* https://doi.org/10.34190/eccws.23.1.2182.
3. Analytics Insight. (2023). Quantum Computing Impact on Cybersecurity Sector. Available online: https://www.analyticsinsight.net/cyber-security/quantum-computing-impact-on-cybersecurity-sector. (accessed on September 22, 2024).
4. Anderson, Margo. Quantum Cryptography Has Everyone Scrambling China, India, the EU, and the US are all pursuing divergent approaches. *IEEE Spectrum*. Available online: https://spectrum.ieee.org/quantum-key-distribution. (accessed on September 22, 2024).
5. Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, Joseph C.; Barends, R.; Biswas, R.; Boixo, S.; Fernando G.S.L.; Buell, D. A. et al. (2019). Quantum supremacy using a programmable superconducting processor, *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5.
6. Asif, Rameez. (2021). Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. *IoT, 2*. 71–91. https://doi.org/10.3390/iot2010005
7. Baseri, Yaser, Chouhan, Vikas, & Ghorba, Ali. Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure. https://doi.org/10.48550/arXiv.2404.10659.
8. Bennett, Charles H., & Brassard, Gilles. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theoretical Computer Science*, *560*, 75–179. http://dx.doi.org/10.1016/j.tcs.2011.08.039.
9. Caltech. (2024). How Will Quantum Technologies Change Cryptography? Available online: https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography. (accessed on September 22, 2024).
10. Daemen, J., & Rijmen, V.. (2002). The Design of Rijndael. : AES - The Advanced Encryption Standard. Available online:http://dx.doi.org/10.1007/978-3-662-04722-4. (accessed on September 22, 2024).
11. Di M.; Alberto, J., Karl, T., Ivano, A., Constantia, A., Srinivasan, B., Christian W., Borras, K., Carrazza, S., Crippa, A., et al. (2024). Quantum Computing for High-Energy Physics: State of the Art and Challenges. *PRX Quantum: a Physical Review Journal*, *5*(3). https://link.aps.org/doi/10.1103/PRXQuantum.5.037001.
12. Dwork, C., &Roth, Aaron. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*. *9(3-4)*, 211–407. https://doi.org/10.1561/0400000042.
13. Eastlake, D. & T. Hansen, US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). *RFC 6234 2011*. https://doi.org/10.17487/RFC6234.
14. Feynman, Richard P. (1982). Simulating Physics with Computers. *International Journal of Theoretical Physics*, 21, 467–488. https://doi.org/10.1007/BF02650179.
15. Flöther, Frederik F. (2023). The state of quantum computing applications in health and medicine. *Research Directions: Quantum Technologies*. http://dx.doi.org/10.1017/qut.2023.4.
16. Fowler, Austin G., Mariantoni, Matteo, Martinis, John M., Cleland, & Andrew N. (2012). Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, *86*(3), 032324. http://dx.doi.org/10.1103/PhysRevA.86.032324.
17. Advances and open problems in federated learning. Available online: https://www.researchgate.net/publication/337904104_Advances_and_Open_Problems_in_Federated_Learning . *(*accessed on September 22, 2024).

18. IBM. A Brief History Of Cryptography: Sending Secret Messages Throughout Time. Available online: https://www.ibm.com/blog/cryptography-history/ (accessed on August 11, 2024).
19. IBM. The Future of Computing Is Quantum-centric. Available online: https://www.ibm.com/roadmaps/quantum/. (accessed on August 11, 2024).
20. Kirsch, Zachary J., & Chow, Ming. Quantum Computing: The Risk to Existing Encryption Methods. Available online: https://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf. (accessed on August 11, 2024).
21. Koblitz, N. (1978). Elliptic curve cryptosystems. *Mathematics of Computation, 48(177)*, 203–209. https://doi.org/10.1090/S0025-5718-1987-0866109-5.
22. Kurose, James, & Ross, Keith. Computer Networking: A Top-Down Approach. London, UK: Pearson.
23. Lai, J., Yao, F., Wang, J., Zhang, M., Li, F., Zhao, W., & Zhang, H. (2023). Application and Development of QKD-Based Quantum Secure Communication, *25(4)*, 627. https://doi.org/10.3390/e25040627.
24. National Academies of Sciences, Engineering, and Medicine. (2018). Encryption and Its Applications. In Decrypting the Encryption Debate: A Framework for Decision Makers. Available online: https://doi.org/10.17226/25010. (accessed on August 11, 2024).
25. Pirandola, U.L; Stefano, A.; Banchi, L.; & Berta, M. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, *12*(4), 1012–1236. http://dx.doi.org/10.1364/AOP.361502
26. Pixelplex. 9 Promising Quantum Computing Applications: Breaking Barriers in Scientific Research. Available online: https://pixelplex.io/blog/quantum-computing-applications/. (accessed on September 22, 2024).
27. Preskill, John. Quantum computing in the NISQ era and beyond. *Quantum* 2018, *2*, 79. http://dx.doi.org/10.22331/q-2018-08-06-79.
28. Rivest, R.L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 1978, *21*(2), 120–126. https://doi.org/10.1145/359340.359342.
29. Savage, Neil. Keeping secrets in a quantum world: Cryptographers are preparing for new quantum computers that will break their ciphers. Available online: https://www.nature.com/articles/d41586-023-03336-4. (accessed on September 22, 2024).
30. Schneier, Bruce. Lattice-Based Cryptosystems and Quantum Cryptanalysis. Communications of the ACM 2024. Available online: http://dx.doi.org/10.1145/3665224. (accessed on September 22, 2024).
31. Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *The Bell System Technical Journal, 28(4)*, 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.
32. Shor Peter. (1997). Polynomial-time algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*. Available online: https://doi.org/10.1137/S0097539795293172 (accessed on September 22, 2024).
33. Shor, Peter. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science, USA, November 22, 124–134.
34. Singh, Manoj Kumar. (2022). Code-Based Cryptography: A Comparative Study of Key Sizes. In *Advanced Communication and Intelligent Systems*. Proceedings of ICACIS 2022 Communications in Computer and Information. R.N Science: Berlin/Heidelberg, Germany,https://doi.org/10.1007/978-3-031-25088-0_32.
35. Stallings, William. (2003). Cryptography and Network Security: Principles and Practice. Available online: https://www.researchgate.net/publication/243772991_Cryptography_and_Network_Security_Principles_And_Practices. (accessed on September 22, 2024).
36. Subramanian, R. B., Siva, T., Maheswari, P., Nithya, M., Girija, Karthikeyan, & T. Saraswathi, (2024). Quantum Computing: Unveiling the Paradigm Shift and Diverse Applications.Available online: http://doi.org/10.4018/979-8-3693-1168-4.ch006. (accessed on September 22, 2024).
37. Sundar, K., S., Sasikumar, & C. Jayakumar, (2024). Efficient and Secure Long-Distance Quantum Key Distribution by using a Proxy Encryption Scheme. *Multimedia Tools and Applications*, *83*, 80285–80298. https://doi.org/10.1007/s11042-024-18835-3.
38. Terhal. (2015). Barbara Quantum error correction for quantum memories. *Reviews of Modern Physics*, *87(2)*, 307. http://dx.doi.org/10.1103/RevModPhys.87.307.
39. Thales. A Brief History Of Encryption (And Cryptography). Available online: https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption. (accessed on September 22, 2024).
40. Toshiba. Quantum Key Distribution (QKD). Delivering Provably Secure Networking For The Quantum Computing Age. Available online: https://www.toshiba.eu/solutions/quantum/products/quantum-key-distribution/. (accessed on September 22, 2024).
41. Wehner, Stephanie, Elkouss, Davis, & Hanson, Ronald. (2018). Quantum internet: A vision for the road ahead. *Science*, *362*, 6412. https://doi.org/10.1126/science.aam9288.

42. Yu, Y. (2021). Preface to Special Topic on Lattice-based Cryptography. *National Science Review*, *8*(9), nwab154. https://doi.org/10.1093/nsr/nwab154.