Quantum DNA Partial Permutation-based Secure Encryption Scheme

Esmot Ara Tuli, and Dong-Seong Kim
Networked Systems Laboratory, Department of IT Convergence Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
(esmot, and dskim)@kumoh.ac.kr

***Abstract*—The rapid development of quantum hardware puts classical encryption techniques at risk of quantum attacks. Therefore, the development of post-quantum encryption techniques is indispensable. This paper proposes a quantum-enabled encryption technique based on DNA coding called QDPP. Here, information is first encoded as a DNA sequence, and then partial permutation is performed on the information as a sequence of blocks. Theoretically, our proposed method is secure against both classical and quantum attacks, offering a potential solution to the vulnerabilities exposed by quantum computing.**

***Index Terms*—Post-quantum cryptography, quantum cryptography, permutation, DNA coding, bio-inspired.**

I. Introduction

The rapid advancement of quantum hardware and algorithms suggests that the transition from the noisy intermediate-scale quantum (NISQ) era to the fault-tolerant quantum computer (FTQC) era is imminent. However, this progress poses a significant threat. Quantum algorithms like Grover's and Shor's algorithms could disrupt current cryptosystems, blockchain, financial systems, and security mechanisms. This event is referred to as Q-Day [1]. In 2014, the National Institute of Standards and Technology (NIST) projected that a quantum computer capable of breaking RSA could be developed by 2030 [2]. Subsequently, in 2015, the National Security Agency (NSA) cautioned that the progress in quantum computing had reached a stage where organizations should begin deploying encryption algorithms designed to resist attacks by quantum computers [3]. At the current stage of quantum computer development, a concerning attack associated with quantum computing is the store-now-decrypt-later (SNDL) attack. This type of attack collects encrypted data that obtained illicitly, with the intention of decrypting it in the future when a sufficiently powerful quantum computer becomes available [4].

Post-quantum cryptography is classified into two categories: quantum-enabled cryptography and quantum-resistant cryptography. Quantum-resistant encryption schemes cannot guarantee their security against sufficiently powerful quantum computers, thus, it is prudent to consider quantum-enabled encryption. The first quantum-enabled encryption algorithm proposed was quantum key distribution (QKD) by Bennett and Brassard. Subsequently, various other quantum-enabled encryption algorithms have been proposed, such as quantum superdense coding, quantum permutation pad, quantum secret sharing, and others. [5],[6].

Adleman's seminal work marked the inception of DNA (deoxyribonucleic acid) computing, wherein DNA molecules were employed to tackle a directed Hamiltonian path problem [7]. Subsequently, numerous scholars have utilized DNA coding algorithms for encryption purposes. DNA sequences adopt a double-helical structure through the arrangement of adenine (A), guanine (G), cytosine (C), and thymine (T) nucleotides in diverse combinations.This bio-inspired concept has found applications in DNA permutation, addition, XOR operations, as well as encoding and decoding procedures.

II. Proposed System Model

The proposed encryption model is shown in Figure 1. Suppose two parties, wants to share secret information using QDPP encryption scheme. The corresponding steps of encoding and decoding message is given below:

1) First, the sender and receiver share the DNA Mapping table and Rules table shown in Figure 1 (B) and (C) via secure quantum channel. As seen in (B), the QDPP scheme takes two bits to make one nucleotide.
2) Each pair of bits is mapped to a corresponding nucleotide according to Table (b).
3) The information is then converted into a classical bit of N. Later the bit is divided into k blocks as $k = N\%i$, where i represents the number of bits in each block and even number as shown in (A).
4) Then the information block is converted into qubit. This work utilised the Pauli operator on a different basis. The Pauli matrices (X, Y, and Z) represent rotations around the X, Y, and Z axes of the Bloch sphere, respectively. When combined with arbitrary unitary operations, any point on the Bloch sphere representing a single-qubit state can be reached. Qubit blocks are later encrypted using permutation using one of the basis and corresponding rules from Figure 1(C). For example, if $\downarrow$ is selected, then the corresponding rule "ACGT" is used to encryption key where "ACGT"=00011011. The encrypted message is then sent to the receiver along with the basis.
5) At the receiver side, where the Rules table is already given. Therefore, according to the qubit basis, reciever

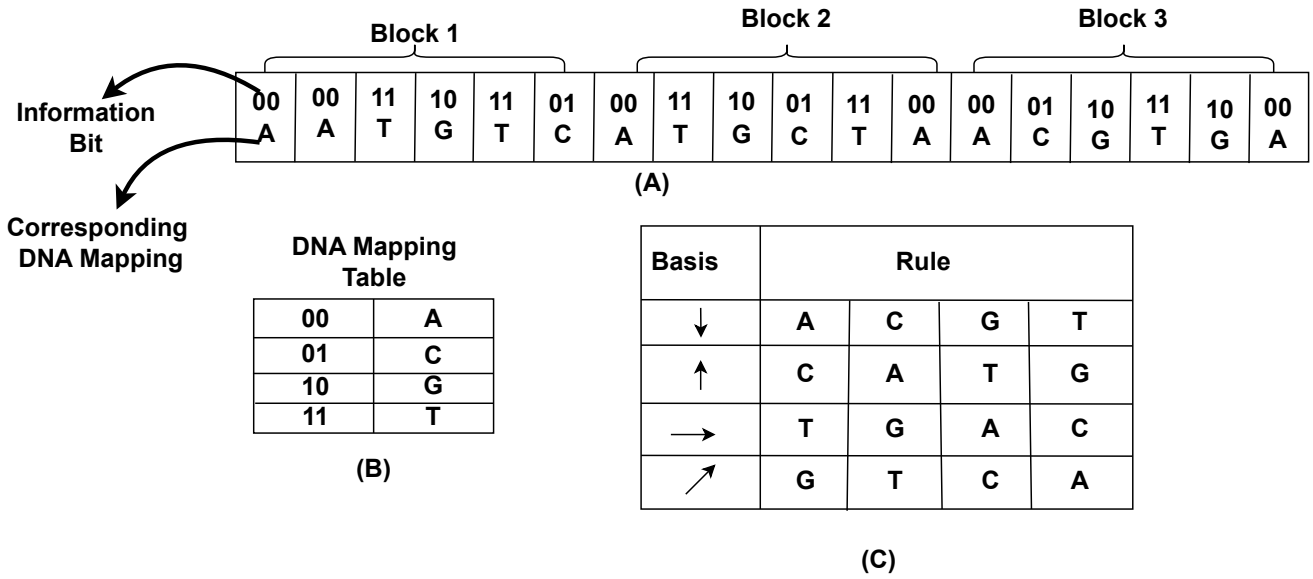

Fig. 1: Syetem diagram for QDPP encryption

decrypt the information by inverse permutation and the DNA sequence key from Rule table.

.

III. Security Analysis

A. Outside attack

Proposed QDPP encryption scheme is designed to resist external attacks through a multi-layered security approach. Information is not transmitted as a single block; instead, it is segmented into distinct blocks. Each block undergoes encryption using a unique basis (the reference frame for quantum states) and a corresponding key. This dynamic assignment of bases and keys for every block ensures that even if an attacker manages to compromise one block, they cannot leverage that knowledge to decipher other blocks. The continuous variation of keys and bases adds another layer of complexity, making it computationally infeasible for an attacker to guess or predict the correct combinations for the remaining encrypted blocks. Therefore, the system's security is significantly enhanced due to the independent and unpredictable nature of each block's encryption parameters.

IV. Conclusion

In this paper, we have introduced QDPP, a novel quantum-enabled encryption scheme based on DNA coding and partial permutation. The proposed system demonstrates theoretical resilience against both classical and quantum attacks, offering a promising solution to the looming threat of quantum computing to current cryptographic standards. By encoding information into DNA sequences and employing dynamic block-wise permutation with varying bases and keys, QDPP introduces a multi-layered security approach that significantly complicates unauthorized decryption attempts.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization programme through the Institute of IITP grant funded by the Korean government (MSIT) (IITP-2024-2020-0-01612, 50%) and by Priority Research Centres Programme through the NRF funded by the MEST (2018R1A6A1A03024003, 50%)

References

[1] E. A. Tuli, J.-M. Lee, and D.-S. Kim, "Integration of quantum technologies into metaverse: Applications, potentials, and challenges," *IEEE Access*, vol. 12, pp. 29 995–30 019, 2024.

[2] S. Grobman, "Quantum computing's cyber-threat to national security," *PRISM*, vol. 9, no. 1, pp. 52–67, 2020.

[3] J. R. Lindsay, "Surviving the quantum cryptocalypse," *Strategic Studies Quarterly*, vol. 14, no. 2, pp. 49–73, 2020.

[4] B. Halak, T. Gibson, M. Henley, C.-B. Botea, B. Heath, and S. Khan, "Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices," *IEEE Access*, vol. 12, pp. 8791–8805, 2024.

[5] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical computer science*, vol. 560, pp. 7–11, 2014.

[6] E. Ara Tuli, M. Golam, J.-M. Lee, and D.-S. Kim, "Quantum superdense coding-based secure authentication for military metaverse," in *Proceedings of the 2024 Winter Conference of the Korea Institute of Communication Sciences*. Seoul, South Korea: Korea Institute of Communication Sciences, 2024, pp. 835–836.

[7] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *science*, vol. 266, no. 5187, pp. 1021–1024, 1994.