Optimized Quantum Circuit

Implementation of HQC Core Arithmetic

Sejin Lim, Kyungbae Jang, Yujin Yang, Yujin Oh, and Hwajeong Seo

Abstract—As the development of quantum computers progresses rapidly, there is a growing concern about the weakening and eventual obsolescence of traditional encryption methods due to accelerated computation and the Shor algorithm. To address this challenge, NIST has organized a competition to develop post-quantum cryptography, focusing on encryption schemes that are resistant to attacks by quantum computers. To assess the security strength of encryption algorithms on quantum computers, it is necessary to implement the encryption process as quantum circuits. This paper proposes an optimized quantum circuit implementation for the key generation and encoding operations of HQC (Hamming Quasi-Cyclic), which is one of the fourth-round candidate algorithms in the aforementioned competition organized by NIST. The key focus is on optimizing the binary field arithmetic, which plays a crucial role in these operations. The paper presents a quantum circuit implementation that is tailored for HQC, aiming to reduce the required resources for efficient execution. Additionally, the paper performs resource estimation to evaluate the required quantum resources for implementing HQC.

Research Keywords— PQC, Code-based Cryptography, Quantum Circuit, Optimization
 Published by the Institution of Creative Research Professionals

- *Sejin Lim is with the Division of IT Convergence Engineering, Hansung University, Seoul, 02876. E-mail: dlatpwls834@gmail.com*
- *Kyungbae Jang is with the Division of IT Convergence Engineering, Hansung University, Seoul, 02876. E-mail: starj1023@gmail.com*
- *Yujin Yang is with the Division of IT Convergence Engineering, Hansung University, Seoul, 02876. E-mail: yujin.yang34@gmail.com*
- *Yujin Oh is with the Division of IT Convergence Engineering, Hansung University, Seoul, 02876. E-mail: oyj0922@gmail.com*
- *Hwajeong Seo (corresponding author) is with the Division of IT Convergence Engineering, Hansung University, Seoul, 02876. E-mail: hwajeong84@gmail.com*

1 INTRODUCTION

Quantum computers, based on quantum mechanics, offer rapid computational speeds through superposition and entanglement. However, these capabilities pose a threat to symmetric and public key cryptography. The Shor algorithm, specifically designed for quantum computers, can efficiently break the mathematical problems underlying public key cryptography. To address this challenge, NIST is organizing a competition to standardize post-quantum cryptography, ensuring secure public key algorithms in the face of practical quantum computers.

This paper focuses on HQC (Hamming Quasi-Cyclic) [1], a code-based cryptographic algorithm, and proposes an optimized quantum circuit implementation for binary field arithmetic, which is essential for key generation and encoding. The goal is to estimate the required quantum resources for HQC's quantum circuit implementation, contributing to the analysis of its security strength.

2 BACKGROUND

2.1 HQC

HQC is a code-based encryption scheme that utilizes the Hamming metric and random Quasi-Cyclic codes. Quasi-Cyclic codes are designed to have a cyclic relationship among some of the matrix rows, enabling efficient computations. By exploiting this property, only the first row needs to be stored, reducing the key size efficiently. The encryption process of HQC consists of key generation, where a public key $pk = (h, s)$ and a secret key $sk = (x, y)$ are generated, encoding, which generates the ciphertext $ct = (u, v)$ from the message m, and decoding, which recovers the message by removing the error e from the ciphertext. In binary field arithmetic, a primitive polynomial $\mathbb{F}_2^n/((X^n - 1)/(X - 1))$ is used, where n must be a prime number. For hqc-128, n is set to 17669, and based on the factorization property in the equation, $\mathbb{F}_{2^{17668}}/(X^{17668} + X^{17667} + \cdots + X + 1))$ is used. Due to the large magnitude of the errors introduced during encoding, direct decoding is impossible. Only users with the secret key can reduce the errors and perform the decoding process easily. The decoding process may have a probability of failure, but the HQC paper provides detailed mathematical analysis demonstrating that the failure probability is negligible. Consequently, HQC offers a high level of security. Unlike many code-based encryption schemes that introduce vulnerabilities during the transformation of the code's generator matrix to achieve randomness, HQC avoids this issue by using the generator matrix code in its original form. This ensures that there are no structural weaknesses in the code-based approach. This is a significant advantage and characteristic of HQC.

3 QUANTUM IMPLEMENTATION OF HQC

The key generation in HQC involves calculating $s \leftarrow x + hy$ for the given x, y, and h, which all exist in the same binary field. Similarly, the encoding process takes place in the same binary field and involves calculating $u \leftarrow r_1 + hr_2$ and $v \leftarrow mG + sr_2 + e$, where r_1 and r_2 are also in the binary field. It can be observed that both the key generation and encoding steps are performed through multiplication and addition operations in the binary field. For hqc-128, the operations are carried out in the binary field of $\mathbb{F}_{2^{17668}}$. However, for the binary field of size 2^{17668}, quantum simulation is not possible. Therefore, in this paper, the binary field is reduced to 2^{12} for the implementation of quantum circuits and resource estimation. The choice of primitive polynomial aligns with the formula mentioned in the HQC paper.

The addition operation can be implemented with a depth of 1 by using *CNOT* gates of the same size as the field. However, the multiplication operation, which is performed through AND operations and XOR operations for modular reduction, requires high computational complexity in binary field arithmetic. In a binary field of size n, Schoolbook multiplication requires n^2 AND operations. In quantum circuits, the AND operation is implemented using Toffoli gates, and the T gates used in Toffoli gate implementation are costly. Therefore, optimizing multiplication operations in the binary field is crucial. In this paper, we applied the most efficient quantum multiplication technique [2] in terms of Toffoli-depth and Full-depth. This technique recursively applies the Karatsuba algorithm, which reduces the complexity of multiplication by performing additional additions.

By introducing additional qubits to remove the dependencies between multiplication factors and optimizing for Toffoli-depth 1, the multiplication circuit is optimized regardless of the field size. As a result, the overall depth can be significantly reduced. While there is a trade-off between the number of qubits and depth, for HQC with large field size, the multiplication circuit with Toffoli-depth 1 is considered the most suitable for our implementation.

Table 1 presents the results of implementing the core arithmetic of addition and multiplication in the reduced binary field $\mathbb{F}_{2^{12}}$ for both key generation and encoding steps.

Table 1. Quantum circuit implementation in $\mathbb{F}_{2^{12}}$

Step	Qubits	Clifford gates	T gates	T-depth	Full-depth
KeyGen	174	939	378	4	40
Encoding	234	1968	756	8	72

4 ACKNOWLEDGEMENTS

This work was supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (<Q|Crypton>, No.2019-0-00033, Study on Quantum Security Evaluation of Cryptography based on Computational Quantum Complexity, 50%) and this work was supported by Institute for Information & communications Technology Promotion(IITP) grant

funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 50%).

REFERENCES

[1] Jang, Kyungbae, et al. "Optimized implementation of quantum binary field multiplication with toffoli depth one." International Conference on Information Security Applications. Cham: Springer Nature Switzerland, 2022.

[2] Melchor, Carlos Aguilar, et al. "Hamming quasi-cyclic (HQC)." NIST PQC Round 2.4 (2018): 13.