Quantum Implementation of Core Operations in Classic McEliece

1st Yujin Oh
IT Department
Hansung University
Seoul, South Korea
oyj0922@gmail.com

2nd Kyungbae Jang
IT Department
Hansung University
Seoul, South Korea
starj1023@gmail.com

3rd Sejin Lim
IT Department
Hansung University
Seoul, South Korea
dlatpwls83484@gmail.com

4th Yujin Yang
IT Department
Hansung University
Seoul, South Korea
yujin.yang34@gmail.com

5th Hwajeong Seo
IT Department
Hansung University
Seoul, South Korea
hwajeong84@gmail.com

***Abstract*—If large-scale quantum computers capable of running quantum algorithms are developed, it is expected that powerful quantum cryptanalysis will become possible. To establish secure quantum-resistant encryption systems, it is necessary to evaluate the quantum security of cryptographic algorithms. As a result, various quantum cryptanalysis research studies have been published, and implementation techniques that minimize the resources required for analyzing encryption have been proposed.**

In this paper, we present an efficient quantum circuit implementation of Classic McEliece, which is one of the candidate algorithms in the NIST Post-Quantum Cryptography Standardization Round 4. We optimize the encoding, and decoding operations of Classic McEliece on quantum circuits, with a specific focus on binary field arithmetic, linear operations, and the Berlekamp-Massey decoding quantum circuit.

***Index Terms*—Quantum Cryptanalysis , Quantum Circuit , Berlekamp-Massey, Code-based Cryptography.**

I. Introduction

Quantum cryptanalysis is an active research field in recent years as the development and interest in quantum computers is growing. The Grover search algorithm [1] and the Shor algorithm [2] are representative quantum algorithms used in quantum cryptanalysis. The Grover search algorithm reduces the brute force complexity to the square root of symmetric key cryptography. Another quantum algorithm, the Shor algorithm, threatens public key cryptography systems. The famous public key ciphers RSA and ECC (Elliptic Curve Cryptography) are based on security based on factoring and discrete logarithm problems that are difficult to solve on classical computers.

Therefore, PQC (post-quantum cryptography) that can replace RSA and ECC is needed, which is different from the case that can counter the Grover search algorithm by increasing the key length. In this situation, NIST (National Institute of Standards and Technology) has hosted a PQC contest and several algorithms have been selected for standardization. In addition, as the fourth round proceeds, additional algorithms are expected to be standardized. As such, quantum computers, which take a different approach from classical computers to certain problems, have an unprecedented impact on cryptography community. For cryptanalysis on a quantum computer, the analysis technique and the core operations of the target cipher must be implemented as a quantum circuit. In order to find the key using the Grover search algorithm, the encryption of the target cipher must be implemented as a quantum circuit [3]. For the Shor algorithm, the modular exponential of RSA and scalar multiplication on an elliptic curve must be implemented as a quantum circuit [4], [5]. In quantum cryptanalysis, these quantum circuits are essential and efficient implementation to reduce the required quantum resources (e.g., qubit count, quantum gates, circuit depth) is also important.

In this paper, we present a quantum circuit for the encoding and the Berlekamp-Massey algorithm [6] of decoding, used in the code-based cipher Classic McEliece [7]. We use the binary field quantum multiplication technique from WISA'22 [8] in the proposed Berklemp-Massey's quantum circuit.

A. *Our Contribution*

Contributions of this paper are:

1) **Quantum circuit of the encoding using three method.** We use the three method to implement the matrix-vector multiplication of the encoding in Classic McEliece and compare the resources of them.
2) **Quantum circuit of the Berlekamp-Massey algorithm.** We present for the first time a quantum circuit of the Berlekamp-Massey decoding algorithm, the core operation of Classic McEliece.
3) **Efficient quantum implementation with WISA'22 quantum multiplication** We use the technique of [8] to implement binary field multiplication and inverse operation, which are key operations in the Berlekamp-Massey decoding algorithm. Through this, our proposed quantum circuit provides relatively low T-depth and full depth.

The contents of the paper are as follows. Section II describes the quantum gates used in this work and the code-based cipher Classic McEliece. In Section III, the quantum circuit implementation of the proposed method is described. In Section IV, the quantum resources required for the quantum circuit in Section III are estimated and the performance is evaluated. Finally, we conclude this paper in Section V.

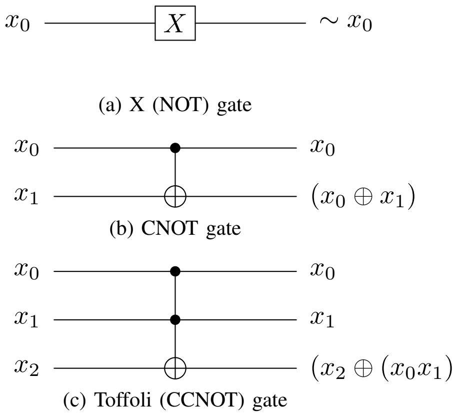
II. Background

A. *Classic McEliece*

Classic McEliece [7] is a code-based cipher using the Goppa code and is currently one of the NIST Round 4 candidate algorithms. It is the Niederreiter system that uses the parity check matrix generated from the Goppa code as a public key. A ciphertext is a syndrome value computed by multiplying a public key, a parity check matrix, and a secret information, a low-weight vector. For decryption, the syndrome value is decoded using a private key (monic polynomial and field elements used to generate the public key) and a decoder. By performing syndrome decoding, a low-weight vector is recovered from the syndrome value.

B. *Quantum Gates*

This section describes the X, CNOT, and Toffoli gates, which are quantum gates used in the proposedBerlekamp-Massey quantum circuit. The X gate operates on a single qubit and inverts the value. In the X gate in Figure 1, the value of x_0 is inverted. The CNOT gate operates on two qubits and performs an XOR operation. In the CNOT gate of Figure 1(b), x_0 is XORed to x_1. The Toffoli gate operates on three qubits and performs an AND operation. In the Toffoli gate of Figure 1(c), x_0x_1 is XORed to x_2.



(a) X (NOT) gate

(b) CNOT gate

(c) Toffoli (CCNOT) gate

Fig. 1: Quantum gates.

III. Proposed Method

We implement the quantum circuit of the encoding and the Berlekamp-Massey decoder used in Classic McEliece. In the encoding of Classic Mceliece, the matrix - vector multipliacation are required. Furthermore, in the Berlekamp-Massey decoder of Classic McEliece, multiplication and inversion of binary field $\mathbb{F}_{2^{12}}$ or $\mathbb{F}_{2^{13}}$ are required. We use the technique of WISA'22 for the quantum circuit of $\mathbb{F}_{2^{12}}, \mathbb{F}_{2^{13}}$ multiplication. For the inversion quantum circuit of $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{2^{13}}$, we implement it using the Itoh-Tsujii method (multiplications + squarings).

A. Quantum Binary Field Multiplication

The multiplication technique of [8] is optimized with a Toffoli depth of one for any field size. This optimization is achieved by the recursive application of the Karatusba algorithm and the allocation of additional ancilla qubits. Through recursive application of the Karatsuba algorithm, all the AND operations involved in multiplication become independent. Furthermore, allocating additional ancilla qubits allows for the operation of all Toffoli gates in parallel, resulting in a Toffoli depth of one. We apply this technique to implement the multiplication of fields $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{2^{13}}$, used in the Berlekamp-Massey decoding algorithm of Classic McEliece.

Table I shows quantum resources for the quantum multiplication circuit of $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{2^{13}}$ implemented by the technique of [8]. Although the implementation requires relatively many qubits, we can use quantum multiplication with very low full depth and optimized Toffoli depth.

TABLE I: Quantum resources for the quantum multiplication circuit of $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{2^{13}}$.

Binary Field	#Clifford	#T	T-depth	#Qubits	Full depth
$\mathbb{F}_{2^{12}}$	761	378	4	162	37
$\mathbb{F}_{2^{13}}$	966	462	4	198	54

B. Quantum Binary Field Inversion

We implement the Itoh-Tsujii based binary field inversion as a quantum circuit. For the inversion of $\mathbb{F}_{2^n}$, it is implemented with multiplications and squarings for $x^{-1} = x^{2n-2}$. Algorithm 1 describes the implementation of the inversion quantum circuit of $\mathbb{F}_{2^{12}}$ and Table II shows quantum resources for the quantum inversion (i.e., Algorithm 1).

Algorithm 1 Inversion quantum circuit of $\mathbb{F}_{2^{12}}$

```
Input: 12-qubit $x$, 12-qubits $temp_{0\sim6}$, ancilla qubits $ac$
Output: $x^{-1}$
$temp_0 \leftarrow$ CNOT32($x$, $temp_0$)
$temp_0 \leftarrow$ Squaring($temp_0$)
$temp_1 \leftarrow$ Multiplication($x$, $temp_0$, $ac$)
$temp_2 \leftarrow$ CNOT32($temp_1$, $temp_2$)
$temp_1 \leftarrow$ Squaring($temp_1$)
$temp_1 \leftarrow$ Squaring($temp_1$)
$temp_3 \leftarrow$ Multiplication($temp_2$, $temp_3$, $ac$)
$temp_4 \leftarrow$ CNOT32($temp_3$, $temp_4$)
$temp_3 \leftarrow$ Squaring($temp_3$)
$temp_3 \leftarrow$ Squaring($temp_3$)
$temp_3 \leftarrow$ Squaring($temp_3$)
$temp_3 \leftarrow$ Squaring($temp_3$)
$temp_5 \leftarrow$ Multiplication($temp_3$, $temp_4$, $ac$)
$temp_5 \leftarrow$ Squaring($temp_5$)
$temp_5 \leftarrow$ Squaring($temp_5$)
$temp_6 \leftarrow$ Multiplication($temp_2$, $temp_5$, $ac$)
$temp_6 \leftarrow$ Squaring($temp_6$)
$temp_7 \leftarrow$ Multiplication($x$, $temp_6$, $ac$)
$temp_7 \leftarrow$ Squaring($temp_7$)
return $temp_7$
```

As noted in [8], this technique is more efficient when multiple multiplications are performed rather than a stand-alone multiplication. Quantum multiplication of [8] requires many ancilla qubits. However, since these ancilla qubits can be initialized as 0 after multiplication, they can be reused in the subsequent multiplications. Therefore, the multiplication technique of [8] is effective for Itoh-Tsujii-based inversion where multiple multiplications are performed. Ancilla qubits are allocated only in the first multiplication and subsequent multiplications reuse the previous ancilla qubits without additional ancilla qubits. Quantum resources for the reverse operation to be reused are needed, but this is a negligible cost.

For quantum circuit implementation of squaring, only CNOT gates for modular reduction are required, so it is implemented at low cost. The implementation of the squaring quantum circuit of $\mathbb{F}_{2^{12}}$ is as follows: CNOT($x[6]$, $x[0]$), CNOT($x[7]$, $x[1]$), CNOT($x[8]$, $x[2]$), CNOT($x[9]$, $x[3]$), CNOT($x[10]$, $x[4]$), CNOT($x[11]$, $x[5]$), CNOT($x[11]$, $x[2]$), $x = (x[10], x[5], x[9], x[4], x[8], x[3], x[7], x[2], x[6], x[1], x[11], x[0])$

TABLE II: Quantum resources for the quantum inversion circuit of $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{2^{13}}$.

Binary Field	#Clifford	#T	T-depth	#Qubits	Full depth
$\mathbb{F}_{2^{12}}$	4758	1890	20	402	194
$\mathbb{F}_{2^{13}}$	4988	1848	16	422	369

C. Quantum Circuit Implemetation of Encoding

The encoding in Classic McEliece performs matrix-vector multiplication between the public key matrix H generated using binary field operations and a random vector s. The value of the public key matrix H is predetermined, allowing for the implementation of quantum circuits based on its values. This paper explores three methods of implementation and compares their circuit costs.

The first method is a naive implementation that performs CNOT gates (XOR operations) on the result vector based on the values of matrix H. This method requires ancilla qubits to store the result vector. The second method is an in-place implementation based on the LUP decomposition of matrix H, where the result vector is computed directly. When performing LUP decomposition, we obtain three matrices: a permutation matrix, a lower triangular matrix, and an upper triangular matrix. By utilizing these three matrices, we can achieve the implementation without the need for additional ancilla qubits to store the result(i.e., in-place), and it can be accomplished solely using CNOT gates. The third method is specific to cases where both matrix H and vector s are in a quantum state. This method performs the AND operation between the matrix and vector qubits and then implements the XOR operation with the result vector, using Toffoli gates.

It should be noted that due to the infeasibility of simulating quantum circuits for the smallest parameter public key (768 × 3844) matrix, this implementation and cost analysis use a reduced matrix-vector multiplication.

D. Qunatum Circiut Implementation of the Berlekamp-Massey Decoding Algorithm

The Berlekamp-Massey algorithm can be used as a decoder for solving sets of linear equations and is used in Classic McEliece. In Classic McEliece, this decoding algorithm recovers the vector of secret weight-t from the ciphertext syndrome value. In the Berlekamp-Massey decoding algorithm, multiplication and inversion are repeated as key operations. For quantum multiplication and quantum inversion, which are the core operations of the BM algorithm, the quantum circuit implemented by the technique of [8] and the quantum circuit of Algorithm 1 are used. With iterations of multiplications and inversions, additional qubits for temporary storage are allocated during the process.

We only target the Berlekamp-Massey decoding algorithm used in mceliece34-8864 ($t = 64$ and $\mathbb{F}_{2^{12}}$), but it can be extended according to parameters (t and field size). Algorithm 2 describes the implementation of the Berlekamp-Massey quantum circuit of mceliece348864. MultiplicationXOR means that the product is XORed on the result (i.e., in $z \leftarrow$ MultipltcaiotXOR(x, y, ac), $z = z + xy$).

IV. Performance

In this section, we estimate the quantum resources required for the proposed quantum circuit. In this work, we used the quantum programming tool ProjectQ [9]. Using ProjectQ, we can check the resulting values for the quantum circuit we have implemented, and we can also estimate the required quantum resources.

For detailed resource estimation, Toffoli gates are decomposed and estimated. We decompose one Toffoli gate into 7 T gates + 8 Clifford gates, T-depth 4, full depth 8 following one of the decomposition methods in [10]. We estimate the resources for the quantum circuit at the logical level where no error occurs.

In the proposed encoding quantum ciruit, the three method are performed. Table III shows the results of implementing matrix-vector multiplication as quantum circuits. Analyzing the implementation results, the LUP decomposition allows for an in-place implementation, minimizing the required number of qubits. On the other hand, the naive implementation requires allocating qubits for the result vector, resulting in an increased number of qubits. In terms of CNOT gate count and depth, both methods offer similar performance. For the case of multiplication where both the matrix and vector are in a quantum state, the highest implementation cost is observed, utilizing Toffoli gates. The matrix,

Algorithm 2 The Berlekamp-Massey quantum circuit of Classic McEliece

```
Input: 12-qubit $b$, 12-qubit array $T[t+1]$, $C[t+1]$, $B[t+1]$, $s[2t]$, ancilla qubits $ac$, $L = 0$ (classical)
Output: $C$
$b \leftarrow$ X($b[0]$)
$C[0] \leftarrow$ X($C[0][0]$)
$B[1] \leftarrow$ X($B[1][0]$)
for $N = 0$ to $2t - 1$ do
    $d \leftarrow$ new 12-qubit allocation
    for $i = 0$ to min(N, $t$) do
        $d \leftarrow$ MultiplicationXOR($C[i]$, $s[N - i]$, $ac$)
    end for
    if $(2L \leq N)$ then
        for $i = 0$ to $t$ do
            $T[i] \leftarrow$ new 12-qubit allocation
            $T[i] \leftarrow$ CNOT32($C[i]$, $T[i]$)
        end for
    end if
    $b^{-1} \leftarrow$ Inversion($b$, $ac$)
    if $(2L > N)$ then
        for $i = 0$ to $t$ do
            $C[i] \leftarrow$ MultiplicationXOR($f$, $B[i]$, $ac$)
        end for
    end if
    if $(2L \leq N)$ then
        for $i = 0$ to $t$ do
            $C[i] \leftarrow$ MultiplicationXOR($f$, $B[i]$, $ac$)
            $L \leftarrow N + 1 - L$ (classical)
        end for
        for $i = 0$ to $t$ do
            $B[i] \leftarrow T[i]$
        end for
        $b = d$ (classical)
    end if
    for $i = 0$ to $t - 1$ do
        $B[t - i] \leftarrow B[t - 1 - i]$
    end for
    $B[0] \leftarrow$ new 12-qubit allocation
end for
return $C$
```

vector, and result vector are prepared in qubit states, with the matrix qubits and vector qubits acting as control qubits, and the result vector qubits serving as target qubits. This allows performing the AND operation between the matrix and vector qubits and XORing the result with the result vector.

In the proposed Berlekamp-Massey quantum circuit, multiple multiplications and inversions are performed, and qubits for temp storage are additionally allocated during the process. For quantum circuits of multiplication and inversion, the multiplication technique of [8] is used and recycling of ancilla qubits is performed. Table IV shows the quantum resources required for the Berlekamp-Massey quantum circuit.

Multiplication and inversion are operations that require many quantum resources and are repeated in the proposed Berlekamp-Massey quantum circuit. Therefore, many quantum resources are used and the number of qubits is also very high. Because the parameters used in Classic McEliece are large, this has a high cost even when ported to quantum.

TABLE III: Quantum resources for the quantum circuit of the matrix-vector multiplication encoding algorithm.

matrix-vector encoding	Method	#Clifford	#T	T-depth	#Qubits	Full depth
Quantum-Quantum	Naive	784	896	92	152	147
Classic-Quantum	Naive	45	-	-	24	14
	LUP	37	-	-	16	13

TABLE IV: Quantum resources for the quantum circuit of the Berlekamp-Massey decoding algorithm.

Berlekamp-Massey	#Clifford	#T	T-depth	#Qubits	Full depth
$t = 64$ and $\mathbb{F}_{2^{12}}$	12823392	579384	60800	888492	363696

V. Conclusion

As the potential and powerful cryptanalytic capabilities of quantum computers have emerged, reevaluating the security of existing cryptographic systems is necessary to establish secure encryption systems. In this paper, we optimized and implemented the core operations of Classic McEliece, one of the code-based cryptographic algorithms among the NIST Round 4 candidate algorithms, on quantum circuits. We applied state-of-the-art implementation techniques to realize the core operations of encoding, and decoding on quantum circuits. In particular, the Berlekamp-Massey decoding quantum circuit presented in this paper is the first of its kind. We aim to contribute to the smooth quantum cryptanalysis of Classic McEliece by utilizing the proposed quantum circuits.

As a future research direction, we plan to complete the entire quantum circuit for Classic McEliece based on the implemented core operations. Given the significantly large key size of Classic McEliece, adjustments may be required to define the range within which simulations are feasible. Additionally, finding the optimized combination of the core operations will be crucial.

VI. Acknowledgement

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] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[3] J. Zou, Z. Wei, S. Sun, X. Liu, and W. Wu, "Quantum circuit implementations of AES with fewer qubits," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 697–726, Springer, 2020.

[4] T. Häner, S. Jaques, M. Naehrig, M. Roetteler, and M. Soeken, "Improved quantum circuits for elliptic curve discrete logarithms," in *International Conference on Post-Quantum Cryptography*, pp. 425–444, Springer, 2020.

[5] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, "Quantum resource estimates for computing elliptic curve discrete logarithms," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 241–270, Springer, 2017.

[6] J. Massey, "Shift-register synthesis and bch decoding," *IEEE transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, 1969.

[7] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, *et al.*, "Classic mceliece: conservative code-based cryptography," *NIST submissions*, 2017.

[8] K. Jang, W. Kim, S. Lim, Y. Kang, Y. Yang, and J. Hwa, "Optimized implementation of quantum binary field multiplication with toffoli depth one," in *International Conference on Information Security Applications*.

[9] D. S. Steiger, T. Häner, and M. Troyer, "ProjectQ: an open source software framework for quantum computing," *Quantum*, vol. 2, p. 49, 2018.

[10] M. Amy, D. Maslov, M. Mosca, M. Roetteler, and M. Roetteler, "A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 32, p. 818–830, Jun 2013.