Security analysis for BIKE, Classic McEliece and HQC against the quantum ISD algorithms

Asuka Wakasugi[1] and Mitsuru Tada[2]

[1] Graduate School of Science and Engineering, Chiba University, Japan
ahha3764@chiba-u.jp
[2] Graduate School of Science, Chiba University, Japan
m.tada@faculty.chiba-u.jp

28 December 2022

Abstract. Since 2016, NIST has been standardrizing Post-Quantum Cryptosystems, PQCs. Code-Based Cryptosystem, CBC, which is considered to be one of PQCs, uses the Syndrome Decoding Problem as the basis for its security. NIST's PQC standardization project is currently in its 4th round and some CBC encryption schemes remain there. In this paper, we consider the quantum security for these cryptosystems.

Keywords: Code-based cryptography · MMT/BJMM algorithms · Grover's algorithm · Quantum walk search algorithm

1 Introduction

In modern information society, a public-key cryptosystem is one of the tools used to ensure secure communication. In 1994, Shor proposed the quantum algorithm to solve the integer factorization problem and the discrete logarithm problem in polynomial time, and hence once a large quantum computer is built, the RSA cryptosystems, widely used in our current communication, shall lose its security. Then, we need to think about Post-Quantum Cryptosystems, PQCs, which are resistant to the computational power of quantum computers. In fact, recently quantum computers have been progressing remarkably, so PQC is expected to be put into early practical use.

1.1 Syndrome Decoding Problem (SDP)

Denote, by $\mathrm{wt}(x)$, the number of the non-zero elements for $x \in \mathbb{F}_2^n$.

Definition 1 (SDP). *Let n, k and w be positive integers, H be a matrix in $\mathbb{F}_2^{(n-k)\times n}$, and s be a vector in $\mathbb{F}_2^{n-k}$. Then, SDP is the problem to find an $e \in \mathbb{F}_2^n$ such that $He^T = s$ and $\mathrm{wt}(e) = w$, on input n, k, w, H and s.*

The SDP is known to be NP-complete [16], so Code-Based Cryptosystem (CBC), which uses the SDP as the basis for its security, is considerd to be one of PQCs. NIST has been standardrizing PQCs since 2016, and the project is currently in its 4th Round. BIKE [13], Classic McEliece [1] and HQC [14] remain as the candidates for CBC at the 4th Round.

1.2 Information Set Decoding algorithm (ISD algorithm)

The ISD algorithm is to solve the SDP efficiently. Prange [20] proposed the classical ISD algorithm with its subsequent derivarations. Also, in 2010, Bernstein [3] proposed the quantum ISD algorithm. In this paper, we use the MMT [11] and BJMM [2] as the classical ISD algorithms, and the quantum one. The quantum MMT/BJMM algorithms are proposed by Kachigar and Tillich [9] in 2017. As far as the authors have surveyed, it is the best quantum ISD algorithm. We briefly explain the classical MMT/BJMM algorithms in Chapter 2, and give the quantum MMT/BJMM algorithms in Chapter 4.

1.3 Previous study

CBC is derived from the McEliece cryptosystem [12]. Since the McEliece cryptosystem appeared in 1978, there are a number of studies of security from classical view. For example, Esser and Bellini [5] proposed an estimator, which is a more realstic computation of the ISD algorithms. And Narisada et al. introduce, in [15], studies on decoding the high-dimensional SDPs by parallelizing parts of the ISD algorithm. However, there are not many studies from quantum view. Perriello et al. [18] proposed an attack by using the Bernstein's algorithm for BIKE and Classic McEliece. And they improved that attack by using the quantum version of the Lee-Brickell algorithm [10], which is one of the ISD algorithms. Also, Esser et al. [6] proposed another atttack method by using the Bernstein's algorithm, and extended to all CBC candidates at NIST PQC 4th Round, also including HQC.

1.4 Our contribution and Organization

In this paper, we propose how to calculate the computational cost on the classical circuits equivalent to the quantum circuits for the quantum MMT/BJMM algorithms. Also, we consider the security of all CBCs at the 4th Round of the NIST PQC standardization project against the attack method by using the quantum MMT/BJMM algorithms. As a result, the computational cost for this attack is less than that of the attack using the Bernstein's algorithm. Then, we find that our result is less than that by the previous study [18].

This paper is constructed as following. First, we have already seen the SDP's definition and the abstract of the ISD algorithm. In Chapter 2, we simply explain the classical MMT/BJMM algorithms. In Chapter 3, we introduce the Grover's algorithm [7] and the quantum walk search algorithm [9]. In Chapter 4, based on the above preparations, we give the quantum MMT/BJMM algorithms. In Chapter 5, for cryptosystems remaining as the CBC candidates, we consider the attack strategy, and obtain the result by using the quantum MMT/BJMM algorithms. Finally, we conclude this paper in Chapter 6.

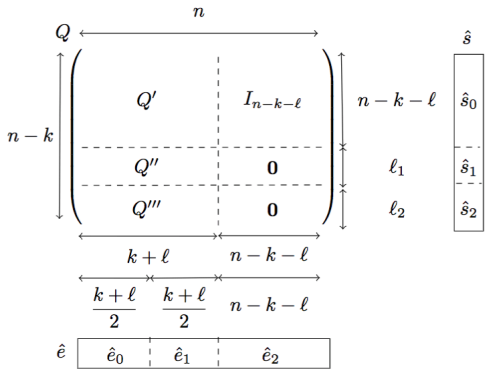

Fig. 1. The partitions for the Classical MMT/BJMM algorithms

2 Classical MMT/BJMM algorithms [11] [2]

Suppose that the SDP's input n, k, w, H, s is given as follows. Let P be an $n \times n$ permutation matrix and U be the matrix to execute the Gaussian Elimination for HP. Let $Q = UHP$, $\hat{e} = P^{-1}e$ and $\hat{s} = Us$, so in the SDP, $He = s$ is an equivalent to $Q\hat{e} = \hat{s}$. $Q, \hat{e}$ and $\hat{s}$ are described in **Fig. 1**. It shows that the upper right $(n-k-\ell) \times (n-k-\ell)$ block of Q is the identity matrix. Then, for the lower $\ell \times n$ block of Q, we further take ℓ_1 and ℓ_2 such that $\ell_1 + \ell_2 = \ell$. The left $(n-k)\times(k+\ell)$ block of Q is partitioned by Q' with $n-k-\ell$ rows, Q'' with ℓ_1 rows and Q''' with ℓ_2 rows, from top to bottom. Also, for the corresponding $(n-k)$-dimensional vector $\hat{s}$, we partition it by $n-k-\ell, \ell_1, \ell_2$ rows and put $\hat{s}_0, \hat{s}_1, \hat{s}_2$ respectively. We consider a similar partition for the n-dimensional vector $\hat{e}$. We put the partitions by $\frac{k+\ell}{2}, \frac{k+\ell}{2}, n-k-\ell$ columns as $\hat{e}_0, \hat{e}_1, \hat{e}_2$, respectively. Also, in the MMT algorithm, the weights of $\hat{e}_0, \hat{e}_1, \hat{e}_2$ are $\frac{p}{2}, \frac{p}{2}, w-p$, respectively. And in the BJMM algorithm, the weights of $\hat{e}_0, \hat{e}_1, \hat{e}_2$ are $\frac{p}{2}+2\varepsilon, \frac{p}{2}+2\varepsilon, w-p-4\varepsilon$, respectively.

In the MMT/BJMM algorithms, SDP can be reducted to the generalised 4-sum problem, G4SP for short. Let V_{11}, V_{12}, V_{21} and V_{22} be as following (in BJMM, this $p/4$ is altered $p/4 + \varepsilon$):

$$
\begin{aligned}
V_{11} &= \{(\hat{e}_{11}, 0^{\frac{3(k+\ell)}{4}}) \in \mathbb{F}_2^{k+\ell} \mid \hat{e}_{11} \in \mathbb{F}_2^{\frac{k+\ell}{4}}, \mathrm{wt}(\hat{e}_{11}) = p/4\},\\
V_{12} &= \{(0^{\frac{k+\ell}{4}}, \hat{e}_{12}, 0^{\frac{k+\ell}{2}}) \in \mathbb{F}_2^{k+\ell} \mid \hat{e}_{12} \in \mathbb{F}_2^{\frac{k+\ell}{4}}, \mathrm{wt}(\hat{e}_{12}) = p/4\},\\
V_{21} &= \{(0^{\frac{k+\ell}{2}}, \hat{e}_{12}, 0^{\frac{k+\ell}{4}}) \in \mathbb{F}_2^{k+\ell} \mid \hat{e}_{21} \in \mathbb{F}_2^{\frac{k+\ell}{4}}, \mathrm{wt}(\hat{e}_{21}) = p/4\},\\
V_{22} &= \{(0^{\frac{3(k+\ell)}{4}}, \hat{e}_{22}) \in \mathbb{F}_2^{k+\ell} \mid \hat{e}_{22} \in \mathbb{F}_2^{\frac{k+\ell}{4}}, \mathrm{wt}(\hat{e}_{22}) = p/4\}
\end{aligned}
$$

Algorithm 1 Classical MMT/BJMM algorithms

Input: $n, k, w, H, s, p, \ell, \ell_1, \ell_2, \varepsilon$
Output: e
1: $e \leftarrow 0^n$
2: **while** $e == 0^n$ **do**
3: $P \xleftarrow{\$} n \times n$ permutation matrix
4: $Q, U \leftarrow GE(HP)$
5: $\hat{s} \leftarrow Us$
6: $\hat{e} \leftarrow \mathsf{G4SP\_BD}(Q, p, \ell_1, \ell_2, \hat{s})$
7: **if** $\mathrm{wt}(\hat{e}) == w - p - 4\varepsilon$ **then**
8: $e \leftarrow P\hat{e}$
9: **return** e

The G4SP is the problem to search $(v_{11}, v_{12}, v_{21}, v_{22}) \in V_{11} \times V_{12} \times V_{21} \times V_{22}$ satisfying as following:

$$\begin{cases} Q''(v_{11} + v_{12}) & = 0^{\ell_1} \quad (1) \\ Q''(v_{21} + v_{22}) + \hat{s_2} & = 0^{\ell_1} \quad (2) \\ Q'''(v_{11} + v_{12}) + Q'''(v_{21} + v_{22}) + \hat{s_1} & = 0^{\ell_2} \quad (3) \\ Q'(v_{11} + v_{12}) + Q'(v_{21} + v_{22}) + \hat{s_0} & = 0^{n-k-\ell} \quad (4) \end{cases}$$

In the classical MMT/BJMM algorithms, we search $(v_{11}, v_{12}, v_{21}, v_{22})$ by the Birthday Decoding algorithm. So, the classical MMT/BJMM algorithms are described in **Algorithm 1**.

In the MMT algorithm, $\varepsilon = 0$. Here, GE described in Line 4 refers to the subroutine to execute the Gaussian Elimination. And G4SP_BD in Line 6 is the subroutine to solve the G4SP using the Birthday Decoding algorithm. We explain the details of **Algorithm 1**. First, e is initialised at 0^n. Then, this algorithm halts by updating the value of e in the **while** sentence of Lines 2-10. In one iteration, an $n \times n$ permutation matrix P is randomly chosen in Line 3. If both Q and $\hat{s}$ are formalized in **Fig. 1**, we can get $\hat{e}$ in **Fig. 1** in Line 6. That $\hat{e}$ satisfies the condition of the **if** statement in Line 7, so the value of e is updated in Line 8. The times of the loop excution during the **while** sentence of Lines 2-10 is $\frac{\binom{n}{w}}{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}$.

3 Grover's algorithm and Quantum walk

In this chapter, we explain about the Grover's algorithm [7] and the quantum walk search algorithm over Johnson graph [9] after the roughly introduction about the quantum computation.

3.1 Quantum computation

Let H be an n-dimensional Hilbert space. For each $1 \leq i \leq n$, we denote, by $|i\rangle$, the n-length vector in which the i-th element is 1 and the others are 0. In other words, $\{|1\rangle, |2\rangle, \cdots, |n\rangle\}$ are an orthnormal basis of H. For $1 \leq i, j \leq n$, $|i\rangle \otimes |j\rangle$ is written also as $|i\rangle|j\rangle$ or $|ij\rangle$. The quantum state $|\phi\rangle$ of H can be represented as $|\phi\rangle = \sum_{i=1}^{n} \alpha_i |i\rangle$, where $(\alpha_1, \cdots, \alpha_n) \in \mathbb{C}^n$ and $\sum_{i=1}^{n} |\alpha_i|^2 = 1$. A map $f : H \to H$ is said to be an operator if f is linear. We equate an operator with its representation matrix hereafter. An operator f is said to be unitary if the representation matrix of f is unitary, and such an f is said to be a quantum gate. Clifford gate is the set of H gate, S gate and CNOT gate, and each of them is represented as follows:

$$\mathrm{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \ \mathrm{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \ \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

T gate is the quantum gate represented by $\mathrm{T} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$, and Clifford+T gate is Clifford gate plus T gate.

3.2 Grover's algorithm [7]

Let V be $\{0,1\}^n$ and M be a non-empty subset of V. And let $f : V \to \{0,1\}$ be the function such that $f(v)$ is 1 if $v \in M$ and 0 otherwise. The Grover's algorithm is the quantum algorithm to search $x_0 \in M$ taking (V, f) as inputs. This algorithm has the computational complexity of $O\left(\sqrt{\frac{|V|}{|M|}}\right)$. Let H^V is the Hilbert space associated with V. U_o and U_d are the unitary operators over H^V and defined as following:

$$U_o(|i\rangle) := \begin{cases} -|i\rangle & i \in M \\ |i\rangle & \text{o.w.} \end{cases}$$
$$U_d(|i\rangle) := (2\mathrm{H}^{\otimes n}|0\rangle\langle 0|\mathrm{H}^{\otimes n} - I_n)|i\rangle$$

$\mathrm{H}^{\otimes n}$ denotes $\underbrace{\mathrm{H} \otimes \cdots \otimes \mathrm{H}}_{n}$, that is, the Tensor products of n H gates. U_o is called the oracle operator and U_d is the unitary operator called diffuser. Then, the Grover's algorithm is written by **Algorithm 2**. In Lines 1 and 2, $|\psi\rangle$ is initialised at 0^n and updated by superposition of the quantum states of H^V. Then, in Lines 3-6, $|\psi\rangle$ is multiplied by U_o and U_d a specific number of times. Finally we can get x_0 by measuring $|\psi\rangle$.

Algorithm 2 Grover's algorithm

Input: $V \subset \{0,1\}^n,\ f : V \to \{0,1\}$
Output: $x_0 \in \{0,1\}^n$ s.t. $f(x_0) = 1$
1: $|\psi\rangle \leftarrow |0^n\rangle$
2: $|\psi\rangle \leftarrow H^{\otimes n}|\psi\rangle$
3: **for** $i := 1$ to $\left\lfloor \frac{\pi}{4\arcsin(\sqrt{\frac{|M|}{|V|}})} \right\rfloor$ **do**
4: $\quad |\psi\rangle \leftarrow U_o|\psi\rangle$
5: $\quad |\psi\rangle \leftarrow U_d|\psi\rangle$
6: **return** $|\psi\rangle$

3.3 Quantum walk search algorithm(QW search algorithm) [9]

Definition 2 (Johnson Graph). *A Johnson Graph $J(x,r)$ is a graph, in which every vertex is labeled by an r-element subset V of the set $\{1,2,\ldots,x\}$, and in which two vertices, U and V, are adjacent to each other if and only if $|U \cap V| = r-1$.*

In particular, a Johnson Graph is a complete graph when $r = 1$.

Let $G = J(x,r) = (V,E)$ and let M be a non-empty subset of V. A_G denotes the adjacent matrix of G, and P_G denotes the stochastic transition matrix of G. And we put $P_G = \dfrac{A_G}{r(x-r)}$. That is, for each vertex in $J(x,r)$, there are $r(x-r)$ adjacent vertices in that graph. So the transition probability to each vertex is $\dfrac{1}{r(x-r)}$. The QW search algorithm is a quantum algorithm that searches for a vertex v belonging to M taking G, M and P_G as the input. While the Grover's algorithm can be regarded as a search algorithm for one-dimensional arrays, the QW search algorithm can be regarded as a search algorithm for two-dimensional arrays such as graphs. In fact, the QW search algorithm on a complete graph with a loop at each vertex can be the Grover's algorithm. And in general, a Johnson Graph is an undirected graph. We denote, by $|i\rangle$, the quantum state of a vertex i, and denote by $|ij\rangle$, the quantum state of the edge (i,j). Then we have to assign, to one edge (i,j), two quantum states $|ij\rangle$ and $|ji\rangle$ which are distinct in general. Hence here, we identity one undirected edge with two directed edges which are mutually oriented. Thereby we consider a Johnson Graph to be a directed graph. For an edge set E, let H^E be the Hilbert space associated with E, and we define the unitary operators U_o and U_d over H^E as following:

$$U_o(|i\rangle|j\rangle) := \begin{cases} -|i\rangle|j\rangle & i \in M \\ |i\rangle|j\rangle & \text{o.w.} \end{cases}, U_d(|i\rangle|j\rangle) := U_{dL}(U_{dR}(|i\rangle|j\rangle)),$$

where U_{dL} and U_{dR} are defined as

$$U_{dR} := 2\sum_{x\in V} |\Phi_x\rangle\langle\Phi_x| - I_{|V|^2}, U_{dL} := 2\sum_{y\in V} |\Psi_y\rangle\langle\Psi_y| - I_{|V|^2},$$

Algorithm 3 QW search algorithm

Input: $G = J(x, r) = (V, E \subset V \times V), P_G, M \subset V$
Output: $x \in M$
1: $|\psi\rangle \leftarrow |0^n\rangle$
2: $|\psi\rangle \leftarrow H^{\otimes n}|\psi\rangle$
3: **for** $i := 1$ to $\left\lfloor \frac{1}{\sqrt{\varepsilon\delta}} \right\rfloor$ **do**
4: $\quad |\psi\rangle \leftarrow U_o|\psi\rangle$
5: $\quad |\psi\rangle \leftarrow U_d|\psi\rangle$
6: **return** $|\psi\rangle$

with $I_{|V|^2}$, the $|V|^2 \times |V|^2$ identity matrix. Furthermore, $|\Phi_x\rangle$ and $|\Psi_y\rangle$ are defined as

$$|\Phi_x\rangle := |x\rangle \left(\sum_{y \in V, (x,y) \in E} \sqrt{P_G[x][y]} |y\rangle \right), |\Psi_y\rangle := \left(\sum_{x \in V, (y,x) \in E} \sqrt{P_G[y][x]} |x\rangle \right) |y\rangle,$$

where $P_G[x][y]$ is the (x, y) component of P_G. The unitary operator U_o is similar to the Grover's algorithm. $|\Phi\rangle_x$ is represented by the Tensor product of the sum of the quantum states of all adjacent vertices with the quantum state of x. And the coefficients represent as the root of the transition probability from x. We then construct the unitary operator U_{dR} from $|\Phi\rangle_x$. $|\Phi\rangle_x$ is the vector whose length is $|V|$, so U_{dR} is the $|V| \times |V|$ matrix. Similarly, we consider $|\Psi\rangle_y$ and construct the unitary operator U_{dL} from $|\Psi\rangle_y$. The QW search algorithm is written in **Algorithm 3**. In **Algorithm 3**, ε is $\frac{|M|}{|V|}$, which is the ratio of the number of the vertices to be searched out of the total number of vertices. $\delta = \frac{x}{r(x-r)}$ is the spectral gap. Lines 1 and 2 are similar to the Grover's algorithm. Then, in Lines 3-6, U_o and U_d are in turn multiplied by $|\psi\rangle$ appropriate number of times. Finally, we can observe $|\psi\rangle$.

4 Quantum MMT/BJMM algorithms [9]

In this chapter, we consider the quantum MMT/BJMM algorithms by combining the classical MMT/BJMM algorithms, the Grover's algorithm and the QW search algorithm. We improve Lines 3 and 6 in **Algorithm 1** respectively by using the Grover's algorithm and the QW search algorithm as subroutines. We describe how to incorporate these two algorithms as subroutines.

First, in Line 6, we use the QW search algorithm over the products of Johnson Graphs.

Definition 3 (The product of graphs). *For finite graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, the product $G := G_1 \times G_2 = (V, E)$ of G_1 and G_2 is given in $V = V_1 \times V_2$ and $E = \{(u_1u_2, v_1v_2) \mid (u_1 = v_1 \wedge (u_2, v_2) \in E_2) \vee ((u_1, v_1) \in E_1 \wedge u_2 = v_2)\}$.*

For $0 \leq i \leq 3$, we consider the whole of the r-element subsets of V_i in the G4SP. Then such a set is a JG, and can be denoted by $J_i(N, r)$ ($i \in \{11, 12, 21, 22\}$) where $N = \binom{\frac{k+\ell}{4}}{\frac{p}{4}+\frac{\varepsilon}{2}}$ and r is the number of $(v_{11}, v_{12}, v_{21}, v_{22})$ satisfying the G4SP, given in $r = N^{\frac{4}{7}}\binom{p}{\frac{p}{2}}^{\frac{2p}{7}}$. And we put $J(N, r) = J_{11}(N, r) \times J_{12}(N, r) \times J_{21}(N, r) \times J_{22}(N, r)$. Therefore, let $G = J(N, r)$, and let P_G be the strochastic transition matrix and M be the set of all vertices on G satisfying the G4SP condition. Then, we can use the QW search algorithm as a subroutine in Line 6 in **Algorithm 1**.

Next, we use the Grover's algorithm in Line 3. Let V be the entire set of $n \times n$ permutation matrix. Also, the function $f : V \to \{0, 1\}$ returns 1 if there exists a $(v_{11}, v_{12}, v_{21}, v_{22})$ satisfying the G4SP condition, and otherwise returns 0. In more details, it is as following. When performing the Gaussian Elimination on HP with $P \in V$ and H, $Q = UHP$ has the form shown in **Fig. 1**. That is, the upper right $(n-k-\ell) \times (n-k-\ell)$ block of Q is the identity matrix and the lower right $\ell \times (n-k-\ell)$ block of Q is the zero matrix. Using Q and $\hat{s} = Us$, we search for $(v_{11}, v_{12}, v_{21}, v_{22})$ in the subroutine in Line 6. U, Q and $\hat{s}$ are uniquely determined for each P, and it is highly probable that such a $(v_{11}, v_{12}, v_{21}, v_{22})$ exists. Therefore, we can use the Grover's algorithm as subroutine in Line 3 in **Algorithm 1** by constructing V, f as above.

Based on the above preparations, the quantum MMT/BJMM algorithms are written in **Algorithm 4**. Grover in Line 3 denotes the subroutine to search for the permutation matrix P using the Grover's algorithm. And G4SP_QW in Line 6 denotes the subroutine solving the G4SP by using the QW search algorithm. Other lines except for Lines 3 and 6 are similar in **Algorithm 1**. The number of execution times in Lines 2-8, denoted by ℓ_{Grover}, is $\sqrt{\frac{\binom{n}{w}}{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}}$ by the computational complexity of the Grover's algorithm given in Section 3.2. And the number of execution times in Line 6, denoted by $\ell_{\mathrm{BJMM\_QW}}$, is $\frac{\left(\frac{\frac{k+\ell}{2}}{\frac{p}{4}+\frac{\varepsilon}{2}}\right)^{\frac{6}{5}}}{\binom{p}{\frac{p}{2}}^{\frac{1}{2}}\binom{k+\ell-p}{\varepsilon}^{\frac{1}{2}}}$ [9]. We search for $(v_{11}, v_{12}, v_{21}, v_{22})$ satisfying the G4SP condition in $\ell_{\mathrm{BJMM\_QW}}$ times, and construct $\hat{e}$. The value of e is updated and **Algorithm 4** halts if $(v_{11}, v_{12}, v_{21}, v_{22})$ found matches the condition of **if** sentence in Line 7. Hence, the quantum MMT/BJMM algorithms have the computational cost as much as the square root of those of the classical MMT/BJMM algorithms.

The key point of the quantum MMT/BJMM algorithms is the use of the quantum algorithm in Lines 3 and 5. In both the Grover's algorithm and the QW search algorithm, a quantum state is initialised to be a superposition of all quantum states that is $H^{\otimes}|0^n\rangle$, and it is multiplied by U_o and U_d the predetermined times according to the input. We note that quantum states are vectors and unitary operators are matrices. So both algorithms only perform matrix

Algorithm 4 Quantum MMT/BJMM algorithms

Input: $n, k, w, H, s, p, \ell, \ell_1, \ell_2, \varepsilon$
Output: e
1: $e \leftarrow 0^n$
2: **while** $e == 0^n$ **do**
3: $P \leftarrow \mathsf{Grover}(\ell, H)$
4: $Q, U \leftarrow GE(HP)$
5: $\hat{s} \leftarrow Us$
6: $\hat{e} \leftarrow \mathsf{G4SP\_QW}(Q, p, \ell_1, \ell_2, \hat{s})$
7: **if** $\mathrm{wt}(\hat{e}) == w - p - 4\varepsilon$ **then**
8: $e \leftarrow P\hat{e}$
9: **return** e

cryptosystems	security bit	n	k	w
BIKE	128	24646	12323	134
	192	49318	24659	199
	256	81946	40973	264
Classic McEliece	128	3488	2720	64
	192	4608	3360	96
	256	8192	6528	128
HQC	128	35338	17669	132
	192	71702	35851	200
	256	115274	57637	262

Table 1. Targeted cryptosystems and security bits

addition and multiplication. And in the quantum MMT/BJMM algorithms, in Lines 4 and 7, we can see that they essentially only multiply matrices. Thus, the quantum MMT/BJMM algorithms can be regarded as an algorithm consisting only of matrix addition and multiplication.

5 Analysis

In this chapter, we discuss the attack method using the quantum MMT/BJMM algorithms and its result for the SDP with the parameters given in **Table. 1**. **Table. 1** shows the SDP instances which correspond to the BIKE, Classic McEliece and HQC, the cryptosystems remaining at the 4th Round of the NIST PQC standardization project, with the security leveles of 128, 192 and 256.

First, we introduce the G-cost, D-cost and W-cost as the new computational costs. Next, we consider the quantum circuit consisting of Clifford+T gates to simulate the **Algorithm 4**. We reconstruct the classical circuit to implement the quantum operator by Clifford+T gates, and verify that each computational cost is kept within a constant multiple of the number of input qubits. Finally, we investigate whether each cryptosystem with the parameters (n, k, w) given by **Table. 1** is secure against our atttack, or not.

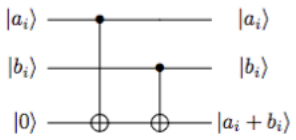

Fig. 2. The addition for one qubit

5.1 Introducing the new computational costs

In this section, we introduce the computational costs used in the paper [8] by Jaque et al. Let C be a quantum circuit consisting of Clifford+T gates. The G-cost refers to the number of all the quantum gates in C. The D-cost refers to the depth of C, and the W-cost is the number of the qubits in C. These computational costs are evaluated by $\log_2$. Also, in this paper, we compare the security bit with the G-cost obtained by our strategy from the parameters (n, k, w) in **Table. 1**. These computational costs are based on the computational model, called the memory peripheral model, in which the quantum gates in the Clifford+T gates are equivalent to the RAM operations in the classical circuit. As seen in [8] by Jaques et al., also in this paper, we do not consider about the superposition of the quantum states in estimating the G-cost. This is because the superposition which can be executed in the quantum RAM operations cannot be executed in the classical ones. Therefore, we do not care the computational costs of the Grover's algorithm and the QW search algorithm themselves. In the following, we consider the G-cost, D-cost and W-cost about the operations in the quantum MMT/BJMM algorithms.

5.2 The computational cost for the addition of quantum bits

In the following, let ℓ, m, n be positive integers, and let $a = a_1 \cdots a_m, b = b_1 \cdots b_m \in \mathbb{F}_2^m, A \in \mathbb{F}_2^{\ell \times m}$ and $B \in \mathbb{F}_2^{m \times n}$. Then, $|a\rangle = |a_1 \cdots a_m\rangle$ and $|b\rangle = |b_1 \cdots b_m\rangle$. We define $|a\rangle + |b\rangle := |a + b\rangle$. In other words, the sum of m-quantum bits $|a\rangle$ and $|b\rangle$ corresponds to $|a + b\rangle$, the quantum state of $a + b$, as $a, b \in \mathbb{F}_2^m$. Since $|(a + b)[i]\rangle = |a_i + b_i\rangle$ for $1 \leq i \leq m$, we consider the quantum circuit to calculate $|a_i + b_i\rangle$ from $|a_i\rangle$ and $|b_i\rangle$. Such a quantum circuit can be constructed from two CNOT gates as shown in **Fig. 2**. That is, the quantum circuit to realize the sum $|a + b\rangle$ of m-quantum bits $|a\rangle$ and $|b\rangle$, has the G-cost of $2m$, the D-cost of 2 and the W-cost of $3m$.

5.3 The computational cost for the product of matrices

Also, we think the product of $|A\rangle$ and $|B\rangle$, where $|A\rangle$ is the quantum state corresponding to the $\ell \times m$ matrix A, and $|B\rangle$ is the quantum state corresponding to the $m \times n$ matrix B. $|AB\rangle$ denotes the quantum state of the $\ell \times n$ matrix

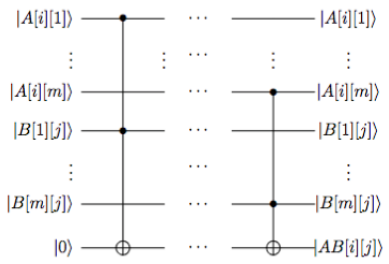

Fig. 3. The matrix products for qubits

AB. Therefore, for $1 \leq i \leq \ell, 1 \leq j \leq n$, we consider the quantum circuit to compute $|AB[i][j]\rangle = \left|\sum_{k=1}^{m} A[i][k]B[k][j]\right\rangle$. Such a quantum circuit can be constructed from m Toffoli gates as shown in **Fig. 3**. Toffoli gate is a quantum gate expressed as following:

$$\text{Toffoli} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The construction from Toffoli gate by Clifford+T gates is given in the paper by Shende [21]. The G-cost, D-cost and W-cost of that quantum circuit are 24, 16 and 3 respectively. Hence, the G-cost, D-cost and W-cost of the circuit to calculate $|AB\rangle$ from $|A\rangle$ and $|B\rangle$ are $24\ell mn$, $16m$ and $\ell m+\ell n+mn$, respectively.

5.4 The computational cost for the Gaussian Elimination

In this section, we discuss the quantum circuit to output the matrcies $U \in \mathbb{F}_2^{(n-k)\times(n-k)}$ and $Q = UHP \in \mathbb{F}_2^{(n-k)\times n}$, where U is a matrix to execute the Gaussian Elimination for HP, and P is an $n \times n$ permutation matrix. That is, for $|H\rangle$ corresponding to the quantum state of H, we calculate $|U\rangle$, the quantum state of U, and $|Q\rangle$. For $1 \leq i < j \leq k$, we think about the quantum circuit to do the process in the rows 1 and j of H. Such a quantum circuit can be realized with $(n+1)$ Toffoli gates as shown in **Fig. 4**. Therefore, the total quantum circuit to execute the Gaussian Elimination can be constructed from

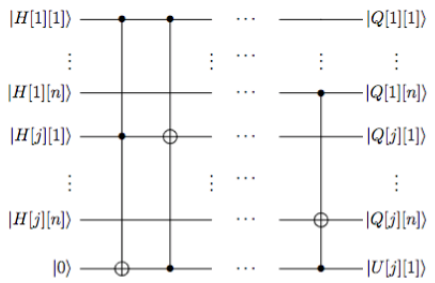

Fig. 4. The Gaussian Elimination for qubits

$\sum_{i=1}^{n-k-1}(n-k-i)(n+2-i) = \frac{1}{6}(n-k-1)(n-k)(2n+k+5)$ Toffoli gates. The G-cost, D-cost and W-cost of that quantum circuit are $4(n-k-1)(n-k)(2n+k+5)$, $16(n-k-1)$ and $2(n-k)n+(n-k)^2$, respectively.

5.5 The computational cost for calculating the Hamming weight

In this section, for a given quantum state $|\psi\rangle = |p_1 \cdots p_n\rangle$, we calculate the Hamming weight $\mathrm{wt}(\psi)$ of $|\psi\rangle$ as an element ψ in $\mathbb{F}_2^m$. We consider the operation which, for $a, b, c \in \mathbb{F}_2$, computes s and $d \in \mathbb{F}_2$ with $|s\rangle|d\rangle = |a+b+c\rangle$, where $a+b+c$ is done in $\mathbb{N}$ not in $\mathbb{F}_2$. That operation outputs 2 qubits on input of 3 qubits. Here we call the operation the 3 adder. We discuss the quantum circuit to execute the quantum state $|a\rangle+|b\rangle+|c\rangle = |sd\rangle$ corresponding to this addition. The quantum circuit can be constructed from two Toffoli gates and three CNOT gates as shown in **Fig. 6**. Hence, the G-cost, D-cost and W-cost of the quantum circuit realizing the 3 adder are 51, 32 and 5, respectively.

Based on the above preparations, we consider the Hamming weight of the quantum state. The circuit to calculate the Hamming weight of classical 10 bits is given in the Brandão et al. [4]. We can construct from the quantum circuit to calculate the Hamming weight of the quantum state by replacing HA and FA in the classical circuit with half-adder, 3 adder, respectively. Here, HA and FA denote 'the half-adder'[3] and 'the full-adder' defined by [4]. Here, the quantum circuit to execute our half-adder is given in **Fig. 5**. Therefore, the quantum circuit to calculate the Hamming weight of $|\psi\rangle = |p_1 \cdots p_n\rangle$ can be constructed using the half-adders and the 3 adders, and the required number of those is $\sum_{i=1}^{\lceil \log_2 n \rceil} \left\lceil \frac{n}{2^i} \right\rceil$ in total. Here, the half-adder in **Fig. 5** has the G-cost of 26, the D-cost of 16 and the W-cost of 4. Since for each of the G, D, W-cost, the 3 adder requires more gates than the half-adder, the number of gates to calculate the

[3] Also in this paper, we define the half-adder operation. Note that 'the half-adder' given by [4] is different from ours.

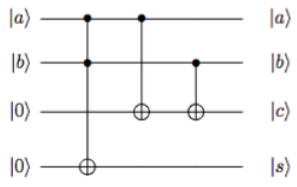

Fig. 5. Half-adder for qubit

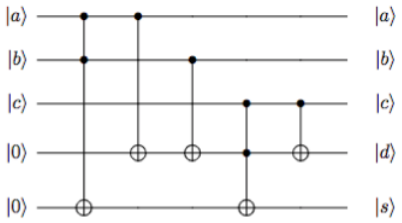

Fig. 6. 3 adder for qubit

Hamming weight has the upper bound of $n-1$, which corresponds to the circuit in which all the operations are of the 3 adder. So the G-cost, D-cost and W-cost of the quantum circuit to calculate the Hamming weight of $|\psi\rangle$ are $51(n-1), 32$ and $n+2(n-1)+\lceil \log_2 n \rceil$, respectively.

5.6 The computational cost for quantum MMT/BJMM algorithms

Table. 2 and **Table. 3** show the result up to the previous section. In this section, we discuss the computational cost for the quantum MMT/BJMM algorithms. In one iteration of **while** sentence in **Algorithm 4**, only one of the operations up to the previous section has been performed. Therefore, the quantum circuit to execute the quantum MMT/BJMM algorithms is consisting of Clifford+T gates, so we can calculate the computational costs of that quantum circuit. The G-cost, D-cost and W-cost in Line i with $4 \leq i \leq 8$ in **Algorithm 4** are denoted by G_i, D_i and W_i respectively. Let $G_{6,G4SP}$ be the G-cost of the quantum circuit representing the four conditions of G4SP in Line 6. The overall G-cost G is given by $G = (G_4 + G_5 + G_{6,G4SP}\ell_{\mathrm{BJMM\_QW}} + G_7)\ell_{\mathrm{Grover}} + G_8$. The overall D-cost D is $D = \max\{\max\{D_4, D_5, D_6, D_7\}\ell_{\mathrm{Grover}}, D_8\}$. The overall W-cost W is the sum of the quantum bits of each parameter and the ancilla bits appearing to the previous section.

5.7 Evaluation criteria and Parallelizing the quantum algorithm

NIST [17] states that the classical circuit corresponding to the 128, 192 and 256 security bits is equivalent to the classical circuit having the $2^{143}, 2^{207}$ and 2^{272} classical gates respectively. Therefore, by considering a classical gate as a RAM operation by a classical computer, we can directly compare the G-cost with the above numbers. For example, for a cryptosystem with 128 security level, if its G-cost is greater than 143, it is secure against this attack. The constraints for each parameter follow the conditions in the paper by Becker et al. on the classical BJMM algorithm [2].

Also, the D-cost is limited to 96 or less under the condition from NIST [17]. If the D-cost exceeds 96, we use the parallel Grover in [8]. This is the technique

Operation	G-cost
Addition	$2m$
Matrix production	$24\ell mn$
Gaussian Elmination	$4(n-k-1)(n-k)(2n+k+5)$
Hamming weight	$\leq 51(n-1)$

Table 2. G-cost for quantum operations

Operation	D-cost	W-cost
Addition	2	$3m$
Matrix production	$16m$	$\ell m + \ell n + mn$
Gaussian Elmination	$16(n-k-1)$	$2(n-k)n + (n-k)^2$
Hamming weight	32	$n + 2(n-1) + \lceil \log_2 n \rceil$

Table 3. D-cost and W-cost for quantum operations

parallelizing **Algorithm 2** and **Algorithm 3**. Let G, D and W be the G-cost, D-cost and W-cost, respectively, for the entire for statement with one processor. Then G-cost, D-cost and W-cost for the entire for statement with p processors are $\sqrt{p}G$, $\frac{1}{\sqrt{p}}D$ and pW. Therefore, if D-cost exceeds 96 with one processor, D-cost can be reduced to less than 96 by using an appropriate number of processors for parallelizing.

5.8 Result

Table. 4 lists the computational costs for each encryption scheme and security level. The upper row for each security level in the table shows the computational cost of incorporating the Bernstein's algorithm into our attack scheme. The lower row shows the computational cost of using the quantum MMT/BJMM algorithms. In conclusion, the computational cost of the attack is less than that of the attack. Furthermore, the computational cost of the quantum MMT/BJMM algorithms is less than that of the Bernstein's algorithm. And **Table. 5** shows the comparison between the previous study [18] and our method, listing the T-gate-based DW-costs for the BIKE and Classic McEliece for each security bit when the Bernstein's algorithm is applied. Here, the T-gate-based cost is defined with the number of T-gates used, so-called T-depth and the W-cost, where T-depth means the number of the sequential gates in the circuit including T gates. The DW-cost is the product of the D-cost and the W-cost. As a result, our cost is less than the previous cost in [18].

6 Conclusion

In this paper, for all CBCs remaining at the 4th Round of the NIST PQC standardization project, we have proposed the attack method with the quantum MMT/BJMM algorithms. Also, we have discussed the security of their cryptosystems by calculating the G-cost, the D-cost and the W-cost over quantum

cryptosystems	security bit	G-cost	D-cost	W-cost
BIKE	128(143 gates)	116	86	31
		113	95	33
	192(207 gates)	213	84	66
		182	95	88
	256(272 gates)	322	88	102
		251	95	157
Classic McEliece	128(143 gates)	110	88	25
		104	93	25
	192(207 gates)	188	77	52
		145	95	52
	256(272 gates)	384	84	108
		262	95	170
HQC	128(143 gates)	116	86	32
		114	95	35
	192(207 gates)	216	85	68
		187	95	93
	256(272 gates)	322	88	105
		252	95	158

Table 4. Cost for each cryptosystem and security bit

cryptosystems	security bit	[18]	this paper
BIKE	128	138	115
	192	176	149
	256	212	189
Classic McEliece	128	124	111
	192	149	127
	256	209	176

Table 5. DW-cost evaluated by the number of T gates

circuits consisting of Clifford+T gates. All of the previous papers on quantum security for CBCs developed their arguments over those quantum circuits. As far as we survey, we have never seen discussion on the quantum security of CBC using the quantum MMT/BJMM algorithms. We cannot take into account the computational costs of the quantum RAM operations over classical circuits. We can see from **Table. 5** that the computational costs over classical circuits are less than those on quantum circuits. Therefore, we cannot conclude from **Table. 4** that the security of each cryptosystem has been weakened. However, from this result, we have shown the validity of the attack method used in this paper. So, we calculate the computational costs over quantum circuits for quantum MMT/BJMM algorithms, and consider the cryptanalysis for CBCs by using those exact costs in the future.

References

1. M. R. Albrecht, D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurich, R. Misoczki, R. Niederhagen, K. G. Paterson, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C. J. Tjhai, M. Tomlinson, W. Wang: "Classic McEliece", Tech. rep., National Institute of Standards and Technology (2020).
2. A. Becker, A. Joux, A. May, A. Meurer: "Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding", In Annual international conference on the theory and applications of cryptographic techniques, pp.520–536, 2012.
3. D. J. Bernstein: "Grover vs. McEliece", In Post-Quantum Cryptography 2010 (2010), N. Sendrier,Ed., vol.6061 of Lecture Notes in Comput. Sci., Springer, pp.73–80, 2010.
4. L. T. A. N. Brandão, C. Çalık, M. S. Turan, R. Peralta: "Upper bounds on the multiplicative complexity of symmetric Boolean functions", Cryptogr. Commun. 11, pp.1339–1362, 2019.
5. A. Esser, E. Bellini: "Syndrome decoding estimator", In: IACR International Conference on Public-Key Cryptography. Springer, Cham, pp.112-141, 2022.
6. A. Esser, S. Ramos-Calderer, E. Bellini, J. I. Latorre, M. Manzano: "Hybrid Decoding–Classical-Quantum Trade-Offs for Information Set Decoding", Cryptology ePrint Archive, 2022.
7. Lov K. Grover: "A fast quantum mechanical algorithm for database search", In Gary L. Miller, editor, Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996, pp.212–219, ACM, 1996.
8. S. Jaques, J. M. Schanck: "Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE", Annual International Cryptology Conference - CRYPTO (Springer), pp.32-61, 2019.
9. G. Kachigar and J.P. Tillich: "Quantum information set decoding algorithms", In: International Workshop on Post-Quantum Cryptography. Springer, Cham, pp.69-89, 2017.
10. P. Lee and E. Brickell: "An observation on the security of McEliece's public-key cryptosystem", In Advances in Cryptology—EUROCRYPT'88, C. Günter, Ed. New York: Springer-Verlag, p.275, 1988.
11. A. May, A. Meurer, E. Thomae: "Decoding random linear codes in $\tilde{\mathcal{O}}(2^{0.054n})$", In International Conference on the Theory and Application of Cryptology and Information Security, pp.107–124, 2011.
12. R. J. McEliece: "A public-key cryptosystem based on algebraic coding theory", Deep Space Network Progress Report, vol.44, pp.114-116, Jan, 1978.
13. C. A. Melchor, N. Aragon, P. S. L. M. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J. Deneuville, P. Gaborit, G. Santosh, S. Gueron, T. Güneysu, R. Misoczki, E. Persichetti, N. Sendrier, J. Tillich, V. Vasseur, G. Zémor: "BIKE", Tech. rep., National Institute of Standards and Technology, 2020.
14. C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J. C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, J. Bos : "HQC", Tech. rep., National Institute of Standards and Technology, 2020.
15. S. Narisada, K. Fukushima, S. Kiyomoto: "Multi-Parallel MMT Algorithm for Solving High-Dimensional SDP", The 2022 Symposium on Cryptography and Information Security SCIS2022, 4A2-1, 2022.
16. H. Niederreiter: "Knapsack-type cryptosystems and algebraic coding theory", Problems of Control and Information Theory, vol.15(2), pp.159-166, 1986.

17. NIST: "Post-Quantum Cryptography, Security (Evaluation Criteria)", available at `https://csrc.nist.gov/projects`.
18. S. Perriello, A. Barenghi, G. Pelosi: "A complete quantum circuit to solve the information set decoding problem", In: 2021 IEEE International Conference on Quantum Computing and Engineering (QCE). IEEE, pp.366-377, 2021.
19. S. Perriello, A. Barenghi, G. Pelosi: "A Quantum Circuit to Speed-up the Cryptanalysis of Code-based Cryptosystems", In: International Conference on Security and Privacy in Communication Systems. Springer, Cham, pp.458-474, 2021.
20. E. Prange: "The use of information sets in decoding cyclic codes", Information Theory, IRE Transactions on, vol.8(5):pp.5-9, September, 1962.
21. V. V. Shende, I. L. Markov: "On the CNOT-cost of TOFFOLI gates", Quantum Info. Comput. vol.9(5), pp.461-486, May, 2009.