Computer Security Symposium 2022
24 - 27 October 2022

符号ベース暗号に対する量子的な安全性の解析

若杉 飛鳥[1,a)]　多田 充[2,b)]

概要：多くの公開鍵暗号系の安全性の根拠となっている素因数分解問題や離散対数問題は Shor の量子アルゴリズムによって多項式時間で解けることが知られているため，大規模な量子計算機が実現すると，現在最も広く利用されている RSA 暗号方式はその安全性を失う．そのため，2016 年から米国国立標準技術研究所（NIST）が PQC の標準化を進めている．符号ベース暗号は量子計算機に耐性がある耐量子計算機暗号（PQC）の 1 つと考えられている．本稿では，現在の NIST PQC 標準化プロジェクト第 4 ラウンドの候補として残っている符号ベース暗号の方式に対して，量子的な安全性を考察する．

キーワード：符号ベース暗号，MMT/BJMM アルゴリズム，Grover のアルゴリズム，量子ウォーク探索アルゴリズム

Quantum security analysis for code-based cryptosystems

Asuka Wakasugi[1,a)]　Mitsuru Tada[2,b)]

Abstract: Since the factorization problem and the discrete logarithm problem, which are based on the security of many public-key cryptosystems, are known to be solved in polynomial time by Shor's quantum algorithm, after building large quantum computers, RSA cryptosystem currently widely used loses that security. So the US National Institute of Standards and Technology (NIST) has been standardizing PQCs since 2016. Code-Based Cryptosystem(CBC) is considered to be one of Post-Quantum Cryptosystems(PQCs) which is resistent to quantum computers. In this paper, we consider the quantum security of the CBC encryption schemes in the NIST PQC standardization project 4th Round now.

Keywords: Code-based cryptosystem, MMT/BJMM algorithm, Grover's algorithm, Quantum walk search algorithm

1. はじめに

現代の情報化社会において，安全な通信を実現するために公開鍵暗号系が用いられている．1994 年に Shor が素因数分解問題や離散対数問題を多項式時間で解く量子アルゴリズムを提案したことにより，大規模な量子計算機の実現後には，現在広く普及している RSA 暗号などの公開鍵暗号系の安全性が失われてしまう．そこで，量子計算機に耐性のある耐量子計算機暗号（PQC）を考える必要があり，実際，近年，量子計算機の開発が急速に進展しており，PQC の早急な実用化が期待されている．

[1] 千葉大学大学院 融合理工学府 数学情報科学専攻 数学・情報数理学コース
Department of Mathematics and Informatics, Division of Mathematics and Informatics, Graduate School of Science and Engineering, Chiba University
[2] 千葉大学 大学院理学研究院
Graduate School of Science, Chiba University
a) ahha3764@chiba-u.jp
b) m.tada@faculty.chiba-u.jp

1.1 シンドローム復号問題（SDP）

$x \in \mathbb{F}_2^n$ に対して，$\mathrm{wt}(x)$ で x の非零要素の数を表す．SDP とは，正整数 n, k, w と行列 $H \in \mathbb{F}_2^{(n-k)\times n}$，ベクトル $s \in \mathbb{F}_2^{n-k}$ が与えられたとき，$He = s$ かつ $\mathrm{wt}(e) = w$ なる $e \in \mathbb{F}_2^n$ を求める問題である．SDP は NP 困難な問題である [17] ことが知られているため，SDP を安全性の根拠とする符号ベース暗号は，PQC だと考えられている．2016 年から米国国立標準技術研究所（NIST）が PQC の標準化を進めており，2021 年 8 月現在は第 4 ラウンドである．BIKE [14]，Classic McEliece [1]，HQC [15] の 3 方式が第 4 ラウンドに

符号ベース暗号の候補として残っている．

1.2 Information Set Decoding （ISD）アルゴリズム

SDP を効率よく解けるアルゴリズムとして, ISD アルゴリズムが知られている．古典版の ISD アルゴリズムは，1962 年に Prange [21] が提唱し，その後様々な派生がある．また，量子版の ISD アルゴリズムを，2010 年に Bernstein [3] が提案した．本稿では，古典から 2011 年の MMT [12] と 2012 年の BJMM [2]，量子から 2018 年の Kirshanova [10] を取り上げる．量子版の MMT/BJMM アルゴリズムは，2017 年に Kachigar [9] らによって提案された．その後 Kirshanova [10] が改善し，著者が調べた限りでは，現状最善の量子 ISD アルゴリズムである．古典 MMT/BJMM アルゴリズムの概要を第２節で展開し，Kirshanova によるその量子版は第４節で与える．

1.3 先行研究

符号ベース暗号は 1978 年の McEliece 暗号 [13] に由来するため，符号ベース暗号の古典での安全性に関する研究は多くある．例えば，2021 年には，Esser, Bellini [5] らによって，Estimator という，ISD アルゴリズムのより現実に即した計算量を算出する手法が提案されている．また，成定ら [16] によって，ISD アルゴリズムの一部を並列化することで，高次元の SDP を解読した手法も知られている．しかし，量子からの安全性に関する研究は，著者が調べた限り少ない．Perriello ら [19] は，BIKE と Classic McEliece に対して，Bernstein のアルゴリズムを使った攻撃手法を提案している．その後，Perriello ら [20] は，ISD アルゴリズムの１つである Lee-Brickell のアルゴリズム [11] の量子版を考えることで，上記の攻撃手法を改善している．また，Esser ら [6] によって，Bernstein のアルゴリズムを用いた別の攻撃手法が提案され，更にその対象の暗号化方式が，HQC を含む第４ラウンド全方式に拡張されている．

1.4 本稿の目的と構成

本稿では，Kirshanova [10] による量子 MMT/BJMM アルゴリズムを実行する量子回路と等価な古典回路の計算コストの導出方法を提案する．また，量子 MMT/BJMM アルゴリズムを用いた攻撃手法に対する NIST の PQC 標準化プロジェクト第４ラウンドでの全ての符号ベース暗号方式の安全性を考察する．結果として，量子 MMT/BJMM アルゴリズムを用いた攻撃手法の計算コストは，Bernstein のアルゴリズムを用いた場合の計算コストを下回った．更に，今回の手法で得られる計算コストは，先行研究 [19] よりも少ないことを確認した．

本稿は次のように構成される．まず，第１章では，SDP の定義と ISD アルゴリズムの概要について述べた．第２章では，古典の MMT/BJMM アルゴリズムの概要を説明する．

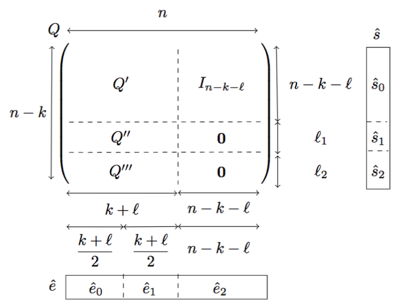

図 1　古典 MMT/BJMM アルゴリズムでの分割

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

第３章では，量子計算とグローバーのアルゴリズム [7]，そして Quantum walk 探索アルゴリズム [9] [10] を導入する．第４章では，以上の準備をもとに量子 MMT/BJMM アルゴリズムを与える．第５章では，BIKE, Classic McEliece, HQC で用いられているパラメタを整理する．第６章では，第５章で与えた方式に対して，量子 MMT/BJMM アルゴリズムを用いた攻撃方針と結果を考察する．最後の第７章で，結論を述べる．

2. 古典 MMT/BJMM アルゴリズム [12] [2]

SDP でのインプット n,k,w,H,s を以下では固定する．$n \times n$ 置換行列 P と HP に対して Gauss の消去法を実行する行列を U とする．$Q = UHP, \hat{e} = P^{-1}e, \hat{s} = Us$ と置くと，SDP での $He = s$ は $Q\hat{e} = \hat{s}$ と同値である．$Q, \hat{e}, \hat{s}$ は **図 1** のようになる．つまり，Q の右上 $(n-k-\ell) \times (n-k-\ell)$ ブロック行列は単位行列であり，右下 $\ell \times (n-k-\ell)$ ブロック行列は零行列である．更に，$\ell_1 + \ell_2 = \ell$ なるパラメタ ℓ_1, ℓ_2 を取る．Q の行を $n-k-\ell, \ell_1, \ell_2$ と分割し，Q の左側 $(n-k) \times (k+\ell)$ ブロック行列を上から順に Q', Q'', Q''' と置く．同様の分割を $\hat{s}$ にも行い，上から順に $\hat{s}_0, \hat{s}_1, \hat{s}_2$ とする．また，$\hat{e}$ を $\frac{k+\ell}{2}, \frac{k+\ell}{2}, n-k-\ell$ と分割し，それぞれを $\hat{e}_0, \hat{e}_1, \hat{e}_2$ とする．このとき，MMT では，$\mathrm{wt}(\hat{e}_0) = p/2, \mathrm{wt}(\hat{e}_1) = p/2, \mathrm{wt}(\hat{e}_2) = w-p$ として, BJMM では，$\mathrm{wt}(\hat{e}_0) = p/2+2\varepsilon, \mathrm{wt}(\hat{e}_1) = p/2+2\varepsilon, \mathrm{wt}(\hat{e}_2) = w-p-4\varepsilon$ とする．MMT/BJMM アルゴリズムでは，SDP は次の generalised 4-sum problem （G4SP）に帰着できる．

$$V_0 = \{(\hat{e}_0, 0^{\frac{k+\ell}{4}}, 0^{\frac{k+\ell}{2}}) \in \mathbb{F}_2^{k+\ell} \mid \hat{e}_{00} \in \mathbb{F}_2^{\frac{k+\ell}{4}}, \mathrm{wt}(\hat{e}_{00}) = \frac{p}{4}\},$$
$$V_1 = \{(0^{\frac{k+\ell}{4}}, \hat{e}_1, 0^{\frac{k+\ell}{2}}) \in \mathbb{F}_2^{k+\ell} \mid \hat{e}_{01} \in \mathbb{F}_2^{\frac{k+\ell}{4}}, \mathrm{wt}(\hat{e}_{01}) = \frac{p}{4}\},$$
$$V_2 = V_0,\ V_3 = V_1$$

とする（BJMM では，上記の重み $p/4$ を $p/4+\varepsilon$ へ変更する）とき，G4SP は次を満たす $(v_0, v_1, v_2, v_3) \in V_0 \times V_1 \times V_2 \times V_3$ を求める問題になる．

Algorithm 1 古典 MMT/BJMM アルゴリズム

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: $P \xleftarrow{\$} n \times n$ 置換行列全体
4: $Q,U \leftarrow GE(HP)$
5: $\hat{s} \leftarrow Us$
6: $\hat{e} \leftarrow$ G4SP_BD$(Q,p,\ell_1,\ell_2,\hat{s})$
7: **if** wt$(\hat{e}) == w-p-4\varepsilon$ **then**
8: $e \leftarrow P\hat{e}$
9: **end if**
10: **end while**
11: return e

$$\begin{cases} Q''(v_0+v_1) & = 0^{\ell_1} & (1) \\ Q''(v_2+v_3)+\hat{s_1} & = 0^{\ell_1} & (2) \\ Q'''(v_0+v_1)+Q'''(v_2+v_3)+\hat{s_1} & = 0^{\ell_2} & (3) \\ Q'(v_0+v_1)+Q'(v_2+v_3)+\hat{s_0} & = 0^{n-k-\ell} & (4) \end{cases}$$

古典 MMT/BJMM アルゴリズムでは，Birthday Decoding アルゴリズムをサブルーチンとして上記の (v_0,v_1,v_2,v_3) を探索する．以上をまとめて，古典 MMT/BJMM アルゴリズムの擬似コードは，**Algorithm 1** となる．MMT アルゴリズムでは，$\varepsilon=0$ である．ここで，4 行目の GE とは，行列 HP に対する Gauss の消去法を行うサブルーチンのことであり，6 行目の G4SP_BD とは，Birthday Decoding アルゴリズムを用いて，G4SP を解くサブルーチンを表す．まず，e を 0^n で初期化し，2-10 行目の while 文内で，e の値が更新されたら，Classical MMT/BJMM アルゴリズムは停止する．1 回のループでは，まず，3 行目で $n\times n$ 置換行列 P をランダムに選ぶ．4, 5 行目で $Q,\hat{s}$ が **図 1** の形式である場合には，6 行目で **図 1** の $\hat{e}$ を得る．その $\hat{e}$ は，7 行目の if 文の条件に合致するため，8 行目で e の値が更新される流れである．2-10 行目の while 文のループの実行回数は，$\frac{\binom{n}{w}}{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}$ 回である [12] [2]．

3. 量子計算/量子アルゴリズム

本章では，量子計算の簡単な導入の後に，Grover のアルゴリズムと Johnson graph 上の Quantum walk 探索アルゴリズムについて解説する．

3.1 量子計算

H を n 次元 Hilbert 空間とする．$1\le i,j\le n$ とするとき，H の元 $|i\rangle$ は，n 次元ベクトルであって，i 番目の要素が 1 で、それ以外の要素が全て 0 であるようなベクトルとする．つまり，$\{|1\rangle,\cdots,|n\rangle\}$ は H の正規直交基底である．$|ij\rangle := |i\rangle\otimes|j\rangle$ とする．$|ij\rangle=|i\rangle|j\rangle$ とも書く．H の量子状態 $|\psi\rangle$ は, $|\psi\rangle=\sum_{i=1}^{n}\alpha_i|i\rangle$ で表される．ここで, $(\alpha_1,\cdots,\alpha_n)\in\mathbb{C}^n$ かつ $\sum_{i=1}^{n}|\alpha_i|^2=1$ である．$f:H\to H$ で f が線型のとき，f を演算子という．以降は演算子とその表現行列を同一視する．f がユニタリ行列のとき，f をユニタリ演算子や量子ゲートと呼ぶ．Clifford ゲートとは，H ゲート，S ゲート，CNOT ゲートからなる量子ゲートの集合であり，それぞれ次のように表せる:

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

T ゲートとは，$\mathrm{T}=\begin{pmatrix}1 & 0\\ 0 & e^{\frac{i\pi}{4}}\end{pmatrix}$ で表される量子ゲートであり，Clifford ゲートと T ゲートの和集合を Clifford+T ゲートという．

3.2 Grover のアルゴリズム [7]

$V=\{0,1\}^n$ として，M を V の空でない部分集合とする．$f:V\to\{0,1\}$ を $f(v)=1$ ($v\in M$ のとき) かつ $f(v)=0$（それ以外）と定める．Grover のアルゴリズムとは，(V,f) をインプットとして，$x_0\in M$ なる x_0 を探索する量子アルゴリズムである．その計算量は $O\left(\sqrt{|V|/|M|}\right)$ である．H^V を V が付随する Hilbert 空間として，H^V 上のユニタリ演算子 U_o,U_d を次で定める:

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

ここで, $\mathrm{H}^{\otimes n}=\underbrace{\mathrm{H}\otimes\cdots\otimes\mathrm{H}}_{n\text{ 個}}$ であり, H ゲートの n 個の Tensor 積を表す．U_o はオラクル演算子であり，U_d は diffuser と呼ばれる．このとき，Grover のアルゴリズムは **Algorithm 2** で書ける．1, 2 行目で $|\psi\rangle$ の初期化と全状態の重ね合わせに変更する．そして，3-6 行目で $|\psi\rangle$ に適切な回数 U_o,U_d を順に掛けて，最後に測定することで x_0 を得る．$\theta=\arcsin\left(\sqrt{|M|/|V|}\right)$ とする．$\phi=\theta$ として，ϕ の値は 1 回のループで 2θ だけ加算され，ϕ が $\frac{\pi}{2}$ に近いときに測定する．よって，測定までの適切なループ回数は，$\lfloor\pi/(4\theta)\rfloor$ となる．

3.3 Quantum walk （QW）探索アルゴリズム [9] [10]

Johnson graph（JG） $J(x,r)$ とは，$v\subset\{1,2,\cdots,x\}$ かつ $|v|=r$ なる v を頂点とし，頂点 u,v において，$|u\bigcap v|=r-1$ の時に限り，u と v は隣接しているグラフのことである．特に $r=1$ のとき, JG は完全グラフである．$G=J(x,r)=(V,E)$

Algorithm 2 Grover のアルゴリズム

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 $\left\lfloor \dfrac{\pi}{4\arcsin(\sqrt{\frac{|M|}{|V|}})} \right\rfloor$ **do**
4: $\quad |\psi\rangle \leftarrow U_o|\psi\rangle$
5: $\quad |\psi\rangle \leftarrow U_d|\psi\rangle$
6: **end for**
7: return $|\psi\rangle$

Algorithm 3 QW 探索アルゴリズム

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 $\left\lfloor \dfrac{1}{\sqrt{\varepsilon\delta}} \right\rfloor$ **do**
4: $\quad |\psi\rangle \leftarrow U_o|\psi\rangle$
5: $\quad |\psi\rangle \leftarrow U_d|\psi\rangle$
6: **end for**
7: return $|\psi\rangle$

として，M を V の空でない部分集合とする．以降では，V に適切に辞書式順序を入れることで，V と $\{1,2,\cdots,\binom{x}{r}\}$ を同一視する．ここで，G の隣接行列を A_G，G の確率遷移行列を P_G と置いて，$P_G = \dfrac{A_G}{r(x-r)}$ とする．つまり，任意の頂点に対して，隣接する頂点は $r(x-r)$ 個あり，それぞれの頂点への遷移確率は $\dfrac{1}{r(x-r)}$ である．QW 探索アルゴリズムは，G, M, P_G をインプットとするとき，M に属する頂点を探索する量子アルゴリズムである．Grover のアルゴリズムは，1 次元配列に対する探索アルゴリズムに対して，QW 探索アルゴリズムは，グラフなどの 2 次元配列に対する探索アルゴリズムである．実際，各頂点にループをつけた完全グラフ上の QW 探索アルゴリズムは，Grover のアルゴリズムと見なせる．一般に，JG は無向グラフである．しかし，以下では辺の量子状態を考えるため，任意の無向辺を双方向の有向辺とみなして，JG を有向グラフとする．以降では，頂点 i の量子状態を $|i\rangle$ とし，i から隣接する頂点 j に向かう辺の量子状態を $|ij\rangle$ とする．H^E を E が付随する Hilbert 空間として，H^E 上のユニタリ演算子 U_o, U_d を次で定める:

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

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

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

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

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

$$U_d(|i\rangle|j\rangle) := U_{dL}(U_{dR}(|i\rangle|j\rangle))$$

オラクル演算子 U_o は Grover のアルゴリズムと同様である．$|\Phi\rangle_x$ は，頂点の量子状態 $|x\rangle$ と係数を x からの遷移確率のルートとする全頂点の量子状態の総和の Tensor 積で表される．係数が遷移確率のルートとなのは，2 乗の総和が 1 にするための調整である．そして，$|\Phi\rangle_x$ からユニタリ演算子 U_{dR} を構成する．$|\Phi\rangle_x$ は，長さが $|V| \times |V|$ のベクトルゆえ，U_{dR} は $|V| \times |V|$ の行列となる．$|\Psi\rangle_y, U_{dL}$ も同様に構成され，$U_d = U_{dL}U_{dR}$ とする．このとき，QW 探索アルゴリズムは，**Algorithm 3** で与えられる．ここで，$\varepsilon = |M|/|V|$ であり，$\delta = x/(r(x-r))$ は spectral gap と呼ばれる．1, 2 行目は，Grover のアルゴリズムと同様である．そして，3-6 行目で $|\psi\rangle$ に適切な回数 U_o, U_d を順に掛けて，最後に測定することで x を得る．

4. 量子 MMT/BJMM アルゴリズム [10]

本章では，古典 MMT/BJMM アルゴリズム，Grover のアルゴリズム，QW 探索アルゴリズムを組合せることで，量子 MMT/BJMM アルゴリズムを与える．Grover のアルゴリズム, QW 探索アルゴリズムをサブルーチンとして用いて，**Algorithm 1** の 3, 6 行目それぞれを改善することが目標である．これら 2 つのアルゴリズムをどのようにしてサブルーチンとして組み込むかについて解説する．まず，6 行目では，QW 探索アルゴリズムを用いる．有限グラフ $G_1 = (V_1.E_1), G_2 = (V_2, E_2)$ に対して，G_1 と G_2 の直積 $G := G_1 \times G_2 = (V, E)$ は，$V = V_1 \times V_2$，$E = \{(u_1u_2, v_1v_2) \mid (u_1 = v_1 \wedge (u_2, v_2) \in V_2) \vee ((u_1, v_1) \in E_1 \wedge u_2 = v_2)\}$ で与えられる．G を JG の直積とする．$0 \leq i \leq 3$ として，G4SP での V_i において, r 個の要素を持つ V_i の部分集合全体は JG ゆえ, $J_i(N,r)$ と置ける．ここで，$N = \binom{\frac{k+\ell}{4}}{\frac{p}{4}}$ である．また，r は G4SP を満たす (v_0, v_1, v_2, v_3) の個数であり，$r = N^{\frac{4}{7}} \cdot \binom{p}{\frac{p}{2}}^{\frac{2p}{7}}$ で与えられる [10]．そして，$J(N,r) = J_0(N,r) \times \cdots \times J_3(N,r)$ とする．以上より，$G = J(N,r)$ として，P_G を G の確率遷移行列，M を G4SP の条件を満たす $J(N,r)$ 上の頂点全体の集合とすると，**Algorithm 1** の 6 行目で，QW 探索アルゴリズムをサブルーチンとして用いることができる．次に，3 行目では，Grover のアルゴリズムを用いる．V を $n \times n$ 置換行列全体とする．また，関数 $f : V \to \{0,1\}$ は，上記の QW 探索アルゴリズムによって，G4SP を満たす (v_0, v_1, v_2, v_3) が存在すれば 1，そうでないときに 0 を返す．より詳細には，以

Algorithm 4 量子 MMT/BJMM アルゴリズム

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: $\quad P \leftarrow \mathrm{Grover}(\ell,H)$
4: $\quad Q,U \leftarrow GE(HP)$
5: $\quad \hat{s} \leftarrow Us$
6: $\quad \hat{e} \leftarrow \mathrm{G4SP\_QW}(Q,p,\ell_1,\ell_2,\hat{s})$
7: $\quad$ **if** $\mathrm{wt}(\hat{e}) == w-p-4\varepsilon$ **then**
8: $\quad\quad e \leftarrow P\hat{e}$
9: $\quad$ **end if**
10: **end while**
11: return e

下の通りである．$P \in V$ と H を用いて HP に対して Gauss の消去法を実行した際に，$Q = UHP$ が **図 1** の形式とする．つまり，Q の右上 $(n-k-\ell)\times(n-k-\ell)$ ブロック行列が単位行列かつ Q の右下 $\ell\times(n-k-\ell)$ ブロック行列が零行列であるとする．$Q,\hat{s}=Us$ を用いて，6 行目のサブルーチン内で (v_0,v_1,v_2,v_3) を探索する．P から $U,Q,\hat{s}$ は一意に定まり，G4SP の条件を満たす (v_0,v_1,v_2,v_3) が存在するかは高い確率で判定できる．よって，上記のように V,f を構成することで，**Algorithm 1** の 3 行目で Grover のアルゴリズムをサブルーチンとして用いることができる．以上の準備をもとに，量子 MMT/BJMM アルゴリズムは **Algorithm 4** で与えられる．**Algorithm 4** の 3 行目の Grover とは，Grover のアルゴリズムを用いて置換行列 P を探索するサブルーチンを表す．また，6 行目の G4SP_QW とは，QW 探索アルゴリズムを用いて，G4SP を解くサブルーチンを表す．3, 6 行目以外は **Algorithm 1** と同様である．2-10 行目の while 文のループの実行回数 ℓ_{Grover} は，Grover のアルゴリズムの計算量から，$\ell_{\mathrm{Grover}} = \sqrt{\frac{\binom{n}{w}}{\binom{k+\ell}{p}\binom{n-k-\ell}{w-p}}}$ 回である．また，6 行目での QW 探索アルゴリズムのループの実行回数 $\ell_{\mathrm{BJMM\_QW}}$ は，$\ell_{\mathrm{BJMM\_QW}} = \frac{\binom{\frac{k+\ell}{2}}{\frac{p}{4}}^{\frac{8}{7}}}{\binom{p}{\frac{p}{2}}^{\frac{3p}{7}}\binom{k+\ell-p}{\varepsilon}^{\frac{3p}{7}}}$ である [10]．この実行回数で G4SP の条件を満たす (v_0,v_1,v_2,v_3) を探索し，$\hat{e}$ を構成する．7 行目の if 文の条件に合致した際に，e の値が更新されて，**Algorithm 4** は停止する．

5. 対象の暗号化方式 [14] [1] [15]

本章では，NIST PQC 標準化プロジェクト第 4 ラウンドに残っている暗号化方式 BIKE, Classic McEliece, HQC について解説する．詳細なプロトコルについては，それぞれ [14] [1] [15] を参照されたい．それぞれの暗号化方式と各 security bit に対応する SDP のインスタンスの一覧が **表 1** である．

暗号化方式	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

表 1　対象とする暗号化方式と security bit
Table 1　Targeted cryptosystems and security bits

6. 本研究の分析方針と結果

本章では，前章で述べたパラメタをインプットとする SDP に対して，量子 MMT/BJMM アルゴリズムを用いた攻撃手法とその結果について考察する．分析方針の概要を解説する．まず，新たな計算コストとして，G-cost, D-cost, W-cost を導入する．次に，**Algorithm 4** を実行する Clifford+T ゲートからなる量子回路を考える．演算を実行する古典回路を Clifford+T ゲートによって再構成し，それぞれの各計算コストが入力量子ビット数の定数倍で抑えられることを確認する．前節で与えられたインスタンスをそれらのコストに代入して得られる結果から，各方式・security bit が今回の攻撃手法に対して安全かどうかを考察する．

6.1 計算コストの導入と比較方法の提案

本節では，Jaques らの論文 [8] に沿って，本稿で用いる計算コストを導入する．Clifford+T ゲートからなる量子回路 C を考える．C に現れる量子ゲートの総数を G-cost という．C の深さを D-cost といい，C の量子ビット数を W-cost という．これらの計算コストは $\log_2$ で評価する．また，本稿では，主に G-cost を用いて各方式・security bit と比較する．これらの計算コストは，Clifford+T ゲートに含まれる量子ゲートは，古典回路における RAM 演算と等価とする計算モデルに基づく．このモデルは memory peripheral model と呼ばれる．本稿では，Jaques らの論文 [8] に沿って，量子状態の重ね合わせに関しては考慮しない．重ね合わせは，量子 RAM 演算では実行できるが，古典 RAM 演算では実行できないためである．よって，Grover のアルゴリズムと QW 探索アルゴリズムそのものの計算コストは無視する．以降では，量子 MMT/BJMM アルゴリズム内で行われる演算について，G-cost などを考察する．

6.2 量子ビットの和と行列の積の計算コスト

以下では，ℓ,m,n を正整数として，$a,b \in \mathbb{F}_2^m$, $A \in \mathbb{F}_2^{\ell\times m}$, $B \in \mathbb{F}_2^{m\times n}$ とする．$|a\rangle = |a_1\cdots a_m\rangle, |b\rangle = |b_1\cdots b_m\rangle$ である．このとき，$|a\rangle$ と $|b\rangle$ の和を $|a\rangle + |b\rangle := |a+b\rangle$ と定める．つま

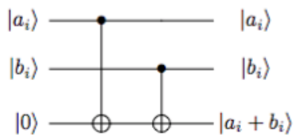

図 2　1 量子ビットの和
Fig. 2　The addition for one qubit

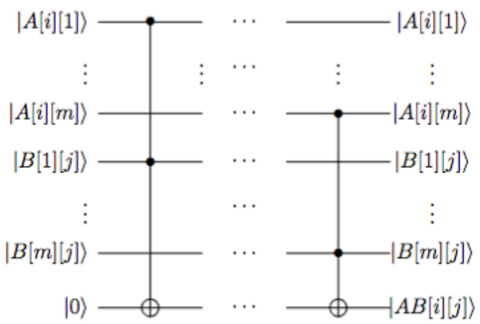

図 3　量子ビットの行列の積
Fig. 3　The matrix products for qubits

り，m 量子ビット $|a\rangle$ と $|b\rangle$ の和は，$a,b \in \mathbb{F}_2^m$ と見たときの $a+b$ の量子状態 $|a+b\rangle$ に対応する．すると，$1 \leq i \leq m$ として，$|(a+b)[i]\rangle = |a_i + b_i\rangle$ である．$|a_i\rangle$ と $|b_i\rangle$ から $|a_i + b_i\rangle$ を算出する量子回路を考える．そのような量子回路は，**図 2** のように CNOT ゲート 2 つで実現できる．つまり，m 量子ビット $|a\rangle$ と $|b\rangle$ の和である $|a+b\rangle$ を実現する量子回路の G-cost は，$2m$ であり，D-cost は 2，W-cost は $3m$ となる．

続いて，$\ell \times m$ 行列 A に対応する量子状態 $|A\rangle$ と $m \times n$ 行列 B に対応する量子状態 $|B\rangle$ の積を考える．これは，A と B の積である $\ell \times n$ 行列 AB に対応する量子状態 $|AB\rangle$ である．すると，$1 \leq i \leq \ell$, $1 \leq j \leq n$ として，$|AB[i][j]\rangle = |\sum_{k=1}^{m} A[i][k]B[k][j]\rangle$ を実行する量子回路を考えればよい．そのような量子回路は，**図 3** のように Toffoli ゲート m 個で実現できる．ここで，Toffoli ゲートとは，次で表される量子ゲートである．

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

Shende [22] らの論文によって，Clifford+T ゲートによる Toffoli ゲートの構成が与えられている．その際の量子回路の G-cost が 24，D-cost が 16，W-cost が 3 である．よって，

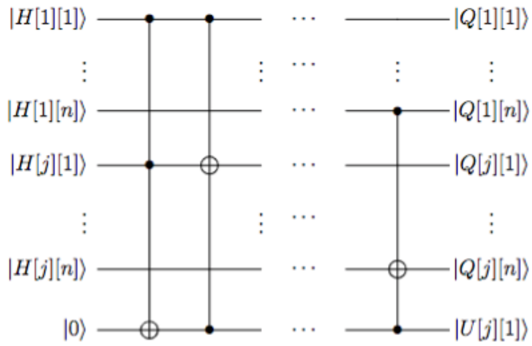

図 4　1 行目と j 行目に対する Gauss の消去法
Fig. 4　The Gaussian Elimination for 1 and j rows

$|A\rangle$ と $|B\rangle$ から $|AB\rangle$ を求める量子回路の G-cost は $24\ell mn$，D-cost は $16m$，W-cost は $\ell m + \ell n + mn$ となる．

6.3　Gauss の消去法の計算コスト

本節では，$H \in \mathbb{F}_2^{(n-k)\times n}$ なる行列に対して，Gauss の消去法を実行する行列 $U \in \mathbb{F}_2^{(n-k)\times(n-k)}$ と実行後の $Q = UH \in \mathbb{F}_2^{(n-k)\times n}$ を出力する量子回路を考える．つまり，H に対応する量子状態 $|H\rangle$ に対して，Gauss の消去法に対応する行列の量子状態 $|U\rangle$ と実行後の行列に対応する量子状態 $|Q\rangle$ を算出する．$1 \leq i < j \leq n-k$ に対して，H の 1 行目と j 行目でのプロセスを実行する量子回路を考えればよい．そのような量子回路は，**図 4** のように Toffoli ゲート $n+1$ 個で実現できる．よって，H の i 行目と j 行目での Gauss の消去法を実行する量子回路は，Toffoli ゲート $n-i+2$ 個で構成できる．以上より，Gauss の消去法を行う全体の量子回路は，Toffoli ゲート $\sum_{i=1}^{n-k-1}(n-k-i)(n+2-i)$ 個から構成される．その量子回路の G-cost は $4(n-k-1)(n-k)(2n+k+5)$，D-cost は $16(n-k-1)$，W-cost は $2(n-k)n + (n-k)^2$ となる．

6.4　量子状態の Hamming 重みの算出の計算コスト

本節では，与えられた量子状態 $|\psi\rangle = |p_1 \cdots p_n\rangle$ の Hamming 重み，つまり，$\psi \in \mathbb{F}_2^m$ と見たときの $\mathrm{wt}(\psi)$ を算出することを考える．1 量子ビット 3 つに対する adder を考える．この adder を本稿では 3-1-adder と呼ぶことにする．つまり，$a,b,c,s,d \in \mathbb{F}_2$ に対して，$\mathbb{F}_2$ 上の和として，$a+b+c = sd$ とする．ここで，sd は $s,d \in \mathbb{F}_2$ の連結であり，$s=0$ のとき，$sd = d$ とする．この和に対応する量子状態 $|a\rangle + |b\rangle + |c\rangle = |sd\rangle$ を実現する量子回路を考える．

そのような量子回路は，**図 6** のように Toffoli ゲート 2 個と CNOT ゲート 3 個で実現できる．よって，3-1-adder を実現する量子回路の G-cost は 51，D-cost は 32，W-cost は 5 である．

以上の準備をもとに，量子状態の Hamming 重みを考察する．Luis [4] らの論文に古典 10 ビットでの Hamming 重みを算出する回路が掲載されている．その古典回路中

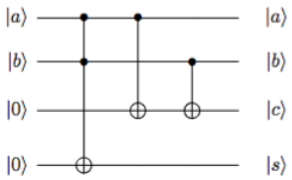

図 5　量子ビットの half-adder

Fig. 5　Half-adder for qubit

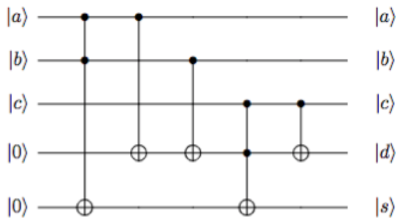

図 6　量子ビットの 3-1-adder

Fig. 6　3-1-adder for qubit

演算操作	G-cost	D-cost	W-cost
和	$2m$	2	$3m$
行列の積	$24\ell mn$	$16m$	$\ell m+\ell n+mn$
GE	$4(n-k-1)\times (n-k)(2n+k+5)$	$16(n-k-1)$	$2(n-k)n+ (n-k)^2$
重み	$\leq 51(n-1)$	32	$n+2(n-1)+ \lceil\log_2 n\rceil$

表 2　量子 MMT/BJMM アルゴリズムの演算コスト

Table 2　Cost for quantum MMT/BJMM algorithm operations

の HA, FA をそれぞれ half-adder, 3-1-adder と読み替えることで，量子状態の Hamming 重みを算出する量子回路を構成することができる．なお，half-adder を実行する量子回路は，**図 5** のようになる．よって，$|\psi\rangle = |p_1 \cdots p_n\rangle$ の Hamming 重みを導出する量子回路は，half-adder, 3-1-adder 合わせて $\sum_{i=1}^{\lceil\log_2 n\rceil} \left\lceil \frac{n}{2^i} \right\rceil$ 個必要である．つまり，高々 $n-1$ 個の 3-1-adder があれば十分ゆえ，$|\psi\rangle$ の Hamming 重みを算出する量子回路の G-cost は $51(n-1)$，D-cost は 32，W-cost は $n+2(n-1)+\lceil\log_2 n\rceil$ となる．

6.5　量子 MMT/BJMM アルゴリズムの計算コスト

前節までの結果が **表 2** である．GE とは，Gauss の消去法を表す．本節では，量子 MMT/BJMM アルゴリズムの G-cost などを導出する．**Algorithm 4** での while 文内の 1 回のループでは，前節までのいずれかの操作しか行なっていない．よって，量子 MMT/BJMM アルゴリズム全体を実行する量子回路は，Clifford+T ゲートから構成されるため，その量子回路の G-cost などを求めることができる．i 行目の G-cost, D-cost, W-cost をそれぞれ G_i, D_i, W_i とする．6 行目の G4SP の 4 条件を表す量子回路の G-cost を $G_{6,G4SP}$ とする．全体の G-cost G は，$G = (G_4 + G_5 + G_{6,G4SP}\ell_{\mathrm{BJMM\_QW}} + G_7)\ell_{\mathrm{Grover}} + G_8$ で与えられる．全体の D-cost D は，$D = \max\{D_4, D_5, D_6, D_7\} \cdot \ell_{\mathrm{Grover}}$ で与えられる．全体の W-cost W は，各パラメタの量子ビットと前節までの導入で現れる補助量子ビットの和である．

暗号化方式	security bit	G-cost	D-cost	W-cost
BIKE	128(143 gates)	116	86	31
		112	79	30
	192(207 gates)	213	84	66
		207	79	64
	256(272 gates)	322	88	102
		315	83	99
Classic McEliece	128(143 gates)	110	88	25
		104	77	23
	192(207 gates)	188	77	52
		178	70	48
	256(272 gates)	384	84	108
		320	90	75
HQC	128(143 gates)	116	86	32
		113	79	31
	192(207 gates)	216	85	68
		212	80	66
	256(272 gates)	322	88	105
		316	83	102

表 3　それぞれの方式と security bit に対するコスト

Table 3　Cost for each cryptosystem and security bit

暗号化方式	security bit	[19]	本研究
BIKE	128	138	115
	192	176	149
	256	212	189
Classic McEliece	128	124	111
	192	149	127
	256	209	176

表 4　T ゲートの個数で評価した DW コスト

Table 4　DW-cost evaluated by the number of T gates

6.6　比較方法の提案と結果

第 5 章で導入した 128, 192, 256 security bit に相当する古典回路は，それぞれ $2^{143}, 2^{207}, 2^{272}$ 個の古典ゲートを持つ回路と等価であると NIST [18] は主張している．よって，1 つの古典ゲートを 1 つの古典計算機による RAM 演算とみなすことで，G-cost と上記の個数を直接比較できる．例えば，128 security level の方式に対して，その G-cost が 143 よりも大きければ，今回の攻撃手法に対して安全だと言える．

各パラメタの制約条件は Becker らによる古典 BJMM アルゴリズム [2] での論文の条件に沿っている．また，D-cost は，NIST からの条件により，96 以下に限定されている．それぞれの暗号化方式と各 security level に対応する計算コ

ストの一覧を **表 3** に示している．各計算コストの上段は，Bernstein のアルゴリズムを今回の攻撃手法に組み込んだ際の計算コストを表す．下段は，量子 MMT/BJMM アルゴリズムを用いた場合での計算コストである．結論として，security level が低い場合には，今回の攻撃手法による計算コストが下回った．更に，量子 MMT/BJMM アルゴリズムの計算コストが Bernstein のアルゴリズムの計算コストを下回った．また，先行研究と今回の手法の比較として，Bernstein のアルゴリズムを用いた場合での，BIKE, Classic McEliece と各 security bit での T ゲートベースの DW-cost の一覧を **表 4** に示している．T ゲートベースのコストとは，G-cost, D-cost の定義で，全量子ゲートから T ゲートのみに制限したものである．DW-cost とは，D-cost と W-cost の積を表す．結果として，本研究のコストが先行研究のコストを下回った．

7. まとめ

本稿では，NIST の PQC 標準化プロジェクト第 4 ラウンドでの全ての符号ベース暗号方式に対して，Kirshanova による量子 MMT/BJMM アルゴリズムを用いた攻撃手法を提案した．また，古典回路上で G-cost を算出することで，それらの方式の安全性について議論した．符号ベース暗号への量子的な安全性に関する先行論文は，いずれも量子回路上で議論を展開している．著者が調べた限りでは，量子 MMT/BJMM アルゴリズムを用いて並びに古典回路上の G-cost を基準にして，符号ベース暗号の量子的な安全性を議論した研究については，本稿が初である．古典回路上だと，量子 RAM 演算の計算コストを考慮できない．古典回路上での計算コストが，量子回路上での計算コストを下回ることは，**表 4** からも確認できる．よって，**表 3** から各方式の安全性が破られたとは一概には結論づけられない．しかし，今回の結果から，本稿で用いた攻撃手法の妥当性が示された．今後の課題は以下の４つである．まず，量子 MMT/BJMM アルゴリズムの量子回路上の G-cost を導出し，今回の結果との差異を調べたい．また，NIST PQC 標準化プロジェクト第２ラウンドなどでの符号ベース暗号の方式にも対象を広げることが考えられる．更に，Bernstein のアルゴリズムのみならず，使用する量子 ISD アルゴリズムを更に増やしたい．最後に，**表 4** のように，評価の基準を変更した際の計算コストの導出も行いたい．

参考文献

[1] M.R. Albrecht, D.J. Bernstein et. al. : “Classic McEliece”, Tech. rep., National Institute of Standards and Technology (2020).

[2] A. Becker, A. Joux, A. May, and 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.

[4] L.T.A.N. Brandao, C. Çalık, M. S. Turan, R. Peralta: “Upper bounds on the multiplicative complexity of symmetric Boolean functions”, Cryptogr. Commun. 11, 1339–1362 (2019).

[5] A. Esser, E. Bellini: “Syndrome decoding estimator”, In: IACR International Conference on Public-Key Cryptography. Springer, Cham, 2022. p. 112-141.

[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, pages 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, 2017. p. 69-89.

[10] E. Kirshanova: “Improved quantum information set decoding”, In: International Conference on Post-Quantum Cryptography. Springer, Cham, 2018. p. 507-527.

[11] 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, 1988, pp. 275.

[12] A. May, A. Meurer, and 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.

[13] R. J. McEliece: “A public-key cryptosystem based on algebraic coding theory”, Deep Space Network Progress Report, 44:114-116, Jan, 1978.

[14] C. A. Melchor, N. Aragon et. al. : “BIKE”, Tech. rep., National Institute of Standards and Technology (2020).

[15] C. A. Melchor, N. Aragon et. al. : “HQC”, Tech. rep., National Institute of Standards and Technology (2020).

[16] 成定真太郎，福島和英，清本晋作：“Multi-Parallel MMT アルゴリズムによる高次元 SDP の解読”，暗号と情報セキュリティシンポジウム SCIS2022，4A2-1 （2022）．

[17] H. Niederreiter: “Knapsack-type cryptosystems and algebraic coding theory”, Problems of Control and Information Theory, 15(2):159–166, 1986.

[18] NIST: “Post-Quantum Cryptography, Security (Evaluation Criteria)”, available at `https://csrc.nist.gov/projects`.

[19] 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, 2021. p. 366-377.

[20] 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, 2021. p. 458-474.

[21] E. Prange: “The use of information sets in decoding cyclic codes”, Information Theory, IRE Transactions on, 8(5):5–9, September 1962.

[22] V. V. Shende, I. L. Markov: “On the CNOT-cost of TOFFOLI gates”, Quantum Info. Comput. 9, 5 (May 2009), 461–486.