符号ベース署名方式 RYDE に対する量子的な安全性解析

若杉 飛鳥[1,a)]　多田 充[2,b)]

概要：符号ベース暗号は，耐量子計算機暗号（PQC）の 1 つと考えられている．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，2023 年より，署名方式の追加公募を開始し，2025 年 8 月現在は第 2 ラウンドである．RYDE はそのラウンドに残っている署名方式であり，行列同士の rank 距離に基づく符号に関する計算問題である Rank シンドローム復号問題の変種を安全性の根拠としている．Rank シンドローム復号問題に対する解読アルゴリズムとして，Gaborit らによる GRS アルゴリズムが知られている．本稿では，RYDE に対する量子的な安全性について考察する．まず，Rank シンドローム復号問題の変種に対する古典的な GRS アルゴリズムを与える．続いて，そのアルゴリズムと Grover のアルゴリズムを組合せることで，量子版 GRS アルゴリズムを提案する．最後に，RYDE で与えられているインスタンスを用いて，量子版 GRS アルゴリズムを実行するような量子回路を構成する．そのような量子回路の計算コストを算出することで，RYDE の安全性を評価する．

キーワード：符号ベース暗号，Rank シンドローム復号問題，GRS アルゴリズム，Grover のアルゴリズム

Quantum cryptanalysis for code-based signature scheme RYDE

ASUKA WAKAUSUGI[1,a)]　MITSURU TADA[2,b)]

Abstract: Code-based cryptography is considered to be one of the quantum computer resistant cryptosystems (PQC). Since 2016, the National Institute of Standards and Technology (NIST) has been working on the standardization of PQC. In 2023, NIST began to standardize additional signature schemes, and as of August 2025, it is in the second round of standardization. RYDE is one of the remaining signature schemes in the round, and its security is based on a variant of the Rank Syndrome Decoding problem, which is a computational problem for codes based on the rank distance between matrices. As a decoding algorithm for the Rank syndrome decoding problem, the GRS algorithm by Gaborit et al. is known as a decoding algorithm for the Rank syndrome decoding problem. In this paper, we consider quantum security for RYDE. First, we give the classical GRS algorithm for a variant of the Rank syndrome decoding problem. Then, by combining the algorithm with Grover's algorithm, we propose a quantum version of the GRS algorithm. Finally, we construct a quantum circuit that implements the quantum GRS algorithm using the instances given in RYDE. We evaluate the security for RYDE by the computational costs of the quantum circuit.

Keywords: Code-based cryptography, Rank Syndrome Decoding Problem, GRS algorithm, Grover's algorithm

1. はじめに

符号ベース暗号は，耐量子性を持つ暗号方式の 1 方式と考えられている．符号ベース暗号のうち，公開鍵暗号方式は，1978 年に McEliece [23] によって提案され，署名方式は，2001 年に Courtouis [10] らによって提案された．アメリカの米国国立標準技術研究所（NIST）は，2016 年から，耐量子計算機暗号の標準化を進めており，符号ベース暗号方式 HQC [26] が公開鍵暗号及び鍵カプセル化方式の標準方式として決定された．HQC は，有限体上のベクトルに対する Hamming 距離に基づく Hamming-metric 符号を用いて構成される．さらに，NIST は，2023 年より，耐量子

[1] EAGLYS 株式会社
EAGLYS Inc, Research and Development, Tokyo, Japan
[2] 千葉大学 大学院理学研究院
Graduate School of Science, Chiba University, Chiba, Japan
[a)] a_wakasugi@eaglys.co.jp
[b)] m.tada@faculty.chiba-u.jp

的な署名方式の追加公募を行っており，2025 年 8 月現在は第 2 ラウンドである．第 2 ラウンドにおいては，CROSS [3] や LESS [4] といった符号ベース署名方式が選定されている．また，MPC-in-the-Head 方式に分類される RYDE [2] や SDitH [27] も符号理論に関する計算問題を安全性の根拠とするため，本論文では，符号ベース署名方式として扱う．RYDE は，行列同士の rank 距離に基づく Rank-metric 符号を用いて構成される．

1.1 Rank-metric 符号

q を素数べき，m,n を正整数とする．$x \in \mathbb{F}_{q^m}^n$ に対して，φ_x を $\varphi_x : \mathbb{F}_q^n \ni v \mapsto vx \in \mathbb{F}_{q^m}$ なる線型変換とする．x の rank とは，$\mathbb{F}_q$ による φ_x の像の次元のことで，$\mathrm{rank}_{\mathbb{F}_q}(x)$ と書く．また，長さ n で次元 k の $\mathbb{F}_{q^m}$-線型符号 $\mathscr{C}$ とは，要素数が 2^k 個である $\mathbb{F}_{q^m}^n$ の部分空間のことである．この $\mathscr{C}$ を $[n,k]_{q^m}$ 線型符号と呼ぶ．Rank-metric 符号 $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ とは，rank-metric の意味での $[n,k]_{q^m}$ 線型符号のことである．Rank-metric 符号として，Gabidulin 符号 [13] や LRPC 符号 [14] などが知られている．

1.2 Rank シンドローム復号問題

多くの Hamming-metric 符号による暗号方式の安全性のベースとなる計算問題として，シンドローム復号問題（SDP）が知られている．Rank シンドローム復号問題（Rank SDP）とは，SDP の変種であり，Rank-metric な符号による SDP と考えることができる．Rank SDP は，正整数 q,m,n,k,w と行列 $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$，ベクトル $s \in \mathbb{F}_{q^m}^{n-k}$ が与えられたとき，$He = s$ かつ $\mathrm{rank}_{\mathbb{F}_q}(e) = w$ なる $e \in \mathbb{F}_{q^m}^n$ を求める問題である．一般に H は，パリティ検査行列として与えられ，H から Rank-metric 符号が定まる．Rank SDP そのものが NP 完全であるかは知られていないが，rank SDP が NP 完全な問題に UR reduction [19] できることは知られている [16].

また，RYDE では，Rank SDP の変種である Rank SDP$_s$ を導入している．Rank SDP$_s$ では，正整数 q,m,n,k,w と行列 $H \in \mathbb{F}_{q^m}^{(n-k)\times n}$，ベクトル $s \in \mathbb{F}_{q^m}^{n-k}$ が与えられたとき，$He = s$ かつ $\mathrm{rank}_{\mathbb{F}_q}(e) = w$ かつ $e_1 = 1 \in \mathbb{F}_{q^m}$ かつ $\langle e_1, e_2, \ldots, e_w \rangle_{\mathbb{F}_q} = \mathrm{span}(e)$ なる $e = (e_1, \ldots, e_n) \in \mathbb{F}_{q^m}^n$ を求める問題である．ここで，$\langle e_1, e_2, \ldots, e_w \rangle_{\mathbb{F}_q}$ とは，$\mathbb{F}_q$-線型で $(e_1, e_2, \ldots, e_w)$ によって貼られる $\mathbb{F}_{q^m}$ の部分空間のことであり，$\mathrm{span}(e)$ は $\langle e_1, e_2, \ldots, e_n \rangle_{\mathbb{F}_q}$ を表す．Rank SDP$_s$ は多項式時間で Rank SDP へ帰着できることが知られている [7].

1.3 Rank 符号ベース暗号

Rank 符号ベース暗号とは，前節の Rank SDP を安全性の根拠とするような符号ベース暗号方式である．NIST PQC 標準化プロジェクト第 2 ラウンドまでは，ROLLO [25] と RQC [24] の 2 方式が rank 符号ベース暗号として，標準化の候補に残っていたが，以降のラウンドでは選定されなかった．また，RYDE は Rank SDP を安全性の根拠とする符号ベース署名方式であり，本論文執筆時点では，署名方式追加公募第 2 ラウンドに残っている．

1.4 先行研究

ISD アルゴリズムは Prange [32] が提案し，MMT [22] や BJMM [5] などの派生がある．また，Bernstein [6] によって，Prange のアルゴリズムの量子版や Kachigar ら [20] によって，MMT や BJMM アルゴリズムの量子版も提案されている．Hamming-metric な符号ベース暗号の量子計算に対する安全性に関する研究として，Perriello ら [30] は，Bernstein のアルゴリズムを用いて，既存の Hamming 符号ベース暗号の具体的な方式の安全性解析を行なった．さらに，同研究グループ [31] は，Lee-Brickell [21] のアルゴリズムの量子版を用いて，攻撃手法を改善した．この研究では，量子 ISD アルゴリズムを実行するような量子回路を与え，NIST PQC プロジェクト第 4 ラウンドに残っていた符号ベース暗号方式全てに対して，安全性解析を行った．加えて，Esser ら [12] は，Bernstein のアルゴリズムを用いた，Perriello らとは別の攻撃手法を提案した．Chevignard ら [9] は，Bernstein のアルゴリズムを実行するような量子回路において，Perriello らの手法と比較して，より少ないゲート数による構成を示した．特に，Bernstein のアルゴリズムのサブルーチンである，量子回路上のガウスの消去法に対して，複数の最適化手法を与えた．Bernstein のアルゴリズムを実行する量子回路として，現状最善の構成として知られている．

Rank SDP に対する解読アルゴリズムとして，Gaborit ら [15] による GRS アルゴリズムが知られている．SDP に対して，現状最善だと考えられている手法として，Information Set Decoding（ISD）アルゴリズムが知られている．GRS アルゴリズムは，Rank SDP に対する ISD アルゴリズムの亜種である．2024 年に D'Alconzo ら [11] によって，特定のインスタンスに対して，GRS アルゴリズムの改善版が与えられた．他にも，rank 符号ベース暗号方式に対する攻撃アルゴリズムとして，combinatorial attack や algebraic attack などが知られているが，詳細は RYDE の仕様書 [2] を参照されたい．

Rank-metric な符号ベース暗号方式に対する量子的な安全性の研究として，以前に，我々の研究グループ [34] は，量子 GRS アルゴリズムを提案し，ROLLO と RQC に対して，それを用いた量子的な安全性の解析を行なった．

1.5 本稿の目的と構成

本稿では，Rank SDP$_s$ を解くような GRS アルゴリズムの改良版を提案する．また，上記のアルゴリズムと Grover のアルゴリズムを組合せることで，量子版のアルゴリズムも提供する．我々の研究グループ [34] によって，量子版 GRS

アルゴリズムを実行するような量子回路の回路計算量を算出している．本稿でも，同様のフレームワークに沿って，改良版の量子 GRS アルゴリズムの計算量を解析する．この計算コストは，RYDE で与えられているインスタンスに依存する．結果として，RYDE 仕様書に記載の 128/192/256 bit security を満たす全てのインスタンスに対して，今回の攻撃手法によって，該当 security を下回っていることを確認した．そのため，どのインスタンスをどのような値へ変更すれば，今回の攻撃手法に対して安全になるかの提案も行なった．

本稿は次のように構成される．まず，第 1 章では，rank-metric 符号の定義と Rank SDP の定義について述べた．第 2 章では，Aragon ら [1] による古典 GRS アルゴリズムの概要を説明する．第 3 章では，量子計算と Grover のアルゴリズム [17] を導入する．第 4 章では，Rank SDP$_s$ を解くような，改善版の古典および量子 GRS アルゴリズムを提案する．第 5 章では，RYDE で用いられているパラメタを整理し，それらの方式に対して，量子 GRS 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 6 章で，結論を述べる．

2. Gaborit-Ruatta-Schrek アルゴリズム

本章では，Rank SDP に対する解読アルゴリズムである GRS アルゴリズムを紹介する．以下では，Rank SDP のインスタンス q,m,n,k,w,H,s が与えられているとする．また，$r \geq w$ を正整数とし，$b_{m,r}$ は，$\mathbb{F}_{q^m}$ 上の r 個の線型独立なベクトルとする．$B_{m,r} = \{b_{m,r}\}, V_{m,r} = \mathrm{span}(b_{m,r})$ とおく．このとき，$B_{m,r}$ は $\mathbb{F}_{q^m}$ 上の基底全ての集合であり，$V_{m,r}$ は $\mathbb{F}_{q^m}$ 上の r 次元部分空間全体となる．i,j,ℓ,ℓ' をそれぞれ $i \in [1,m], j \in [1,r], \ell \in [1,n-k], \ell' \in [1,n]$ なる正整数とする．$\beta = (\beta_1,\cdots,\beta_m)$ を $\mathbb{F}_q$-線型な $\mathbb{F}_{q^m}$ の基底とすると，任意の $x \in \mathbb{F}_{q^m}$ に対して，$x = \sum_{i=1}^{m} x_i\beta_i$ なる $x_i \in \mathbb{F}_q$ が一意に存在する．このとき，$p_i : \mathbb{F}_{q^m} \ni x \mapsto x_i \in \mathbb{F}_q$ とする．n と m の大小により，以降のアルゴリズムの流れが異なるが，本稿では $n = m$ の場合のみ扱う．$n \geq m$ の場合でも，以降の議論を同様に導ける．

r を $[w, m - \lceil km/n \rceil]$ からランダムに選び，$F = (F_1,\cdots,F_r)$ を $B_{m,r}$ からランダムに重複なくとる．$e_{\ell'}$ を $e = (e_1,\cdots,e_n)$ の ℓ' 番目の成分とするとき，$e_{\ell'} = \sum_{j=1}^{r} \lambda_{\ell',j}F_j$ であれば，Rank SDP で与えられている $He = s$ の各 ℓ' 番目の成分について，$H_{\ell,1}e_1 + \cdots + H_{\ell,n}e_n = s_\ell$ であることにより，

$$H_{\ell,1}\sum_{j=1}^{r}\lambda_{1,j}F_j + \cdots + H_{\ell,n}\sum_{j=1}^{r}\lambda_{n,j}F_j = s_\ell$$

が成り立ち，

$$\sum_{j=1}^{r}\lambda_{1,j}(H_{\ell,1}F_j) + \cdots + \sum_{j=1}^{r}\lambda_{n,j}(H_{\ell,n}F_j) = s_\ell$$

Algorithm 1 古典 GRS アルゴリズム

Input: $q,m,n,k,w,H,s,\beta = (\beta_1,\cdots,\beta_m),r,B_{m,r}$
Output: e
1: $e \leftarrow 0^n$
2: **while** $\mathrm{rank}_{\mathbb{F}_q}(e) ! = w$ **do**
3: $\quad F = (F_1,\cdots,F_r) \xleftarrow{\$} B_{m,r}$
4: $\quad (\lambda_{\ell',j})_{1\leq\ell'\leq n, 1\leq j\leq r} \leftarrow \mathsf{solve\_LE}(H,s,\beta,F)$
5: $\quad$ **for** $\ell' := 1$ to n **do**
6: $\quad\quad e_{\ell'} \leftarrow \sum_{j=1}^{r}\lambda_{\ell',j}F_j$
7: **return** e

と各 i に対して，両辺 p_i を適用することで

$$\sum_{j=1}^{r}\lambda_{1,j}p_i(H_{\ell,1}F_j) + \cdots + \sum_{j=1}^{r}\lambda_{n,j}p_i(H_{\ell,n}F_j) = p_i(s_\ell)$$

を得る．上式は $\mathbb{F}_q$ に対して，成り立つことに注意されたい．以上をもとに，$\hat{H} \in \mathbb{F}_q^{m(n-k)\times rn}$ を次のように定める:

$$\hat{H} = \begin{pmatrix} \hat{H}[1][1] & \cdots & \hat{H}[1][n] \\ \vdots & \ddots & \vdots \\ \hat{H}[n-k][1] & \cdots & \hat{H}[n-k][n] \end{pmatrix}$$

ただし，

$$\hat{H}[\ell][\ell'] = \begin{pmatrix} p_1(H_{\ell,\ell'}F_1) & \cdots & p_1(H_{\ell,\ell'}F_r) \\ \vdots & \ddots & \vdots \\ p_m(H_{\ell,\ell'}F_1) & \cdots & p_m(H_{\ell,\ell'}F_r) \end{pmatrix}$$

とする．また，$\hat{s}[\ell] = (p_1(s_\ell),\cdots,p_m(s_\ell)) \in \mathbb{F}_q^m$ として，$\hat{s} = (\hat{s}[1],\cdots,\hat{s}[n-k]) \in \mathbb{F}_q^{m(n-k)}$ と定める．このとき，$\hat{H}\lambda = \hat{s}$ なる $\lambda = (\lambda[1],\cdots,\lambda[n]) \in \mathbb{F}_q^{nr}$ が存在する．ただし，$\lambda[\ell'] = (\lambda_{\ell',1},\cdots,\lambda_{\ell',r}) \in \mathbb{F}_q^r$ である．ここで，$He = s$ は $\hat{H}\lambda = \hat{s}$ と同値である．λ を未知数とするこの連立方程式が解を持つには，$\hat{H}$ のサイズに対して，$nr \leq m(n-k)$ が成り立つことが必要であり，この条件から r の上限が定まる．$\hat{H}$ と $\hat{s}$ に $\mathbb{F}_q$ 上のガウスの消去法を用いて算出した λ から e を求められる．

以上をまとめて，古典 GRS アルゴリズムは **アルゴリズム 1** で与えられる．3 行目の $F = (F_1,\cdots,F_r) \xleftarrow{\$} B_{m,r}$ とは，$B_{m,r}$ から $V_{m,r}$ のランダムな基底を選ぶことを表す．4 行目の $\mathsf{solve\_LE}(H,s,\beta,F)$ とは，(H,s,β,F) を受け取って，$\hat{H}$ と $\hat{s}$ を構成し，$\mathbb{F}_q$ 上の 線型連立方程式 $\hat{H}\lambda = \hat{s}$ の解を求めるサブルーチンである．

ここで，q,α を正整数とするとき，$[\alpha]_q := 1 + q + \cdots + q^{\alpha-1}$ としたとき，$[\alpha]_q ! := \prod_{k=1}^{\alpha}[k]_q$ と定める．また，β を正整数として，$\binom{\alpha}{\beta}_q := \dfrac{[\alpha]_q !}{[\alpha-\beta]_q ![\beta]_q !}$ とおく．$\binom{\alpha}{\beta}_q \approx q^{\beta(\alpha-\beta)}$ なる近似 [1] が知られている．このとき，2-6 行目の **while** 文のループ回数の期待値を ℓ_{CGRS} とすると，$\ell_{\mathrm{CGRS}} = \binom{m}{w}_q / \binom{r}{w}_q$ であり，$\ell_{\mathrm{CGRS}} \approx q^{w(m-r)}$ とできる．更に，未知数の個数

が $(n-k)m$ なる連立方程式に対する Gauss の消去法の計算量は $O((n-k)^3m^3)$ ゆえ，**アルゴリズム 1** の計算量は，$O\left((n-k)^3m^3q^{w(m-r)}\right)$ のようになる．

3. Grover のアルゴリズム

本章では，本稿で用いる量子ゲートと Grover のアルゴリズム [17] について解説する．量子計算の基本的な用語や Grover のアルゴリズムの詳細は，以前の我々の研究グループ [34] の論文を参照されたい．まず，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 ゲートに T ゲートを加えた集合を Clifford+T ゲートという．また，Z ゲートとは，次のような量子ゲートであり，$\mathrm{Z}=\mathrm{SS}$ のように S ゲート 2 つで表せる．

$$\mathrm{Z}=\begin{pmatrix}1&0\\0&-1\end{pmatrix}=\begin{pmatrix}1&0\\0&i\end{pmatrix}\begin{pmatrix}1&0\\0&i\end{pmatrix}$$

Toffoli ゲートとは，次で示される量子ゲートである．

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

Clifford+T ゲートによる Toffoli ゲートの構成は，Shende [33] によって与えられている．

以下では，Grover のアルゴリズムについて概説する．n は正整数で，$V=\{0,1\}^N$ 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) を入力として，$x_0\in M$ 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:

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

$$U_d(|i\rangle):=(2\mathrm{H}^{\otimes N}|0\rangle\langle 0|\mathrm{H}^{\otimes N}-I_N)|i\rangle$$

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: $|\psi\rangle\leftarrow\mathrm{H}^{\otimes n}|\psi\rangle$
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: return $|\psi\rangle$

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 個のテンソル積を表す．U_o はオラクル演算子であり，U_d は diffuser と呼ばれる．一般に，U_o は $C^N(Z)$ ゲート 1 つで構成できる．正整数 x に対して，$C^x(Z)$ ゲートとは，x 個の制御ビットが全て $|1\rangle$ であれば，ターゲットビットに Z ゲートを作用させる量子ゲートである．また，$C^x(Z)$ ゲートの構成は，Toffoli ゲート $2(x-1)$ 個と Z ゲート 1 個で構成できる [28]．$2\mathrm{H}^{\otimes N}|0\rangle\langle 0|\mathrm{H}^{\otimes N}-I_N=X^{\otimes N}C^N(Z)X^{\otimes N}$ が成り立つ．以上より，U_o は $2(N-1)$ 個の Toffoli ゲートと 1 個の Z ゲートから構成でき，U_d は，$2N$ 個の X ゲート，$2(N-1)$ 個の Toffoli ゲートと 1 個の Z ゲートからで構成できる．

このとき，Grover のアルゴリズムは **アルゴリズム 2** で書ける．

4. 提案アルゴリズム

本章では，まず Rank SDP$_s$ に対する古典 GRS アルゴリズムを与える，続いて，Grover のアルゴリズムと組み合わせることで，Rank SDP$_s$ に対する量子 GRS アルゴリズムを提案する．また，以降では，**アルゴリズム 1** の引数である β は $\mathbb{F}_{q^m}$ の標準基底とし，$r=m-\lceil km/n\rceil\geq w$ とする．$r'=r-1,w'=w-1$ とおく．

4.1 古典版提案アルゴリズム

Rank SDP$_s$ を解くためには，解 e に対して，$e_1=1\in\mathbb{F}_{q^m}$ かつ $\langle e_1,e_2,\ldots,e_w\rangle_{\mathbb{F}_q}=\mathrm{span}(e)$ の 2 条件を満たす必要がある．よって，以降では $e_1=1$ として固定する．ここで，$\hat{H}\lambda=\hat{s}$ なる $\lambda=(\lambda[1],\ldots,\lambda[n])\in\mathbb{F}_q^{nr}$ に対して，λ を長さ nr のベクトルではなく，$r\times n$ サイズの行列とみなす．このとき，λ の $r\times r$ ブロック $\lambda_r=(\lambda[1],\ldots,\lambda[r])$ を考える．$\langle e_1,e_2,\ldots,e_w\rangle_{\mathbb{F}_q}=\mathrm{span}(e)$ を満たすためには，λ_r が $\mathbb{F}_q$ 上正則であることが必要である．つまり，λ_r が対角行列となることが必要となる．さらに，$e=\lambda F$ によって求められることから，$F_1=1\in\mathbb{F}_{q^m}$ かつ $\lambda[1]=(1,0,\ldots,0)\in\mathbb{F}_q^n$ であることも必要である．このとき，$\mathbb{F}_{q^m}\setminus\mathrm{span}(1)_{\mathbb{F}_q}\cong\mathbb{F}_{q^{m-1}}$ であることに注意されたい．よって，$\mathbb{F}_{q^m}\setminus\mathrm{span}(1)_{\mathbb{F}_q}$ 上の

Algorithm 3 古典版提案アルゴリズム

Input: $q,m,n,k,w,H,s,B_{m-1,r-1}$
Output: e

$e \leftarrow (1,0,\ldots,0)$
$(\lambda_{\ell',j})_{1\le\ell'\le n,1\le j\le r} \leftarrow 0$
while $(\lambda_{\ell',j})_{1\le\ell'\le n,1\le j\le r}$: 正則でない **do**
  $F=(1,F')$ such that $F' \xleftarrow{\$} B_{m-1,w-1}$
  $(\lambda_{\ell',j})_{1\le\ell'\le n,1\le j\le r} \leftarrow \mathsf{solve\_LE}(H,s,F)$
for $\ell' := 1$ to n **do**
  $e_{\ell'} \leftarrow \sum_{j=1}^{r} \lambda_{\ell',j} F_j$
return e

$(r-1)$ 次元部分空間の基底集合を $B_{m-1,r-1}$ とするとき，F' に対して，$F=(1,F')$ とおくことができる．

Rank SDP$_s$ を解くような，改善版の古典 GRS アルゴリズムは **アルゴリズム 3** で与えられる．**アルゴリズム 1** との比較として，e および F の初期化が変更された点があげられる．**アルゴリズム 1** では，**while** 文のループ条件が e のランクに関する条件であったが，λ_r が正則であれば，この条件を満たすため，**アルゴリズム 3** の **while** 文では，λ_r の条件となっている．また，5 行目の $\mathsf{solve\_LE}(H,s,F)$ とは，β を $\mathbb{F}_q$ 上の $\mathbb{F}_{q^m}$ の標準基底とした際の**アルゴリズム 1** の 4 行目 $\mathsf{solve\_LE}(H,s,\beta,F)$ を表す．なお，λ_r が正則であるかどうかは，λ_r が対角行列かどうかを確認すれば良く，この操作は，提案アルゴリズム全体において，漸近的には影響しない．以上より，**アルゴリズム 3** の漸近計算量は，$O\left((n-k)^3 m^3 q^{w'(m-r')}\right)$ で与えられる．

4.2 量子版提案アルゴリズム

本節では，**アルゴリズム 3** の量子版を与える．その際に，**アルゴリズム 2** をサブルーチンとして用いるため，引数をどのように与えるかについて説明する．**アルゴリズム 2** での V を 2 章で定めた $B_{m,w'}$ とする．このとき，$|B_{m,w'}| = \binom{m}{w'}_q$ が成り立つ [1]．また，**アルゴリズム 2** での M を $M = B_{m-w',r'-w'}$ として，f を次のように取る．$v \in V$ に対して，**アルゴリズム 3** での 4, 5 行目のように，(H,s,β,v) から $\hat{H},\hat{s}$ を構成し，$(\lambda_{\ell',j})_{\ell',j}$ を求める．そこから，3 行目のように，$w\times w$ ブロックが正則であるかを判定し，正則であれば，$v \in M$ として，$f(v)=1$ を返す．そうでないときは，$v \notin M$ として，$f(v)=0$ を返すものとする．このとき，$|M|$ は e で生成される次元が w である部分空間 F_e の個数に等しい．そのような個数は，$|M| = \binom{m-w'}{r'-w'}_q$ となる．このとき，$|V|/|M| = \binom{m}{r'}_q / \binom{m-w'}{r'-w'}_q = \binom{m}{w'}_q / \binom{r'}{w'}_q$ より，$|V|/|M|$ は，**アルゴリズム 3** での **while** 文のループ回数と一致する．

ここで，2 行目の $\mathsf{Grover}(w,H,s,\beta,B_{m,r})$ とは，Grover のアルゴリズムを用いた，次のようなサブルーチンである．つまり，**アルゴリズム 4** のサブルーチンでは，**アルゴリズム 1** での **while** 文内に相当する操作が，$\ell_{\mathrm{QGRS}} = \sqrt{\ell_{\mathrm{CGRS}}}$ 回だけ行われる．以上のように V,M,f を構成し，**アルゴリズム 2** を実行する．よって，**アルゴリズム 4** の計算量は，$O\left((n-k)^3 m^3 \sqrt{q^{w'(m-r')}}\right)$ で与えられる．

Algorithm 4 量子版提案アルゴリズム

Input: $q,m,n,k,w,H,s,B_{m-1,r-1}$
Output: e

$e \leftarrow (1,0,\ldots,0)$
$(\lambda_{\ell',j})_{1\le\ell'\le n,1\le j\le r} \leftarrow \mathsf{Grover}(w,H,s,B_{m-1,r-1})$
for $\ell' := 1$ to n **do**
  $e_{\ell'} \leftarrow \sum_{j=1}^{r} \lambda_{\ell',j} F_j$
return e

bit security	q	m	n	k	w
128	2	53	53	45	4
192	2	61	61	51	5
256	2	67	67	55	6

表 1 RYDE の各 bit security によるインスタンス [2]

以下では，**アルゴリズム 4** を更に改良した改善版量子 GRS アルゴリズムを提案する．$B_{m,r}$ から重複なしでランダムに $|B_{m,r}|/|B_{m-w,r-w}|$ 個選んだ基底の集合を $B'_{m,r}$ とする．この $B'_{m,r}$ を **アルゴリズム 2** での V とする．M,f を **アルゴリズム 4** と同様に構成すると，$|M|=1$ となる．このとき，$|V|/|M| = \binom{m}{r}_q / \binom{m-w}{r-w}_q$ である．改善版のメリットとしては，**アルゴリズム 2** において，V のサイズが小さくなるため，2 行目で用いる H ゲート数が減少することである．さらに，$B_{m,r}$ を直接求めなくても，ランダムに $B_{m,r}$ から基底を選ぶことで構成できる利点もある．

5. 提案アルゴリズムを実行する量子回路の計算コスト

本章では，RYDE に対して，前節の **アルゴリズム 4** を用いた理論的な攻撃手法を提案する．そのために，まずは，本論文で用いる計算コストを導入する．また，以下では，$q=2$ として，β を $\mathbb{F}_{q^m}$ の標準基底とする．つまり，$\beta = (\beta_0,\beta_1,\cdots,\beta_{m-1}) = (1,2,\cdots,2^{m-1})$ とする．

5.1 計算コストの導入

以下では，Clifford+T ゲートのみからなる量子回路 $\mathscr{C}$ を考える．$\mathscr{C}$ に現れる量子ゲートの総数を G-cost という．$\mathscr{C}$ の深さを D-cost といい，$\mathscr{C}$ の量子ビット数を W-cost という．また，入力量子ビットとは別の補助量子ビットのことをアンシラビットと呼ぶ．これらの計算コストは $\log_2$ で評価する．

5.2 RYDE のインスタンスと安全性評価手法

表 1 は，RYDE の各 128/192/256 security bit に対応する rank SDP$_s$ のインスタンスを示している．いずれの場合も $m=n$ であるから，$r=m-k$ で与えられる．

本章では，**アルゴリズム 4** のサブルーチンとして用いられる量子ゲートをまとめ，**アルゴリズム 4** 全体の量子回路に関する計算コストを算出する．NIST[29] は，128, 192, 256 bit security に相当する量子回路は，G-cost と D-cost の和が $170,233,298$ である回路と等価であると主張している．よって，例えば，**表 1** の 128 bit security のインスタンスを用いて算出される G-cost と D-cost の和が 170 を下回っているなら，そのインスタンスを用いた RYDE は，128 bit security を満たさない，と判断できる．また，これらの値は，128/192/256 bit security の AES の鍵探索を行うのに必要な量子回路の計算資源でもある．

5.3 量子回路上での提案アルゴリズムの構成と計算コスト

本節では，**アルゴリズム 4** における計算コストを算出する．**アルゴリズム 4** のサブルーチンである Grover のアルゴリズムの 1 回のループ内で，いくつかの演算が行われるため，本節では，それらの演算の計算コストを算出する．また，以下の各種演算の計算コストをまとめたのが **表 2** である．

5.3.1 線型連立方程式の求解

Bonnetain ら [8] は, 長さが n の量子ビットによるベクトルが m 個与えられた場合の線形連立方程式の求解を行う量子回路を構成した．その量子回路では, $m+n(n+1)/2+n(n-1)$ 個のアンシラビットを必要とし，(mn^2+mn) 個の Toffoli ゲートを用いる．Toffoli ゲートを実行する量子回路の G-cost, D-cost, アンシラビット数は，それぞれ 24, 16, 0 である [33]．Bonnetain らは，(mn^2+mn) 個の Toffoli ゲートを直列で構成するのではなく，深さが $(m+n)\log_2(n)$ となるように構成した．ガウスの消去法を用いる場合と比較して，深さを小さくできることが利点である．本論文の設定では，長さ nr のベクトルが $m(n-k)$ 個並んだ行列による連立方程式を考えているため，Bonnetain らによるその求解アルゴリズムの量子回路の G-cost, D-cost, アンシラビット数は，$24(m(n-k)(nr)^2+m(n-k)nr), 16(m(n-k)+nr)\log_2(nr), m(n-k)+nr(nr+1)/2+nr(nr-1)$ となる．

5.3.2 Grover のアルゴリズム

本節では，[30] に沿って，**アルゴリズム 4** のサブルーチンでの量子状態の重ね合わせ，U_o, U_d での計算コストを算出する．3 章における N に対して，4 章より，$N=\log_2(|V|)=\log_2(|B_{m,w'}|)=\log_2(\binom{m}{w'}_2)$ が成り立つ．まず，重ね合わせでは，入力集合に対する量子状態を考えるため，H ゲートが N 個必要である．よって，重ね合わせを行う量子回路の G-cost は，N であり，D-cost は 1 である．次に U_o は，3 章より，$2(N-1)$ 個の Toffoli ゲートと 1 個の Z ゲートから構成できるため，そのような量子回路の G-cost, D-cost, アンシラビット数はそれぞれ $48N-46, 32N-30, 0$ である．最後に U_d を実行する量子回路の G-cost, D-cost, アンシラビット数はそれぞれ $50N-46, 32N-28, 0$ である．

5.4 parllelizing Grover

表 2 に示されたそれぞれの計算コストは，**アルゴリズム 4** の Grover のアルゴリズム 1 回のループ内の計算コストである．よって，**アルゴリズム 4** 全体の計算コストは，**表 2** の計算コストに，**アルゴリズム 4** の Grover のアルゴリズムによるループ回数を掛けることで求められる．

ここで，D-cost は 96 未満，という制約が存在する [29]．この制約は，量子計算機では，極端に長い逐次処理の実行が難しいことにあり，この値は MAXDEPTH と呼ばれる．このとき，1 つの processor で Grover のアルゴリズムを実行する量子回路の G-cost, D-cost, W-cost が G, D, W の場合，p 個の processor で同様のアルゴリズムを実行したときの G-cost, D-cost, W-cost は $\sqrt{p}G, D/\sqrt{p}, pW$ となる．このように Grover のアルゴリズムを並列化することを parallelizing Grover [18] といい，適切な個数の processor を使うことで，D-cost を 96 未満にすることができる．

5.5 結果

前節までをもとに，RYDE の各 security bit に対する計算コストを **表 3** に示している．結果として，RYDE における全ての security bit に対して，G-cost と D-cost の和が $170,233,298$ をそれぞれ上回った．よって，本論文で提案した攻撃手法によっても，現在の RYDE で用いられているインスタンスによる Rank$_s$ を解読することはできず，そのため，RYDE の安全性は保たれることがわかった．

算出された計算コストが大きかった理由を考察する．**アルゴリズム 4** のループ回数を $L(m,k,w)=\sqrt{q^{w'(m-r')}}$ とおくと，$w'=w-1, r'=r-1=(m-k)-1$ であるから，$L(m,k,w)=2^{(w-1)(k+1)/2}$ となる．$L=L(m,k,w)$ とおくと，例えば, 128 bit security のインスタンスにおいて, $w=4, k=45$ より，$L=2^{69}$ を得る．1 回のループでの G-cost, D-cost をそれぞれ G, D とすると, アルゴリズム全体での G-cost, D-cost は LG, LD とそれぞれ表せる．これらを $\log_2$ で考えた和は $2\log_2(L)+\log_2(G)+\log_2(D)=138+\log_2(G)+\log_2(D)$ となる．本論文の設定においては，ループ 1 回における G-cost と D-cost の和に対して，$\log_2(G)+\log_2(D)\leq 32$ を満たさなかった．これは，行列サイズの 3 乗のオーダーで，Toffoli ゲートが必要な構成を用いたため，上記の不等式を満たさなかったと考えられる．

6. まとめ

本稿では，NIST PQC 標準化プロジェクトの追加署名公募第 2 ラウンドに残っている RYDE に対して，量子計算

演算	G-cost	D-cost	アンシラビット数
線型方程式の求解	$24(m(n-k)(nr)^2+m(n-k)nr)$	$16(m(n-k)+nr)\log_2(nr)$	$m(n-k)+nr(3nr-1)/2$
重ね合わせ	N	1	0
U_o	$48N-46$	$32N-30$	0
U_d	$50N-46$	$32N-28$	0

表 2 提案量子アルゴリズムの計算コスト（$N=\log_2(\binom{m}{w-1}_2)$）

security bit	G-cost	D-cost	W-cost	G-cost + D-cost
128	99	85	95	184
192	160	95	181	255
256	233	95	290	328

表 3 各 security bit に対する提案アルゴリズムの計算コスト

機による安全性評価を行なった．初めに，RYDE が安全性の根拠としている，Rank シンドローム復号問題の変種である RSD_s に対して，GRS アルゴリズムの改善版を提案した．本アルゴリズムは，RSD_s における条件である，$e_1=1$ に注目したものである．続いて，上記の GRS アルゴリズムと Grover のアルゴリズムを組合せることで，RSD_s を解くような，量子 GRS アルゴリズムを提案した．後に，量子 GRS アルゴリズムの回路計算量を算出した．具体的には，量子 GRS アルゴリズムを構成する各種演算の計算コストを算出し，それらに Grover のアルゴリズムによるループ回数を掛け合わせることで，アルゴリズム全体の計算コストを見積もった．結果として，本論文による量子アルゴリズムおよび量子回路の構成によって，RYDE の安全性が失われることはなかった．今後の課題として，Grover のアルゴリズムの 1 回のループ内の演算，特に線型方程式の求解に対して，より計算コストが少ない構成を目指す．

参考文献

[1] N. Aragon, P. Gaborit, A. Hauteville, J. P. Tillich: “A new algorithm for solving the rank syndrome decoding problem”, In The 2018 IEEE International Symposium on Information Theory (ISIT), pp.2421–2425, IEEE, 2018.

[2] N. Aragon, M. Bardet et al.: “RYDE Signature Scheme”, In Round 2 additional signatures to the NIST post-quantum cryptography call, Ver.2.0.1, 2025.

[3] M. Baldi, A. Barenghi et al.: “CROSS: Codes and Restricted Objects Signature Scheme”, In Round 1 additional signatures to the NIST post-quantum cryptography call, Algorithm Specifications and Supporting Documentation, 2023.

[4] M. Baldi, A. Barenghi et al.: “LESS: Linear Equivalence Signature Scheme”, In Round 1 additional signatures to the NIST post-quantum cryptography call, Ver.2.0, 2023.

[5] 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, Springer, 2012.

[6] D. J Bernstein: “Grover vs. McEliece”, In International Workshop on Post-Quantum Cryptography, pp.73–80, Springer, 2010.

[7] L. Bidoux, T. Feneuil, P. Gaborit, R. Neveu, M. Rivain: “Dual support decomposition in the head: Shorter signatures from rank SD and MinRank”, In: International Conference on the Theory and Application of Cryptology and Information Security. Springer, Singapore, pp.38-69, 2025.

[8] X. Bonnetain, S. Jaques: “Quantum period finding against symmetric primitives in practice”, arXiv preprint arXiv:2011.07022, 2020.

[9] C. Chevignard, P.-A. Fouque, A. Schrottenloher: “Reducing the Number of Qubits in Quantum Information Set Decoding”, In: International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer Nature Singapore, pp.299-329, 2024.

[10] N. T. Courtouis, M. Finiasz, N. Sendrier: “How to achieve a McEliece-based digital signature scheme”, In: Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9-13, 2001, Proceedings 7, Springer Berlin Heidelberg, pp.157-174, 2001.

[11] G. D’Alconzo, A. Esser, A. Gangemi, C. Sanna: “Sneaking up the Ranks: Partial Key Exposure Attacks on Rank-Based Schemes”, Cryptology ePrint Archive, 2024/2070, 2024.

[12] 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, Report 2022/964, 2022.

[13] E. M. Gabidulin: “Theory of codes with maximum rank distance”, Problemy peredachi informatsii, vol.21, no.1, pp.3–16, 1985.

[14] P. Gaborit, G. Murat et al.: “Low rank parity check codes and their application to cryptography”, In Proceedings of the Workshop on Coding and Cryptography WCC, vol.2013, 2013.

[15] P. Gaborit, O. Ruatta, J. Schrek: “On the complexity of the rank syndrome decoding problem”, IEEE Transactions on Information Theory, vol.62, no.2, pp.1006–1019, 2015.

[16] P. Gaborit, G. Zémor: “On the hardness of the decoding and the minimum distance problems for rank codes”, IEEE Transactions on Information Theory, vol.62, no.12, pp.7245–7252, 2016.

[17] 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.

[18] S. Jaques, J. M. Schanck: “Quantum cryptanalysis in the RAM model: Claw–finding attacks on SIKE”, In Annual International Cryptology Conference, pp.32–61, Springer, 2019.

[19] D. S. Johnson: “A catalog of complexity classes”, In Algorithms and complexity, pp.67–161, Elsevier, 1990.

[20] G. Kachigar, J. P. Tillich: “Quantum information set decoding algorithms”, In International Workshop on Post-Quantum Cryptography, Lecture Notes in Computer Science,

vol.10346, pp.69–89, Springer, 2017.

[21] P. J. Lee, E. F Brickell: “An observation on the security of McEliece’s public-key cryptosystem”: In Eurocrypt 1988, vol.330 of LNCS, pp.275–280. Springer, 1988.

[22] 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, Springer, 2011.

[23] R. J. McEliece: “A public-key cryptosystem based on algebraic coding theory”, Coding Thv, vol.4244, pp.114–116, 1978.

[24] C. A. Melchor, N. Aragon et al.: “Hauteville: Rank quasi cyclic (RQC)”, In Second round submission to the NIST post-quantum cryptography call, 2019.

[25] C. A. Melchor, N. Aragon et al.: “ROLLO – Rank–Ouroboros, LAKE & LOCKER”, In Second round submission to the NIST post-quantum cryptography call, 2019.

[26] C. A. Melchor, N. Aragon et al.: “HQC”, In Round 4 submissions to the NIST post-quantum cryptography call, 2022.

[27] C. A. Melchor, T. Feneuil et al.: “The Syndrome Decoding in the Head(SD-in-the-Head) Signature Scheme”, In Round 1 additional signatures to the NIST post-quantum cryptography call, Algorithm Specifications and Supporting Documentation Ver.1.0, 2023.

[28] M. A Nielsen, I. Chuang: “Quantum computation and quantum information”, Cambridge University Press, 2002.

[29] NIST: available at `https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)`.

[30] 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), pp.366–377, IEEE, 2021.

[31] S. Perriello, A. Barenghi, G. Pelosi: “Improving the efficiency of quantum circuits for information set decoding”, ACM Transactions on Quantum Computing, vol.4, no.4, pp.1-40, 2023.

[32] E. Prange: “The use of information sets in decoding cyclic codes”, IRE Transactions on Information Theory, vol.8, no.5, pp.5–9, 1962.

[33] V. V. Shende, I. L. Markov: “On the cnot-cost of toffoli gates”, arXiv preprint arXiv:0803.2316, 2008.

[34] 若杉, 多田: “Rank 符号ベース暗号への量子的な攻撃手法の提案とその安全性解析”, 電子情報通信学会 情報セキュリティ研究会 2023 年 暗号と情報セキュリティシンポジウム, 2023.