Vol.2021-DPS-186 No.35
Vol.2021-CSEC-92 No.35
2021/3/15

耐量子暗号$Giophantus^+$暗号における多項式の項省略による線形代数攻撃の改良

中村　友耀[1,a)]　奥村　伸也[1,b)]　宮地 充子[1,2,c)]

概要：大規模な量子計算機が実現できると, 現在利用されている RSA 暗号や楕円曲線暗号等の公開鍵暗号は解読可能となる. このため, 量子計算機を用いても解読が困難となる暗号（耐量子暗号）方式の研究が活発になってきている. 耐量子暗号の候補として, SAC2017 において秋山らは不定方程式暗号 *Giophantus* を発表した. *Giophantus* は環 $\mathbb{F}_q[t]/(t^n-1)$ 上の不定方程式の最小解を求める問題を安全性の根拠とする. LWE 問題の一種である IE Ring-LWE(Indeterminate Equation version of Ring-Learning With Error) 問題が困難であれば, *Giophantus* 暗号は IND-CPA 安全である. SAC2019 において, 代入攻撃と格子攻撃を組み合わせることにより, IE Ring-LWE 問題が容易に解かれてしまうことが室井, 奥村, 宮地らにより示されたが, その攻撃は環を $\mathbb{F}_q[t]/(t^n+1)$ に変換した $Giophantus^+$ には適用できない. 本研究では, 不定方程式の項集合や次数などのパラメータを変えて実験を行うことで, $Giophantus^+$ に対する最適な攻撃手法を検討する.

キーワード：耐量子暗号, IE Ring-LWE 問題, 線形代数攻撃

1. はじめに

1.1 背景

近年, 量子計算機の研究開発が急速に発達してきている. 1997 年, P. Shor [1] によって, 大きな合成数を多項式時間で因数分解するアルゴリズムが発見された. これにより, 大規模な量子計算機が構築されれば, 現在用いられている公開鍵暗号の安全性の根拠である離散対数問題が解かれてしまうことが示された. このため, 量子計算機の攻撃に強い耐量子暗号の研究開発が世界中で進められている. また公開鍵暗号は社会基盤において広く用いられているため, 仮に安全性の高い耐量子暗号が開発されたとしても, 現在の公開鍵暗号との置き換えには相当の時間がかかることが見込まれており, 耐量子暗号の研究開発は大変な急務となっている. 2009 年, 秋山ら [2] は代数曲面暗号を提案した. この暗号は 3 変数 x,y,t の関数 $f(x,y,t)$ で与えられる代数曲面上で $f(u_x(t),u_y(t),t)=0$ となる $(x,y)=(u_x(t),u_y(t))$ を t の関数の中から見つける求セクション問題を安全性の根拠とした. 2010 年, J. Faugeré ら [3] によって代数曲面暗号が解かれた. J. Faugeré らは暗号文から平文を直接求めることによって求セクション問題を回避した. 2017 年, 秋山ら [4] は J. Faugeré らによる攻撃にも耐える不定方程式暗号 $Giophantus^{TM}$ を提案した. *Giophantus* は環 $\mathbb{F}_q[t]/(t^n-1)$ 上の 3 変数 t,x,y についての不定方程式の最小解を求める問題を安全性の根拠としており, これが非線形問題であることから, 公開鍵のサイズを抑えることができる可能性がある. 2019 年, 池松ら [5] は環を $\mathbb{F}_q[t]/(t^n+1)$ に改めた不定方程式暗号 $Giophantus^+$ を SCIS2019 において発表した. 同年, 室井ら [6] は代入攻撃と格子攻撃を組み合わせることにより, *Giophantus* の IND-CPA 安全性を容易に解読する方法を示したが, その攻撃は $Giophantus^+$ には適用できない.

Giophantus 計算問題とは, 公開鍵 $X(t,x,y)$, l, 一様ランダムに選択した $m(t)$, $r(t,x,y)$, $e(t,x,y)$ から暗号文 $Y=m+X\cdot r+l\cdot e$ を計算し, 公開鍵 $X(t,x,y)$ と暗号文 $Y(t,x,y)$ のみを用いて m を計算する問題のことをいう. 室井らによって *Giophantus* が解読された後, 秋山ら [7] は *Giophantus* の安全性の基盤を最小解の求解問題から *Giophantus* 計算問題に変更した $Giophantus^-$ を SCIS2020 において発表した. $Giophantus^-$ は室井らによる攻撃を回避するだけでなく, 公開鍵のサイズを *Giophantus*

[1] 大阪大学
Osaka University
[2] 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology
[a)] nakamura@cy2sec.comm.eng.osaka-u.ac.jp
[b)] okumura@comm.eng.osaka-u.ac.jp
[c)] miyaji@comm.eng.osaka-u.ac.jp

に比べて 3 分の 2 にまで削減した.

Giophantus およびそのバリエーションを解読するための有力な攻撃の 1 つである線形代数攻撃は, 公開鍵 $X(t,x,y)$ および暗号文 $Y(t,x,y)$ から $Y = X \cdot r + e$ となる $r(t,x,y)$ および $e(t,x,y)$ を各項の係数比較によって求めるものである. 係数比較の方法として, Babai のアルゴリズム [8] や Kannan の埋め込み法 [9] に従って $X(t,x,y)$ および $Y(t,x,y)$ の各項の係数を配置した格子を生成し, その格子の格子基底縮小を LLL アルゴリズム [10] に従って実行するというものがあり, 池松ら [11] や草川 [12] によって高速化が図られてきた. 本論文では *Giophantus*$^+$ に対し, $Y(t,x,y)$ の各項の係数を省略する新たな写像 ν_2 を提案する. ν_2 はパラメータ $N_2 \in \mathbb{N}$ に対し, $Y(t,x,y)$ の各項の係数を次数の低い方から N_2 個飛ばしで格子に格納するもので, 格子基底縮小の実行に要する時間を削減できることが見込まれる. IE Ring-LWE 問題を高い確率で解き, 同時に所要時間を抑えることができるような N_2 の値を, 実験によって見極める.

本稿の構成は次のとおりである. 2 章では *Giophantus*$^+$ の暗号化手順と IE Ring-LWE 問題について説明する. 3 章では原始的な線形代数攻撃の定義とアルゴリズムについて説明した後, 既存の高速化手法である池松らの方法および草川の方法について比較しながら説明する. 4 章では本稿の提案手法について説明する. 5 章ではパラメータを変えて実験を行った結果と考察を示す. 6 章では本稿の結論を示す.

1.2 成果

本稿では耐量子暗号 *Giophantus*$^+$ 暗号に対する線形代数攻撃の 1 つである Kannan の埋め込み法を N_2 回に分けて適用する方法を提案する. これにより格子基底縮小を行う際に LLL アルゴリズムに代入する格子のランクをおよそ $1/N_2$ にまで削減することができることを示す. さらに線形代数攻撃の成功率の維持をも可能とする N_2 の選び方について考察する.

2. 準備

2.1 本研究に関する準備

q を素数とし, l および n を自然数とする. これらを用いて次のような剰余環を設定する.

$$R_{q,n} := \mathbb{Z}[t]/(q, t^n + 1) \cong \mathbb{F}_q/(t^n + 1).$$

また $R_{q,n}$ に属する t の多項式の集合を次のように設定する.

$$\mathcal{R}_{q,n} := \left\{ \sum_{k=0}^{n-1} a_k t^k \,\middle|\, -\frac{q}{2} < a_k \leq \frac{q}{2}, a_k \in \mathbb{Z} \right\}.$$

同様に 3 変数 t, x, y についての多項式の集合を次のように設定する.

$$\mathcal{R}_{q,n}[x,y] := \left\{ \sum_{i,j} \left(\sum_{k=0}^{n-1} a_{i,j,k} t^k \right) x^i y^j \;\middle|\; \begin{array}{l} -\frac{q}{2} < a_{i,j,k} \leq \frac{q}{2}, \\ a_{i,j,k} \in \mathbb{N}, \\ \sum_{k=0}^{n-1} a_{i,j,k} t^k \neq 0 \end{array} \right\}.$$

ここで任意の多項式 $f \in \mathcal{R}_{q,n}[x,y]$ を t についての多項式とみなしたときの次数を $deg_t f$ とし, 同様に 2 変数 x, y についての多項式とみなしたときの次数を $deg_{x,y} f$ とする. 同様にして $\mathcal{R}_{l,n}$ および $\mathcal{R}_{l,n}[x,y]$ を定義する.
続いて任意の 2 多項式 u_x, $u_y \in \mathcal{R}_{l,n}$ および任意の既約多項式 $X'(t,x,y) \in \mathcal{R}_{q,n}$ を生成し, $X(t,x,y) := X'(t,x,y) - X'(t,u_x,u_y)$ を計算すると, この $X \in \mathcal{R}_{q,n}[x,y]$ は $X = 0$ の解として $(x,y) = (u_x,u_y)$ をもつ. この組 (u_x,u_y) を「X の l-小解」と呼ぶ. 続いて任意の多項式 $f = \sum f_{i,j} x^i y^j$ について, 次のような集合を設定する.

$$\Gamma_f := \{(i,j) \mid f_{i,j} \in \mathbb{Z}[t] \text{ または } \mathcal{R}_{q,n},\ f_{i,j} \neq 0\}.$$

また 2 つの 0 以上の整数によって得られる全ての組 Γ を用いて, 次のような多項式の集合を設定する.

$$\mathcal{R}_{q,n}[\Gamma] := \{X \in \mathcal{R}_{q,n}[x,y] \mid \Gamma_f \subset \Gamma\}.$$
$$\mathcal{R}_{q,n}[\Gamma, l] := \{X \in \mathcal{R}_{q,n}[\Gamma] \mid X \text{ の } l\text{-小解で割り切れない }\}.$$

加えて任意の 2 自然数 d_1, d_2 を用いて次のような集合を設定する.

$$\Gamma_1 := \{(i,j) \mid 0 \leq i + j \leq d_1\},$$
$$\Gamma_2 := \{(i,j) \mid 0 \leq i + j \leq d_2\},$$
$$\Gamma_3 := \{(i,j) \mid 0 \leq i + j \leq d_1 + d_2\}.$$

2.2 *Giophantus*$^+$

公開鍵および秘密鍵を次のように設定する.

– 公開鍵：q, l, n, $X(t,x,y) \in \mathcal{R}_{q,n}[\Gamma_1]$
– 秘密鍵：u_x, $u_y \in \mathcal{R}_{l,n}$

これらを用いて, 送信する平文 $m(t) \in \mathcal{R}_{l,n}$ を暗号化および復号する手順を説明する.

- 暗号化
  (1) ランダムに $r(t,x,y) \in \mathcal{R}_{q,n}[\Gamma_2]$, $e(t,x,y) \in \mathcal{R}_{l,n}[\Gamma_3]$ を構成する.
  (2) $F_0 := m + X \cdot r + l \cdot e \in \mathbb{Z}[t,x,y]$ を計算する.
  (3) $R_{q,n}$ において $F = F_0 \pmod q$ を満たすような暗号文 $F \in \mathcal{R}_{q,n}[x,y]$ を計算する.
- 復号
  (1) $h(t) := F(t,u_x,u_y)$ を計算する.
  (2) $m_0(t) \equiv h(t) \bmod l$ を満たす $m_0(t)$ を計算する.
  (3) 次の条件を満たすような q を用いている場合 $h(t) \in \mathcal{R}_{q,n}$ となり $m_0(t) = m(t) \in \mathcal{R}_{l,n}$ となるこ

とが知られている. 本稿においてはこの条件を満たす q を常に用いるものとする.

$$\frac{q}{2} > l_h + \sum_{k=0}^{deg_{x,y}X+deg_{x,y}r} (k+1)n^k l_h^{k+1}.$$

$$l_h := \left\lceil \frac{l}{2} \right\rceil \in \mathbb{N}.$$

2.3 IE Ring-LWE 問題

IE Ring-LWE 問題とは, 与えられた $X \in R_{q,n}[x,y]$ および $Y \in R_{q,n}[x,y]$ による組 (X,Y) に対し $Y = X \cdot r + e$ となる $e \in R_{l,n}[\Gamma_3]$ が存在するかしないかを識別する問題のことを指す.

3. 既存研究

3.1 線形代数攻撃

3.1.1 定義

与えられた $X \in R_{q,n}[x,y]$ および $Y \in R_{q,n}[x,y]$ の各項の係数を比較することによって IE Ring-LWE 問題を解くことを線形代数攻撃という. この問題を最近ベクトル問題に帰着させるため, 多項式環を $\mathbb{Z}[t,x,y]$ に改めて考える. ランダムな $X \in R_{q,n}[\Gamma_1, l]$, $r \in \mathcal{R}_{q,n}[\Gamma_2]$ に対し, $X_r \equiv X \cdot r \bmod (t^n+1)$ とする. また $deg_{x,y} f \leq d_1 + d_2$ および $deg_t f \leq n-1$ を満たす $f \in \mathbb{Z}[t,x,y]$ を定義する. これらを用いて,

$$Y_{\mathbb{Z}} := X_r + q \cdot f + e \in \mathbb{Z}[t,x,y] \qquad (1)$$

とすると, $R_{q,n}[x,y]$ において $Y_{\mathbb{Z}} = Y$ となる.

3.1.2 最近ベクトル問題への帰着

次のような格子

$$L := \left\{ \sum_{0 \leq i+j \leq d_1+d_2} \left(\sum_{k=0}^{n-1} a_{i,j,k} t^k \right) x^i y^j \;\middle|\; a_{i,j,k} \in \mathbb{Z} \right\}$$

を定義すると, Y, X_r, e, f は L の要素であり, 階数は $n(d_1+d_2+1)(d_1+d_2+2)/2$ となる. 続いて次のような L の部分格子

$$L_{q,X} := \left\{ X_{r'} + q \cdot f' \in L \;\middle|\; \begin{array}{l} r', f' \in \mathbb{Z}[t,x,y], \\ deg_t r', deg_t f' \leq n-1, \\ deg_{x,y} r' \leq d_2, \\ deg_{x,y} f' \leq d_1 + d_2 \end{array} \right\}$$

を定義すると, (1) 式における $X_r + q \cdot f$ は $L_{q,X}$ の要素であり, また $e \in R_{l,n}[x,y]$ の各項の係数が極めて小さく抑えられているため e は L の短いベクトルとなり, $X_r + q \cdot f$ は Y の最近ベクトルとなる. 次のような手順で攻撃を行う.

(1) 項の順の決定と同形写像の定義

$R_L := \mathrm{Rank} L = n(d_1+d_2+1)(d_1+d_2+2)/2$ とする. 任意の格子 $L' \subset L$ の項の種類 $\{v_1, ..., v_k\}$ を, $i(=1,2,3,...,n)$ を用いて,

$$v_i := t^{i-1},$$
$$v_{n+i} := t^{i-1}y,\ v_{2n+i} := t^{i-1}x,$$
$$v_{3n+i} := t^{i-1}y^2,\ v_{4n+i} := t^{i-1}xy,\ v_{5n+i} := t^{i-1}x^2,$$
$$v_{6n+i} := t^{i-1}y^3, ...$$

のように整列する. このとき $L' = \sum_{j=0}^{k} \mathbb{Z} v_j$ となる. また格子 L' の各項の係数 n_j をランク R_L の行ベクトルの j 番目に格納する写像

$$\Phi : L \ni \sum n_j v_j \mapsto \sum n_j U_j \in \mathbb{Z}^{R_L}$$

を定義する. U_j は第 j 成分が 1 でそれ以外すべての成分が 0 であるランク R_L の行ベクトルを表す.

(2) 格子 $M_{q,X}$ の構成

Kannan の埋め込み法を適用できるような格子 $M_{q,X}$ を構成する. $R_r := \mathrm{Rank}\, r = n(d_2+1)(d_2+2)/2$ とすると, $L_{q,X}$ は $X_{v_j} (1 \leq j \leq R_r)$ および $q \cdot v_k (1 \leq k \leq R_L)$ で生成されるため, $M_{q,X}$ は次のようになる.

$$(\Phi(X_{v_1}), 0), ..., (\Phi(X_{v_{R_r}}), 0),$$
$$(\Phi(q \cdot v_1), 0), ..., (\Phi(q \cdot v_{R_L}), 0), (\Phi(Y), 2).$$

よって $M_{q,X}$ のランクは $R_L + 1$ となる.

(3) Kannan の埋め込み法の適用

$M_{q,X}$ の格子基底縮小からベクトル $(\Phi(e), 2)$ が得られる. 前章において $e(t,x,y) \in \mathcal{R}_{l,n}[\Gamma_3]$ の各項の係数 $a_{i,j,k} \in \mathbb{Z}$ は $-\frac{l}{2} < a_{i,j,k} \leq \frac{l}{2}$ という設定であったので, 得られたベクトル e の各成分が同様の条件を満たしていれば, 線形代数攻撃は成功と判定される.

最後に, 線形代数攻撃のアルゴリズムを Algorithm 1 にまとめる.

3.2 池松らの方法

Kannan の埋め込み法の成功率は, 適用する格子のランクが大きいほど減少する [9] . よってこのランクを小さく抑える研究が行われている. 池松ら [11] は, 前章の d_1, d_2 を用いて, 特定の項を省略する写像を次のように定義した.

$$\mathcal{T} := \{t^i x^j y^k \mid 0 \leq i \leq n-1, 0 \leq j+k \leq d_1+d_2\},$$
$$\Phi_{\mathcal{T}} : \sum_{j=1}^{R_L} n_j v_j \mapsto \sum_{v_j \notin \mathcal{T}} n_j U_j \in \mathbb{Z}^{R_L}.$$

これにより 2 格子 $\Phi_{\mathcal{T}}(L_{q,X})$, $\Phi_{\mathcal{T}}(L)$ のランクは $|\mathcal{T}|$ だけ小さくなる.

Algorithm 1 Linear Algebraic Attack

Input: (X, Y)
Output: $r \in \mathcal{R}_{q,n}[\Gamma_2]$, $e \in \mathcal{R}_{l,n}[\Gamma_3]$ such that $Y := X \cdot r + e$

```
R_L ← n(d_1 + d_2 + 1)(d_1 + d_2 + 2)/2
R_r ← n(d_2 + 1)(d_2 + 2)/2
M_{q,X} ← Matrix((Φ(X_{v_1}), 0), ..., (Φ(X_{v_{R_r}}), 0))
M_{q,X} ← Matrix((Φ(q · v_1), 0), ..., (Φ(q · v_{R_L}), 0))
M_{q,X} ← Matrix((Φ(Y), 2))
v ← vector (Φ(e), 2) in the LLL reduced lattice by Kannan's embedding technique
if all coefficients of e are between −l/2 to l/2 then
    Compute r ∈ R_{q,n}[Γ_2] such that (Y − e) mod q = (X_r + q · f) mod q = X_r = X · r mod (t^n + 1)
end if
return r, e
```

3.3 草川の方法

草川 [12] は次のような写像を定義した.

$$\Psi_0 : R_{q,n}[x, y] \ni F(t, x, y) \mapsto F(t, x, 0) \in R_{q,n}[x].$$

これにより 2 格子 $\Psi_0(L_{q,X})$, $\Psi_0(L)$ のランクはおよそ半分になる.

4. 提案

Y のランク R_L, 任意の自然数 N_2 について, R_L を N_2 で割った商を α, 余りを β として, 次のような写像 ν_2 を提案する.

$$\nu_2 : \sum_{j=1}^{R_L} n_j v_j \mapsto \sum_{j=1}^{\alpha+1} n_{jN_2} U_{jN_2} \in \mathbb{Z}^{\alpha+1}.$$

これは組 (X, Y) の項の次数が低い方から順に係数を $N_2 - 1$ 個ずつ飛ばしながら取り出し, Kannan の埋め込み法により $Y = X \cdot r + e$ を満たす e の項の次数が低い方から順に係数を $N_2 - 1$ 個飛ばしで調べるもので, e のすべての項を調べるには Kannan の埋め込み法を N_2 回実行する必要がある. また Kannan の埋め込み法に適用する格子のランクは, $\beta \neq 0$ の場合 β 回目までは $\alpha + 2$ となり, それ以降は $\alpha + 1$ となる. $\beta = 0$ の場合すべて $\alpha + 1$ となる. よってあらゆる N_2 に関して, 格子のランクはおよそ $1/N_2$ になる. 識別が成功するような N_2 の選び方を実験によって見極める.

5. 評価

5.1 実験環境

- CPU
  Intel(R) Xeon(R) CPU E7-4830 v4 @ 2.00Hz
- MEMORY
  3.0T
- OS
  Ubuntu 16.04.7 LTS
- プログラミング言語
  Magma version 2.25-8

5.2 実験結果

攻撃の種類別の結果を以下に示す. 表の左半分には $Y = X \cdot r + e$ となる $e \in R_{l,n}[\Gamma_3]$ が存在するため, 算出に成功した割合を記載した. 逆に右半分には $Y = X \cdot r + e$ となる $e \in R_{l,n}[\Gamma_3]$ が存在しないため, 算出に失敗した割合を記載した. つまり成功率・失敗率ともに 100% となることが望ましい.

表 1 (X, Y) に対する原始的線形代数攻撃

n	Rank	$e \in R_{l,n}[\Gamma_3]$ が存在する		$e \in R_{l,n}[\Gamma_3]$ が存在しない	
		成功率	所要時間 (s)	失敗率	所要時間 (s)
10	61	10/10	6.4	10/10	5.6
20	121	10/10	3.5×10^2	10/10	3.4×10^2
30	181	10/10	2.0×10^3	10/10	2.2×10^3
40	241	10/10	6.0×10^3	10/10	5.8×10^3
50	301	4/10	2.6×10^4	10/10	2.3×10^4
60	361	1/10	1.2×10^5	10/10	1.1×10^5
70	421	0/5	2.3×10^5	5/5	1.9×10^5

表 2 (X, Y) に対する改良版 ($N_2 = 2$) 線形代数攻撃

n	Rank	$e \in R_{l,n}[\Gamma_3]$ が存在する		$e \in R_{l,n}[\Gamma_3]$ が存在しない	
		成功率	所要時間 (s)	失敗率	所要時間 (s)
10	31	10/10	3.7	10/10	4.0
20	61	10/10	1.0×10^2	10/10	1.0×10^2
30	91	10/10	7.7×10^2	10/10	7.5×10^2
40	121	10/10	3.4×10^3	10/10	3.0×10^3
50	151	10/10	9.5×10^3	10/10	9.4×10^3
60	181	7/10	6.1×10^4	10/10	5.6×10^4
70	211	8/10	7.0×10^4	10/10	6.7×10^4
80	241	10/10	9.6×10^4	10/10	9.8×10^4
90	271	7/10	1.5×10^5	10/10	1.4×10^5
100	301	5/10	2.7×10^5	10/10	2.5×10^5

表 3 (X, Y) に対する改良版 ($N_2 = 3$) 線形代数攻撃

n	Rank	$e \in R_{l,n}[\Gamma_3]$ が存在する		$e \in R_{l,n}[\Gamma_3]$ が存在しない	
		成功率	所要時間 (s)	失敗率	所要時間 (s)
10	21	10/10	1.5	0/10	1.6
20	41	10/10	2.2×10	0/10	2.3×10
30	61	10/10	2.5×10^2	0/10	2.4×10^2
40	81	10/10	5.7×10^2	0/10	5.9×10^2
50	101	10/10	1.8×10^3	0/10	1.7×10^3
60	121	10/10	9.0×10^3	0/10	8.0×10^3
70	141	10/10	1.1×10^4	0/10	9.2×10^3
80	161	10/10	2.9×10^4	0/10	2.1×10^4
90	181	8/10	1.0×10^5	2/10	1.1×10^5
100	201	8/10	1.3×10^5	8/10	1.6×10^5

まず原始的線形代数攻撃と改良版 ($N_2 = 2$) 線形代数攻

撃を比較すると, $n = 10$ のとき目立った違いは見られなかったが, $n = 40$ の時点では所要時間に 2 倍近くの差をつけて改良版 ($N_2 = 2$) 線形代数攻撃が短時間で処理を完了した. 原始的線形代数攻撃は徐々に成功率を下げていき, $n = 70$ のとき成功率が 0% となることが予想されたため試行回数を 5 とし, ここで処理を終了した. Kannan の埋め込み法の成功率は一般に格子のランクが大きいほど減少し, 格子のランクは n に比例するため, n が 80 以上のときの原始的線形代数攻撃の成功率は 0% で不変となると考えられたためである. 改良版 ($N_2 = 2$) 線形代数攻撃はその後も 50% 以上の成功率を維持した. また失敗率は実験で用いたすべての n で双方とも 100% となった. このことから原始的線形代数攻撃に比べて改良版 ($N_2 = 2$) 線形代数攻撃がより優れていると言える. 次に改良版 ($N_2 = 3$) 線形代数攻撃は $n = 80$ までは成功率 100% かつ失敗率 0% となった. これはいかなる Y についても $Y = X \cdot r + e$ となるような $e \in R_{l,n}[\Gamma_3]$ が存在すると認識されていたことになり, IE Ring-LWE 問題を解くことはできなかった. しかし $n = 90$ からは変化が見られ, $n = 100$ においては成功率・失敗率ともに 80% となった.

5.3 考察

原始的線形代数攻撃と改良版 ($N_2 = 2$) 線形代数攻撃を比較して改良版 ($N_2 = 2$) 線形代数攻撃がより優れている理由として, Kannan の埋め込み法を適用する格子のランクが抑えられていたため適用 1 回あたりの所要時間を抑えつつ, 成功率を保つことができたためと考えられる. 原始的線形代数攻撃では Kannan の埋め込み法を 1 回ですべての処理を行ったのに対し, 改良版 ($N_2 = 2$) 線形代数攻撃ではランクをおよそ半分にして Kannan の埋め込み法を 2 回にわたって適用した. しかし無闇に大きい N_2 を採用すれば良いわけでもなく, 改良版 ($N_2 = 3$) 線形代数攻撃では $n = 80$ までは IE Ring-LWE 問題を解くことはできなかった. ただし改良版 ($N_2 = 2$) 線形代数攻撃も n が大きくなれば適用できなくなると考えられ, 実際 $n = 80$ 付近から成功率が下がった. より大きな n および N_2 について実験すれば, n の値に対応した最適な N_2 を計算できる可能性が考えられる.

6. 結論

本稿では耐量子暗号 *Giophantus*$^+$ 暗号に対する線形代数攻撃の高速化を目的として, Kannan の埋め込み法を N_2 回に分けて適用する方法を提案した. これにより格子基底縮小を行う際に LLL アルゴリズムに代入する格子のランクをおよそ $1/N_2$ にまで削減することができることを示した. さらに線形代数攻撃の成功率の維持をも可能とする N_2 の選び方について考察した.

謝辞 本研究は JSPS 科研費 JP1910400 の助成を受けたものです. また本研究の一部は文部科学省「Society5.0 に対応した高度技術人材育成事業成長分野を支える情報技術人材の育成拠点の形成 (enPiT)」さらに文部科学省の平成 30 年度「Society 5.0 実現化研究拠点支援事業」の助成を受けています.

参考文献

[1] Shor, P. W.: Algorithms for Quantum Computation: Discrete Logarithms and Factoring, *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, IEEE Computer Society, pp. 124–134 (online), DOI: 10.1109/SFCS.1994.365700 (1994).

[2] Akiyama, K., Goto, Y. and Miyake, H.: An Algebraic Surface Cryptosystem, *Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings* (Jarecki, S. and Tsudik, G., eds.), Lecture Notes in Computer Science, Vol. 5443, Springer, pp. 425–442 (online), DOI: 10.1007/978-3-642-00468-1_24 (2009).

[3] Faugère, J. and Spaenlehauer, P.: Algebraic Cryptanalysis of the PKC'2009 Algebraic Surface Cryptosystem, *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings* (Nguyen, P. Q. and Pointcheval, D., eds.), Lecture Notes in Computer Science, Vol. 6056, Springer, pp. 35–52 (online), DOI: 10.1007/978-3-642-13013-7_3 (2010).

[4] Akiyama, K., Goto, Y., Okumura, S., Takagi, T., Nuida, K. and Hanaoka, G.: A Public-Key Encryption Scheme Based on Non-linear Indeterminate Equations, *Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers* (Adams, C. and Camenisch, J., eds.), Lecture Notes in Computer Science, Vol. 10719, Springer, pp. 215–234 (online), DOI: 10.1007/978-3-319-72565-9_11 (2017).

[5] Ikematsu, Y., Wang, Y., Akiyama, K. and Takagi, T.: Experimental Analysis for Linear Algebraic Attack on a Variant of Indeterminate Equation Public-Key Cryptosystems (2019).

[6] Muroi, A., Okumura, S. and Miyaji, A.: An Improved Security Analysis on an Indeterminate Equation Public Key Cryptosystem by Evaluation Attacks, *Selected Areas in Cryptography - SAC 2019 - 26th International Conference, Waterloo, ON, Canada, August 12-16, 2019, Revised Selected Papers* (Paterson, K. G. and Stebila, D., eds.), Lecture Notes in Computer Science, Vol. 11959, Springer, pp. 421–436 (online), DOI: 10.1007/978-3-030-38471-5_17 (2019).

[7] Ikematsu, Y., Wang, Y., Akiyama, K. and Takagi, T.: A Study on a variant of indeterminate equation public-key cryptosystems assuming one-wayness at SCIS 2020 (2020).

[8] Babai, L.: On Lovász' lattice reduction and the nearest lattice point problem, *Comb.*, Vol. 6, No. 1, pp. 1–13 (online), DOI: 10.1007/BF02579403 (1986).

[9] Kannan, R.: Minkowski's Convex Body Theorem and Integer Programming, *Math. Oper. Res.*, Vol. 12,

No. 3, pp. 415–440 (online), DOI: 10.1287/moor.12.3.415 (1987).

[10] Lenstra, A. K., Lenstra, H. W. and Jr.Lovász, L.: Factoring polynomials with rational coefficients, Math. Ann. 261(4), Springer, pp. 515–534 (1982).

[11] Ikematsu, Y., Akiyama, K. and Takagi, T.: An Improvement on the Linear Algebraic Attack for the Indeterminate Equation Encryption Scheme, *International Symposium on Information Theory and Its Applications, ISITA 2018, Singapore, October 28-31, 2018*, IEEE, pp. 389–393 (online), DOI: 10.23919/ISITA.2018.8664254 (2018).

[12] Xagawa, K.: Practical Cryptanalysis of a Public-Key Encryption Scheme Based on Non-linear Indeterminate Equations at SAC 2017, *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings* (Lange, T. and Steinwandt, R., eds.), Lecture Notes in Computer Science, Vol. 10786, Springer, pp. 142–161 (online), DOI: 10.1007/978-3-319-79063-3_7 (2018).