Vol.2019-DPS-178 No.24
Vol.2019-CSEC-84 No.24
2019/3/5

IE-LWEを用いた不定方程式暗号に対する$t = 1$の代入攻撃

室井　謙典[1,a)]　奥村　信也[2,b)]　宮地　充子[2,c)]

概要：SAC2017 で秋山氏らが提案した耐量子暗号 (Giophantus) は，不定方程式の最小解を求める問題の計算困難性に基づいている．また, IE-LWE 問題という, LWE 問題と多変数多項式を組み合わせた新しい問題の計算困難性を仮定すれば, Giophantus は IND-CPA 安全である．提案後, 格子攻撃や t=1 の代入識別攻撃が提案されてきたが, 現在ではそれらの攻撃に耐性のあるパラメータが提案されており, 暗号文サイズは大きいものの, 秘密鍵サイズは小さく処理速度も高速である．本稿では, IE-LWE 問題に対する新しい t=1 の代入識別攻撃を提案する．提案手法では, IE-LWE 問題に現れる多項式のある変数に 1 を代入後, 多項式の係数比較により得られる連立方程式から, 整数上の非常に階数の低い格子を構成し，その格子に関する最近ベクトル問題を解くことで, 分布の識別を行うものである．計算機実験により, 既存の代入攻撃が回避できると考えられるパラメータに対しても, 効率よく分布の識別を行うことができる, という実験結果が得られた．

A Distinguish Attack Evaluating at $t = 1$ for Indeterminate Equation Scheme based on IE-LWE

1. はじめに

様々な情報が通信によって交換される中，情報を暗号化し，安全に復号することは重要なことである．今までに様々な暗号方式が提案されてきたが，P. Shor によって, 量子コンピュータの完成に伴い, 整数の因数分解問題や離散対数問題ベースの公開鍵暗号基盤が崩壊してしまうことが示されている [13]. 量子コンピュータ完成後も安全である暗号は耐量子暗号と呼ばれる．量子コンピュータの開発が進む中, 耐量子暗号の標準化の動きからもわかるように, 耐量子暗号は非常に重要な暗号方式の一種であると言える．そのため, 近年, 耐量子暗号の候補の提案や, 既存の耐量子暗号の候補に対する安全性解析の研究が活発に行われている.

これまでに, 耐量子暗号の候補として, 格子ベース暗号 [4], 符号ベース暗号 [11], 多変数多項式暗号 [10] などが提案されてきたが, 攻撃手法の改良が進み, パラメータを大きくすることで, 鍵サイズや暗号文サイズの増大や, 暗号化・復号処理の効率が悪くなるなどの問題がある．そのため, 新しい計算困難な問題の発見や, そのような問題に基づく耐量子暗号の構成が大きな課題となっている.

その課題の解決のために, 国際会議 SAC 2017 で秋山氏ら [2] は IE-LWE 問題という, LWE 問題 [12] と多項式を組み合わせた, 量子コンピュータでも計算困難であると思われる新しい問題を導入した．さらに, 秋山氏らは IE-LWE 問題の困難性を仮定すれば IND-CPA 安全な（選択平文攻撃下で識別不可能性を満たす）不定方程式を利用した公開鍵暗号 (Giophantus) を構成した．Giophantus では, p を素数としたとき, $\mathbb{F}_p[t]/(t^n - 1)$ を係数を環とする 2 変数多項式を利用している． IE-LWE 問題はある種の分布識別問題であり, LWE 問題 [12] の多項式類似と考えることができる．提案当初は, 鍵サイズの小ささや処理速度の高速性, さらには多ビットの平文を暗号化し準同型処理ができる準同型暗号とされていた.

しかし, 秋山氏らの提案後, 暗号の構成で利用される多項式の変数にある値を代入する IND-CPA 安全性に対する攻撃や平文復元が可能であることが指摘されている [2], [3]. 現在では, それらの攻撃に耐性のあると考えられるパラメータが提案されている [2], [3]．その新しいパラメータでは,

[1] 大阪大学工学部
Osaka University
[2] 大阪大学大学院　工学研究科
Osaka Uniersity
[a)] muroi@cy2sec.comm.eng.osaka-u.ac.jp
[b)] okumura@comm.eng.osaka-u.ac.jp
[c)] miyaji@comm.eng.osaka-u.ac.jp

公開鍵サイズや暗号文サイズが大きくなってしまうが、秘密鍵のサイズの小ささ，処理速度の高速性と多ビットの準同型性は, いまだに Giophantus の大きな利点であり, さらなる安全性解析が望まれる.

本研究では, 新しい選択平文攻撃可能な条件下での識別不可能性に対する攻撃, つまり, IE-LWE 問題の新しい解法を提案する．秋山氏らによる安全性解析では, 線形代数攻撃や鍵復号攻撃，全数探索攻撃などが紹介されており, さらに，線形代数攻撃や鍵復元攻撃は改良されたものが提案されている [8][9]．しかし, 攻撃に利用する格子の階数が大きいため, IE-LWE 問題の困難性を脅かすもになっていない.

それに対し, 提案手法では, IE-LWE 問題に現れる多項式に $t=1$ を代入後, 多項式の係数比較により得られる連立方程式から, 整数上の格子を構成し，その格子に関する最近ベクトル問題（CVP）を解くことで, 分布の識別を行うものである．提案手法と既存の代入攻撃との違いは, ある範囲の全数探索を行っておらず, 攻撃に現れる格子の階数は, Giophantus の推奨パラメータに対して 6 でしかなく, 真に CVP を解くアルゴリズムを適用しても効率よく攻撃を行うことができる点である．さらに, 計算機実験により, 既存の代入攻撃が回避できると考えられるパラメータに対しても, 効率よく分布の識別を行うことができる, という実験結果が得られた.

本稿の構成は以下のとおりである．2 節で本稿の用語を定義し，3 節で攻撃対象の暗号を考えるうえで必要な問題を紹介する．4 節で IE-LWE を用いた暗号方式とそれに対する既存攻撃を示し，5 節で新たな攻撃を提案する．6 節で新たな攻撃の実験結果を示し，7 節でまとめを述べる．

2. 準備

本稿で使用する用語を定義する．p を素数，$\mathbb{Z}$ を整数環とする．$R_p=\mathbb{Z}_p[t]/(t^n-1)$ と定義し R_q を係数が $\{0,\cdots l-1\}$ の範囲であり次数が $n-1$ までである，集合 R_p の部分集合と定義する．さらに 2 変数多項式を

$$A(x,y)=\sum_{(i,j)\in\Gamma_A} a_{i.j}x^iy^j$$

と定義する．ここで Γ_A を多項式の中のゼロでない単項式 x^iy^j の指数の組と定義する．この Γ_A を, 多項式 A の形式と本稿では呼ぶ.

2.1 代数曲面暗号

ここでは本研究で攻撃対象となっている暗号の下になっている代数曲面暗号について述べる.

Definition 1 (求セクション問題 [2])**.** $X(x,y,t)=0$ が体 K 上の代数曲面とすると, 体 K 上のパラメータ表示された曲線, $(x,y,t)=(u_x(t),u_y(t),t)$ を見つける問題のことを, X 上の求セクション問題という.

セクションは環 $K[t]$ 上の不定方程式 $X(x,y)=0$ の解として考えることができ, 本稿では p を素数として $\mathbb{F}_p$ 上の不定方程式 $X(x,y,t)=0$ の代わりに, $\mathbb{F}_p[t]$ 上の不定方程式 $X(x,y)=0$ と書く．m,r,c,X を $\mathbb{F}_p[t]$ 上の 2 変数多項式で，それぞれを平文，乱数，暗号文，$(u_x(t),u_y(t))$ を解にもつ不定方程式とすると最もシンプルな代数曲面暗号は以下のように平文を暗号化する.

$$c(x,y)=m(x,y)+X(x,y)r(x,y).$$

2.2 IE-LWE 問題

本章では IE-LWE 問題について述べる.

- $\mathfrak{F}_{\Gamma_r}/R_p$ ： 形式が Γ_r の R_p 上の 2 変数多項式の集合
- $\mathfrak{F}_{\Gamma_{X_r}}/R_l$ ： 形式が Γ_{Xr} の R_l 上の 2 変数多項式の集合

と定義する.

$\mathbb{F}_p$ 上の多項式で, 係数の範囲が 0 から $l-1$ のものをサイズ l の多項式という．サイズ l のゼロ点を含んだ多項式の集合を以下のように定義する.

$$\mathfrak{X}(\Gamma_X,l)/R_p=$$
$$\{X\in\mathfrak{F}_{\Gamma_X}/R_p|\ \exists u_x(t),u_y(t)\in R_l,\ X(u_x(t),u_y(t))=0\}.$$

形式が以下の条件

$$(0,0)\in\Gamma_X,(0,0)\in\Gamma_r$$

を満たす多項式集合 $\mathfrak{X}(\Gamma_X,l)/R_p$, $\mathfrak{F}_{\Gamma_r}/R_p$, $\mathfrak{F}_{\Gamma_{X_r}}/R_l$ が与えられたとき, 以下のように IE-LWE の分布識別問題を定義する.

Definition 2 (IE-LWE 問題)**.** U_X,T_X をそれぞれ以下のように書く.

$$U_X=\mathfrak{X}(\Gamma_X,l)/R_p\times\mathfrak{F}_{\Gamma_{X_r}}/R_p,$$
$$T_X=\{(X,Xr+e)|X\in\mathfrak{X}(\Gamma_X,l)/R_p,r\in\mathfrak{F}_{\Gamma_r}/R_p,$$
$$e\in\mathfrak{F}_{\Gamma_{X_r}}/R_l\}.$$

この時, *IE-LWE* 問題 とは与えられた多項式の組が, *'noisy'* な多項式の集合 T_X と, 集合 U_X-T_X のどちらから選択されたかを区別する問題である．T_X は U_X の部分集合である.

2.3 最小解問題

多項式 $u=(u_x(t),u_y(t))$ $(\in(\mathbb{Z}_p[t]/(t^n-1))^2)$ を以下のように書く.

$$u_x(t)=\sum_{i=0}^{n-1}\alpha_it^i,\ u_y(t)=\sum_{i=0}^{n-1}\beta_it^i.$$

この時,u のノルムを以下のように定義する.

$$Norm(u)=max\{\alpha_i,\beta_i\in\mathbb{Z}_l^+\mid 0\le i\le n-1\}.$$

最小解問題を以下のように定義する.

Definition 3 (最小解問題). $X(x,y) = 0$ を剰余環 $\mathbb{Z}_p[t]/(t^n-1)$ 上の不定方程式とすると, 最小のノルムを持つ解 $(x,y) = (u_x(t), u_y(t))$ を見つける問題を X 上の最小解問題という.

この問題は $\deg X \geq 2$ の時, 非線形なので近似格子縮約をそのまま適用し解くことはできない.

3. 秋山氏らの提案暗号とそれに対する既存攻撃

この節では前節で述べた代数曲面暗号の最もシンプルなものを改良した秋山氏らの提案方式とその方式に対する既存攻撃を紹介する.

3.1 IE-LWE を利用した代数曲面暗号

ここでは 2017 年に秋山氏らが提案した IE-LWE を利用した不定方程式暗号について述べる. l を $l \ll p$ を満たす整数とし, $\mathbb{Z}_p^+ = \{0 \cdots p-1\}, \mathbb{Z}_l^+ = \{0 \cdots l-1\}$ と定義する. さらに X と r の総次数をそれぞれ w_x, w_r と表すと, p と l に関する以下の関係式を満たす必要がある.

$$p > \#\Gamma_{X_r} \cdot l(l-1) \cdot (n(l-1))^{w_X + w_r}, \tag{1}$$

- 鍵生成
  秘密鍵を以下のように表す. つまり, R_l からランダムに係数を選びそれらを解に持つ不定方程式 $X(x,y) = 0$ を生成する.

  $$u : (x,y) = (u_x(t), u_y(t)), u_x(t), u_y(t) \in R_l,$$

  $\deg u_x(t) = \deg u_y(t) = n-1$ で $l \ll p$ であることから u を小さな解という. 公開鍵は小さな u を解に持つ不定方程式 $X(x,y) = 0$ である. $X(x,y)$ は以下のように表す.

  $$X(x,y) = \sum_{(i,j)\in\Gamma_X} a_{ij} x^i y^j, a_{ij} \in R_p.$$

- 暗号化

  (1) 平文 M を多項式 $m(t) \in R_l$ の係数に組み込む.
  (2) ランダムな多項式 $r(x,y) \in \mathfrak{F}_{\Gamma_r}/R_p$ を選ぶ.
  (3) noise の多項式 $e(x,y) \in \mathfrak{F}_{X_r}/R_l$ を選ぶ.
  (4) 暗号多項式 $c(x,y)$ を以下のように構成する.

  $$c(x,y) = m(t) + X(x,y)r(x,y) + l \cdot e(x,y).$$

- 復号

  (1) 小さな解 u を代入する

  $$c(u) = m(t) + l \cdot e(u).$$

  p と l が (1) の条件を満たせば $m(t) + l \cdot e(u) \in \mathbb{Z}[t]/(t^n-1)$ の係数は $\mathbb{Z}_p^+$ の範囲の値である.
  (2) $c(u)(mod\ l) = m(t)$ として $m(t)$ を $c(u)$ から取り出す. $c(u)$ は $\mathbb{Z}[t]$ の要素と考えることが出来る.
  (3) 平文 M を $m(t)$ の係数から取り出す.

以上が秋山氏らが提案した不定方程式を利用した公開鍵暗号方式である. 秋山氏らはさらに暗号方式に対する攻撃も述べている. それらについて以下で述べる.

3.2 線形代数攻撃

多項式の組 (X,Y) が与えられたとき, 仮に $Y = Xr + e$ を満たす $r \in \mathfrak{F}_{\Gamma_r}/R_p$ と $e \in \mathfrak{F}_{\Gamma_{X_r}}/R_l$ が見つかれば, (X,Y) は集合 T_X からサンプリングされたと識別できる. 多項式 r と e を見つけるために以下の方法を考える. 線形方程式を作るために $x^i y^j$ の係数を比較する. つまり以下の関係

$$\sum_{(i,j)\in\Gamma_{X_r}} d_{ij}x^i y^j = \left(\sum_{(i,j)\in\Gamma_X} a_{ij}x^i y^j\right)\left(\sum_{(i,j)\in\Gamma_r} r_{ij}x^i y^j\right) + \left(\sum_{(i,j)\in\Gamma_{Xr}} e_{ij}x^i y^j\right)$$

を用いる. r_{ij} と e_{ij} はそれぞれ R_p-*valued* と R_l-*valued* の変数である. $\deg X = \deg r = 1$ の時を考える. 多項式 X, r, e, Y を以下のように書く.

$$\begin{aligned} X(x,y) &= a_{10}x + a_{01}y + a_{00}, \\ r(x,y) &= r_{10}x + r_{01}y + r_{00}, \\ e(x,y) &= e_{20}x^2 + e_{11}xy + e_{02} + e_{10}x + e_{01}y + e_{00}, \\ Y(x,y) &= d_{20}x^2 + d_{11}xy + d_{02} + d_{10}x + d_{01}y + d_{00}. \end{aligned}$$

上の方程式より

$$\begin{aligned} X(x,y)r(x,y) = a_{10}r_{10}x^2 + (a_{10}r_{01} + a_{01}r_{10})xy + a_{01}r_{01}y^2 + \\ (a_{10}r_{00} + a_{00}r_{10})x + (a_{01}r_{00} + a_{00}r_{01})y + a_{00}r_{00} \end{aligned}$$

となるので, 線形方程式を以下のように得る.

$$a_{10}r_{10} + e_{20} = d_{20}, \tag{2}$$
$$a_{10}r_{01} + a_{01}r_{10} + e_{11} = d_{11}, \tag{3}$$
$$a_{01}r_{01} + e_{02} = d_{02}, \tag{4}$$
$$a_{10}r_{00} + a_{00} + e_{10} = d_{10}, \tag{5}$$
$$a_{01}r_{00} + a_{00}r_{01} + e_{01} = d_{01}, \tag{6}$$
$$a_{00}r_{00} + e_{00} = d_{00}. \tag{7}$$

R_l-*valued* の e_{ij} のような解が見つかったとき, (X,Y) は T_X の要素となる. 多項式 e に対する全数探索攻撃を避けるために $\#\Gamma_{Xr}$ は以下の条件を満たす必要がある.

$$((l-1)l^{n-1})\#\Gamma_{Xr} > 2^k,$$

k はセキュリティパラメータである．次に小さな e_{ij} を見つけるために格子縮約攻撃を使用する．a_{10} を次のように表す．

$$a_{10} = a_{n-1}^{(10)} t^{n-1} + \cdots .$$

$r_{10}, d_{20} \in R_p$, $e_{20} \in R_l$ も a_{10} と同じように表したとき $a_{10}r_{10} + e_{20} = d_{20}$ は以下のように表すことができる．

$$\begin{pmatrix} a_{n-1}^{(10)} & a_{n-2}^{(10)} & \cdots & a_1^{(10)} & a_0^{(10)} \\ a_{n-2}^{(10)} & a_{n-3}^{(10)} & \cdots & a_0^{(10)} & a_{n-1}^{(10)} \\ a_{n-3}^{(10)} & a_{n-4}^{(10)} & \cdots & a_{n-1}^{(10)} & a_{n-2}^{(10)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_0^{(10)} & a_{n-1}^{(10)} & \cdots & a_2^{(10)} & a_1^{(10)} \end{pmatrix} \begin{pmatrix} r_0^{(10)} \\ r_1^{(10)} \\ \vdots \\ r_{n-2}^{(10)} \\ r_{n-1}^{(10)} \end{pmatrix} + \begin{pmatrix} e_{n-1}^{(10)} \\ e_{n-2}^{(10)} \\ \vdots \\ e_1^{(10)} \\ e_0^{(10)} \end{pmatrix} = \begin{pmatrix} d_{n-1}^{(10)} \\ d_{n-2}^{(10)} \\ \vdots \\ d_1^{(10)} \\ d_0^{(10)} \end{pmatrix}.$$

よって方程式の一つ目 (2) は以下のように書くことができる．

$$A_{10}\boldsymbol{r_{10}} + \boldsymbol{e_{20}} = \boldsymbol{d_{20}}.$$

上の等式の左辺に整数上の格子を作るために，整数のベクトル $\boldsymbol{g_{20}}$ を加えて以下の方程式を得る．

$$A_{10}\boldsymbol{r_{10}} + \boldsymbol{e_{20}} + p\boldsymbol{g_{20}} = \boldsymbol{d_{20}}.$$

今，整数格子 $\mathcal{L} = (A_{10}\ pI_n)$ を考える．$\boldsymbol{v}$ を $\boldsymbol{d_{20}}$ に最も近い $\mathcal{L}$ のベクトルとすると，$\boldsymbol{v}$ を見つけることができたとき,$\boldsymbol{v} - \boldsymbol{d_{20}}$ を計算することで $\pm\boldsymbol{e_{20}}$ を求められると期待できる．つまり IE-LWE 問題は格子上の CVP に帰着できるということである．この攻撃は線形代数攻撃と呼ばれる．

3.3 t=1 の時の評価攻撃

本節ではあるパラメータで，選択平文攻撃が可能な条件の下での識別不可能性を破ることができる評価攻撃について述べる．サイズ l の多項式で不定方程式の解であるものを不定方程式の小さな解と定義する．

(1) $t = 1$ の時を考えるので，$\mathbb{F}_p$ 上の不定方程式 $X(x, y, 1) = 0$ を考える．

(2) 全数探索を行い, $\mathbb{F}_p$ における $X(x, y, 1) = 0$ の小さな解 $(0 \le u'_x, u'_y \le n(\ell - 1))$ を見つける．そのような解の存在は, $X(u_x(1), u_x(1), 1) = 0$ より保証される．実際, 秘密鍵が以下のように表される．

$$(u'_x, u'_y) = (u_x(1), u_y(1)).$$

秘密鍵が以下のように表されるとすると

$$(u_x(t), u_y(t)) = (\sum_{i=0}^{n-1} \alpha_i t^i,\ \sum_{i=0}^{n-1} \beta_i t^i).$$

解 (u'_x, u'_y) のそれぞれの値の上界は次のようになる．

$$0 \le u'_x, u'_y \le max(\sum_{i=0}^{n-1} \alpha_i, \sum_{i=0}^{n-1} \beta_i) \le n(l-1).$$

この時最小解 (u'_x, u'_y) は以下の二つの方法で見つけることができる．

- $n^2(l-1)^2$ 個の値をすべて不定方程式に代入してみる．
- 最大 $n(l-1)$ 回, 一変数方程式を解く．

(3) $b = 1$ とし，平文は $c(x, y, t) = m_b(t) + X(x, y, t)r(x, y, t) + l \cdot e(x, y, t)$ と暗号化されるので (u'_x, u'_y) を代入して

$$c(u'_x, u'_y, 1) \equiv m_b(1) + l \cdot e(u'_x, u'_y, 1)\ mod\ l$$

を計算する．

(4) $m_b(1) + l \cdot e(u'_x, u'_y, 1) \equiv m_b(1)\ mod\ l$ となる $m_b(1)$ を計算する．

(5) $m_0(1) \not\equiv m_1(1)\ mod\ l$ の条件の下で, $m_b(1) \bmod l$ から $b = 0$ か $b = 1$ かを区別する．

以上の 5 ステップで攻撃は構成されるが,$m_b(1) \bmod l$ が得られるには,

$$p > max\{c(u'_x, u'_y, 1) \mid 0 \le u'_x, u'_y \le n(l-1)\}$$

を満たす必要があり, $c(u'_x, u'_y, 1)$ は

$$\begin{aligned} c(u'_x, u'_y, 1) &= m(1) + l \cdot e(u'_x, u'_y) \\ &= m(1) + l \cdot \sum_{(i,j)\in\Gamma_e} e_{ij}(1)(u'_x)^i(u'_y)^j \end{aligned}$$

であり, さらに

$$0 \le m(1), e_{ij}(1) \le n(l-1)$$

であるから, p は

$$\begin{aligned} p &> max\{c(u'_x, u'_y, 1) \mid 0 \le u'_x, u'_y \le n(l-1)\} \\ &= n(l-1) + l \cdot \sum_{(i,j)\in\Gamma_e} (n(l-1))^{i+j+1} \\ &= n(l-1) + l \cdot \sum_{k=0}^{dX+dr} (k+1)(n(l-1))^{k+1} \end{aligned}$$

を満たす必要がある．秋山氏らは識別攻撃の実験を行い，その結果，不定方程式暗号が IND-CPA 安全性を満たすためには，n, p がある基準を満たす値である必要があり，秋山氏らは $n = 1201, 1733, 2267$ の三つのパラメータならば IND-CPA 安全であると述べている．

Vol.2019-DPS-178 No.24
Vol.2019-CSEC-84 No.24
2019/3/5

4. t=1 の時の代入識別攻撃

本節では前節で紹介した評価攻撃と同様に $t=1$ を代入したときの攻撃を新たに提案する．パラメータに 1 を代入する攻撃は，Ring-LWE や PLWE に対する攻撃 [6][7] として提案されている．前節の線形代数攻撃と同様に以下のように線形方程式を作る．

$$\begin{aligned}
a_{10}r_{10} + e_{20} &= d_{20,}\\
a_{10}r_{01} + a_{01}r_{10} + e_{11} &= d_{11},\\
a_{01}r_{01} + e_{02} &= d_{02},\\
a_{10}r_{00} + a_{00}r_{10} + e_{10} &= d_{10},\\
a_{01}r_{00} + a_{00}r_{01} + e_{01} &= d_{01},\\
a_{00}r_{00} + e_{00} &= d_{00}.
\end{aligned}$$

上式の $a_{ij}, r_{ij}, e_{ij}, d_{ij}$ はすべて t の $n-1$ 次式で表されており，$t=1$ を代入しその時の値を $a_{ij}[1]$ のように表すとする．さらに整数上の方程式とするために上式すべての左辺に ph_{ij} を加えると以下のようになる．

$$\begin{aligned}
a_{10}[1]r_{10}[1] + e_{20}[1] + qh_{20} &= d_{20}[1],\\
a_{10}[1]r_{01}[1] + a_{01}[1]r_{10}[1] + e_{11}[1] + qh_{11} &= d_{11}[1],\\
a_{01}[1]r_{01}[1] + e_{02}[1] + qh_{01} &= d_{02}[1],\\
a_{10}[1]r_{00}[1] + a_{00}[1]r_{10}[1] + e_{10}[1] + qh_{10} &= d_{10}[1],\\
a_{01}[1]r_{00}[1] + a_{00}[1]r_{01}[1] + e_{01}[1] + qh_{01} &= d_{01}[1],\\
a_{00}[1]r_{00}[1] + e_{00}[1] + qh_{00} &= d_{00}[1],
\end{aligned}$$

さらに行列表示すると（[1] は省略）

$$\begin{pmatrix}
a_{10} & 0 & 0 & p & 0 & 0 & 0 & 0 & 0\\
a_{01} & a_{10} & 0 & 0 & p & 0 & 0 & 0 & 0\\
0 & a_{01} & 0 & 0 & 0 & p & 0 & 0 & 0\\
a_{00} & 0 & a_{10} & 0 & 0 & 0 & p & 0 & 0\\
0 & a_{00} & a_{01} & 0 & 0 & 0 & 0 & p & 0\\
0 & 0 & a_{00} & 0 & 0 & 0 & 0 & 0 & p
\end{pmatrix}
\begin{pmatrix}
r_{10}\\ r_{01}\\ r_{00}\\ h_{20}\\ h_{11}\\ h_{02}\\ h_{10}\\ h_{01}\\ h_{00}
\end{pmatrix}$$

$$+ \begin{pmatrix} e_{20}\\ e_{11}\\ e_{02}\\ e_{10}\\ e_{01}\\ e_{00} \end{pmatrix} = \begin{pmatrix} d_{20}\\ d_{11}\\ d_{02}\\ d_{10}\\ d_{01}\\ d_{00} \end{pmatrix}$$

と表される．よって $0 \le e_ij[1] \le n(\ell-1)$ は小さいため，格子

$$\begin{pmatrix}
a_{10} & 0 & 0 & p & 0 & 0 & 0 & 0 & 0\\
a_{01} & a_{10} & 0 & 0 & p & 0 & 0 & 0 & 0\\
0 & a_{01} & 0 & 0 & 0 & p & 0 & 0 & 0\\
a_{00} & 0 & a_{10} & 0 & 0 & 0 & p & 0 & 0\\
0 & a_{00} & a_{01} & 0 & 0 & 0 & 0 & p & 0\\
0 & 0 & a_{00} & 0 & 0 & 0 & 0 & 0 & p
\end{pmatrix}$$

の中で $(d_{20}\ d_{11}\ d_{02}\ d_{10}\ d_{01}\ d_{00})^{\mathrm{T}}$ に最も近いベクトルを見つけることができればそのベクトルから $(d_{20}\ d_{11}\ d_{02}\ d_{10}\ d_{01}\ d_{00})^{\mathrm{T}}$ を引くことにより $(e_{20}\ e_{11}\ e_{02}\ e_{10}\ e_{01}\ e_{00})^{\mathrm{T}}$ を得ることができると考えられる．つまり最近ベクトル問題に帰着できる．CVP を解いた結果，ノイズのすべての係数が $n \times (l-1)$ 以下になった場合，その (X, Y) の組は IE-LWE instance であると判定する．

5. 計算機実験

本節では，前節で述べた代入識別攻撃についての計算機実験について報告する．実験の手順としては，まず IE-LWE instance である X, Y をサンプリングし，そのサンプルに攻撃を行うことによって IE-LWE instance かどうか判別する．次に，ランダムな (X, Y) の組をサンプリングし，そのサンプルに攻撃を行い，IE-LWE instanse と判断してしまわないかどうかを検証する．表 2 では，結果として $n \times (l-1)$ の小さな値が見つかった場合失敗とし，そうでない場合成功としている．

本実験では，$l=4$ つまり秘密鍵 $(u_x(t), u_y(t))$ の係数は 0 から 3 であり，攻撃の試行回数は 100000 回である．計算機環境を以下に示す．

- CPU: Intel(R)XeonCPU E7-4830 v4@2.00GHz
- RAM: 3TB
- OS: Ubuntu 10.04.5 LTS
- プログラミング言語: magma [5]

表 1 IE-LWE instance に対する攻撃

k	n	p	成功回数	成功確率	攻撃の平均時間 (s)
143	1201	467424413	100000	1	0.32235
207	1733	973190461	100000	1	0.61882

表 2 ランダムな sample(X,Y) に対する攻撃

k	n	p	失敗回数	成功回数	識別失敗の割合	攻撃の平均時間 (s)
143	1201	467424413	130	99870	0.0013	0.22551
207	1733	973190461	151	99849	0.00151	0.43368

以上の実験結果からセキュリティパラメータが $k = 143, 207$ のいずれの場合であっても，高い確率でノイズを求めることができた．つまり，二つの多項式の組 (X, Y)

が与えられたとき本稿の提案手法によって，その組が IE-LWE instance であるかどうか判別することができ，さらに Giophantus の IND-CPA 安全性を破ることができると考えられる．

6. 結論

秋山氏らが提案した, 不定方程式の特定の最小解を求める問題の計算困難性に基づく耐量子暗号の候補 (Giophantus) は, IE-LWE 問題の困難性を仮定すれば, IND-CPA 安全であることが示されている．本研究では IE-LWE 問題に対する新しい $t = 1$ の代入識別攻撃を行った．提案手法では, IE-LWE 問題に現れる変数 t に 1 を代入することにより，非常に低次元の格子問題に帰着しており，最近ベクトル問題を解くことによって分布の識別を行っている．格子の次元が小さいことにより，高速に攻撃を行うことができ，また提案攻撃が既存の代入攻撃を回避できるパラメータに対しても有効であることを実験的に確かめた．SCIS2019 で秋山氏らが改良した IE-LWE を利用した暗号方式には本稿の提案手法の攻撃は成功しないと思われる．よって，今後の課題として新たな暗号方式に対しても成功する攻撃を検討していく．

謝辞 本研究の一部は JSPS 科研費基盤 C (JP15K00183), JSPS 科研費若手 B(JP17K184500) Microsoft Research Asia の共同研究費, 科学技術振興機構（JST）の CREST(JPMJCR1404) と国際科学技術協力基盤整備事業（日本―台湾研究交流）, 及び 文部科学省の情報技術人材育成のための実践教育ネットワーク形成事業 分野・地域を越えた実践的情報教育協働ネットワーク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] Koichiro Akiyama, Yasuhiro Goto, Hideyuki Miyake: An Algebraic Surface Cryptosystem. Public Key Cryptography (2009).
[2] Koichiro Akiyama, Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida, Goichiro Hanaoka: A Public-Key Encryption Scheme Based on Non-linear Indeterminate Equations. SAC (2017).
[3] Koichiro Akiyama, Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida, Goichiro Hanaoka, Hideo Shimizu, Yasuhiko Ikematsu: A Public-key Encryption Scheme Based on Non-linear Indeterminate Equations (Giophantus). IACR Cryptology ePrint Archive 2017: 1241 (2017).
[4] Miklós Ajtai, Cynthia Dwork: A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence. STOC (1997).
[5] W. Bosma, J. Cannon, and C. Playoust: The Magma algebra system. I. The user language, J.Symbolic Comput. 24 (1997).
[6] Yara Elias, Kristin E. Lauter, Ekin Ozman, Katherine E. Stange: Provably Weak Instances of Ring-LWE. CRYPTO (1) (2015).
[7] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter : Weak Instances of PLWE. Selected Areas in Cryptography (2014).
[8] Yasuhiko Ikematsu, Koichiro Akiyama, Tsuyoshi Takagi: An Improvement on the Linear Algebraic Attack for the Indeterminate Equation Encryption Scheme. SCIS (2018).
[9] Yasuhiko Ikematsu, Koichiro Akiyama, Tsuyoshi Takagi: 不定方程式における鍵復元攻撃の改良及びパラメータの考察．SCIS(2018).
[10] Tsutomu Matsumoto, Hideki Imai: Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption. EUROCRYPT (1988).
[11] R.J.McEliece: A Public-Key Cryptosystem Based On Algebraic Coding Theory,The Deep Space Network Progress Report DSN PR(1978).
[12] Oded Regev: On lattices, learning with errors, random linear codes, and cryptography. J. ACM 5 (2009).
[13] Peter W. Shor : Algorithms for Quantum Computation: Discrete Logarithms and Factoring. FOCS (1994).
[14] Keita Xagawa: Practical Cryptanalysis of a Public-key Encryption Scheme Based on Non-linear Indeterminate Equations at SAC 2017. IACR Cryptology ePrint Archive 2017: 1224 (2017).