数理解析研究所講究録
第1652巻 2009年 162-172

脆弱性のない代数曲面公開鍵暗号にむけて

Towards designing the invulnerable algebraic surface public-key cryptosystem

岩見 真希
MAKI IWAMI
大阪経済法科大学　教養部
FACULTY OF LIBERAL ARTS AND SCIENCES, OSAKA UNIVERSITY OF ECONOMICS AND LAW*

Abstract

代数曲面公開鍵暗号は，代数曲面の定義方式を公開鍵，代数曲面上の代数曲線を秘密鍵とし，代数曲面上のセクションを求める問題（求セクション問題）の計算困難性に安全性の根拠をおく新しいタイプの公開鍵暗号として，2005年に秋山と後藤により提案された．しかし，公開鍵がある条件を満たすとき，公開鍵と暗号文から，求セクション問題を解くことなく効率よく平文を求めることができる攻撃法が，2007年に内山と徳永により提案された．そこで筆者は，まず，体 $\mathbb{F}_p$ 上の多項式環で行われる内山-徳永の攻撃法を，有理関数体上の多項式環で行えるように拡張することで，全ての場合に適用可能な攻撃法を提案し，その後，グレブナー基底のテクニックを用いることで，全ての場合に適用可能な，体 $\mathbb{F}_p$ 上の多項式環での攻撃法を提案した．本稿では，代数曲面の零点の計算法の説明およびそれを用いた新たな攻撃法の提案を行い，それゆえ，2005年の代数曲面公開鍵暗号と大筋を変えない方法のままでは脆弱性のない新しい代数曲面公開鍵暗号の提案は難しいことを述べる．

Abstract

An Algebraic Surfaces Public-key Cryptosystem was developed by Akiyama and Goto in 2005 as a new type of public key cryptosystem based on the mathematical problem of obtaining factors on an algebraic surface, whose public key is the defining equation of an algebraic surface and the secret keys are algebraic curves on it. But in 2007, in the case that the defining equation of the surface used for the public key is in a certain form, Uchiyama and Tokunaga successed to attack in the sense of getting plaintexts from corresponding ciphertexts efficiently without solving section finding problem. Uchiyama-Tokunaga's attack is performed in the polynomial ring over $\mathbb{F}_p$ under some assumptions whereas the author suggested two algorithms applicable to all cases. One is by extending it to be able to perform in the polynomial ring over rational function field, and the other is by utilizing Gröbner bases techniques in the polynomial ring over $\mathbb{F}_p$. In this paper, methods for calculating zero point of the algebraic surface and a new attack utilizing it are presented, and the approach result in a difficulty of making a suggestion of the invulnerable algebraic surface public-key cryptosystem without changing ideas progressively. [1)]

1　はじめに

公開鍵暗号は，暗号化する鍵が公開できるという特性から，初めてアクセスしてきた相手とも安全な秘密通信を行うことができるため，現在，広く普及している．しかし，現在の公開鍵暗号の技術では，秘密鍵暗号に比べて処理時間や電力がかかるため，携帯電話などのモバイル機器への利用は難しいといわれている．また，量子計算機が実現すると解読されてしまうため，新しい公開鍵暗号の開発が求められている．これら

*maki@keiho-u.ac.jp

1)A part of this work was supported by JSPS. Grant-in-Aid for Scientific Research.

の問題に対処すべく，2005年に秋山（東芝）と後藤（北海道教育大）は，量子計算機による解読にも強く，モバイル機器への導入も視野に入れた暗号として，代数曲面上のセクションを求める問題（求セクション問題）の計算困難性に安全性の根拠をおく代数曲面公開鍵暗号を開発した．この求セクション問題はNP完全である多次多変数方程式を解く問題に帰着される．秋山-後藤代数曲面公開鍵暗号 [1, 3, 4] は，2005年2月，東芝研究開発センターのWebサイト [2] で最新技術情報として一般向けにも公開されている．しかし，2007年に内山と徳永（首都大学東京）が，公開鍵として用いられる代数曲面の定義方程式がある条件を満たすとき，1つの暗号文と公開鍵から，簡約を利用することで，求セクション問題を解くことなく，対応する平文を求める攻撃法を考案し [5]，そのことが，CRYPTREC report 2006 [6] の“付録3 代数曲面を用いた公開鍵暗号の安全性について”の中の“(4) 公開鍵アルゴリズム”でも紹介されている．そこで筆者は，2007年，内山-徳永の攻撃法が体 $\mathbb{F}_p$ 上の多項式環で行なわれる条件つき攻撃法であるのに対して，それを有理関数体上の多項式環で行うことができるように拡張することで，全ての場合に適用可能な攻撃法 [8] を提案した．さらに，グレブナー基底のテクニックを用いることで，体 $\mathbb{F}_p$ 上の多項式環での，全ての場合に適用可能な新しい攻撃法 [8] を提案した．また，攻撃例として，toy example を掲載している．

本稿では，**2章**で秋山-後藤代数曲面公開鍵暗号のサーベイ，**3章**で内山-徳永の条件つき攻撃法のサーベイおよび条件が付く理由の検証，**4章**で筆者による全ての場合に適用可能な有理関数体上の多項式環での攻撃法 [?] をサーベイ，**5章**で，全ての場合に適用可能な，グレブナー基底を利用することで体 $\mathbb{F}_p$ 上の多項式環で扱える攻撃法をサーベイする．これらの手法の証明等，詳しくは [9] を参照されたい．したがって，今後，これらの攻撃に耐える，つまり脆弱性のない代数曲面公開鍵暗号の提案が必要である．**6章**では，代数曲面の零点の計算法とそれを利用した新たな攻撃法の提案を行い，それゆえ，今後の改良が2005年の代数曲面公開鍵暗号のアイディアの延長線上にある限り，その攻撃法が成功すること，すなわち，安全な新しい代数曲面公開鍵暗号を提案するためには，発想の転換が必要であることを述べる．

2 秋山-後藤代数曲面公開鍵暗号 [1, 3, 4]

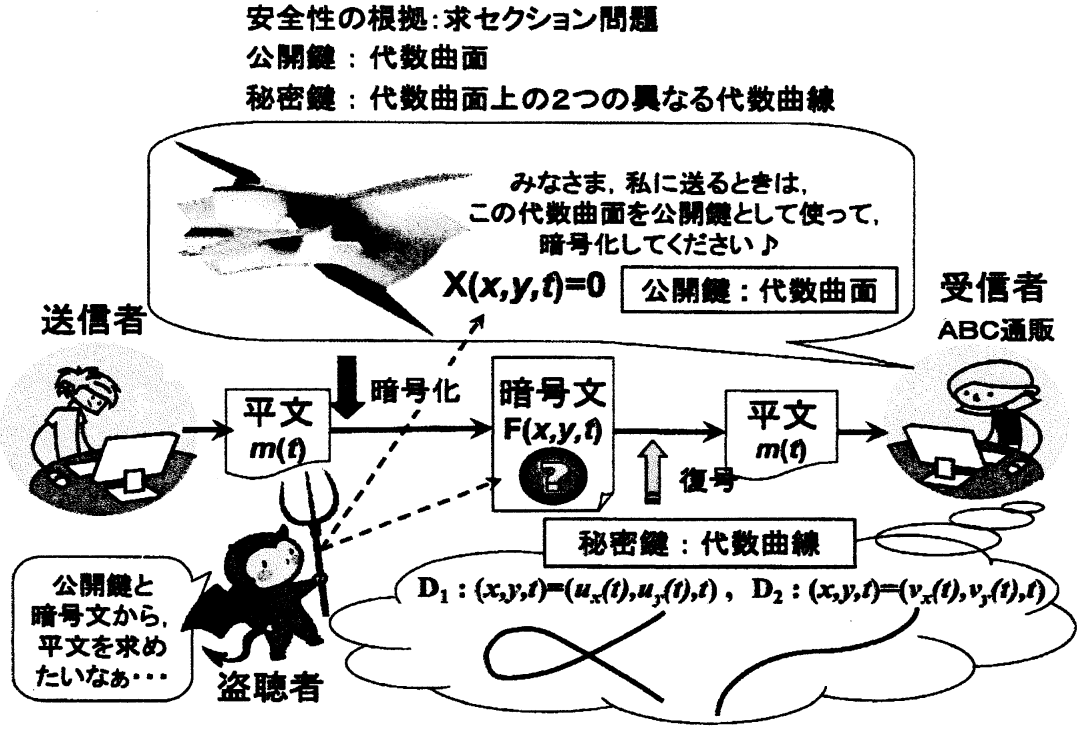

図 1: 秋山-後藤代数曲面公開鍵暗号のスケッチ

本章では，秋山-後藤代数曲面公開鍵暗号をサーベイする．ここで，$\mathbb{F}_p$ 上で定義された代数曲面を考える．

[鍵生成]

1. 秘密鍵: $\mathbb{A}^3(\mathbb{F}_p)$ 内の t をパラメータとする 2 つの異なる曲線 D_1 と D_2 を選ぶ．
   (a) $D_1 : (x,y,t) = (u_x(t), u_y(t), t)$　　(b) $D_2 : (x,y,t) = (v_x(t), v_y(t), t)$
   ただし，復号結果の一意性のため，$\deg u_x(t) \neq \deg v_x(t)$ または $\deg u_y(t) \neq \deg v_y(t)$ を満たすとする．

2. 公開鍵:

   (a) D_1, D_2 を含む，体 $\mathbb{F}_p$ 上の曲面 $X(x,y,t) = 0$ を構成する．このとき $X(u_x(t), u_y(t), t) = X(v_x(t), v_y(t), t) = 0$ を満たす．実際，D_1, D_2 を含む $X(x,y,t) = 0$ は次の方法で構成する．
   まず，$X(x,y,t) = \sum_{i,j} c_{ij}(t) x^i y^j = 0$ で定義される代数曲面を考える．
   $D_1 : (u_x(t), u_y(t), t)$ と $D_2 : (v_x(t), v_y(t), t)$ のようにパラメータ表示された 2 つの異なる曲線が X のセクションとなるための必要十分条件は $\sum_{i,j} c_{ij}(t) u_x(t)^i u_y(t)^j = \sum_{i,j} c_{ij}(t) v_x(t)^i v_y(t)^j = 0$.
   そして，$\sum_{(i,j)\neq(0,0)} c_{ij}(t) \left(u_x(t)^i u_y(t)^j - v_x(t)^i v_y(t)^j\right) = 0$ を満たすことが必要である．したがって，$c_{10}(t)\left(t u_x(t) - v_x(t)\right) = \sum_{(i,j)\neq(0,0),(1,0)} c_{ij}(t) \left(u_x(t)^i u_y(t)^j - v_x(t)^i v_y(t)^j\right)$.
   ここで，$u_x(t)^i u_y(t)^j - v_x(t)^i v_y(t)^j = (u_x(t)^i - v_x(t)^i) u_y(t)^j + v_x(t)^i (u_y(t)^j - v_y(t)^j)$ が成り立ち，この表現は，もし $(u_x(t) - v_x(t)) | (u_y(t) - v_y(t))$ ならば，$(u_x(t) - v_x(t))$ で割ることができる．すなわち，この条件を満たすならば，ランダムな多項式 $c_{ij}(t)$ $((i,j) \neq (0,0),(1,0))$ を用いて，多項式 $c_{10}(t)$ を決定できる．つまり鍵生成アルゴリズムは次のように書くことができる：

      1. $\lambda_x(t) | \lambda_y(t)$ を満たすランダムな 2 つの多項式 $\lambda_x(t), \lambda_y(t)$ を選ぶ．
         (これは $(u_x(t) - v_x(t)) | (u_y(t) - v_y(t))$ であるために必要な条件)
      2. ランダムに $v_x(t)$ を選び，$\lambda_x(t) + v_x(t)$ なる $u_x(t)$ を計算する．
         (*i.e.* $u_x(t) = \lambda_x(t) + v_x(t)$)
      3. ランダムに $v_y(t)$ を選び，$\lambda_y(t) + v_y(t)$ なる $u_y(t)$ を計算する．
         (*i.e.* $u_y(t) = \lambda_y(t) + v_y(t)$)
      4. ランダムに $c_{ij}(t)$ $((i,j) \neq (0,0),(1,0))$ を選び，次の条件を満たす $c_{10}(t)$ を計算する．
         $c_{10}(t)\left(u_x(t) - v_x(t)\right) = \sum_{(i,j)\neq(0,0),(1,0)} c_{ij}(t) \left(u_x(t)^i u_y(t)^j - v_x(t)^i v_y(t)^j\right)$.
      5. $\sum_{i,j} c_{ij}(t) u_x(t)^i u_y(t)^j = \sum_{i,j} c_{ij}(t) v_x(t)^i v_y(t)^j = 0$ より，c_{00} は
         $c_{00} = -\sum_{(i,j)\neq(0,0)} c_{ij}(t) u_x(t)^i u_y(t)^j$ で与えられる．

   以上のアルゴリズムより，$\deg_t X(x,y,t) = \deg c_{00}(t) \geq \deg_{xy} X(x,y,t) d$ を得る．
   ここで $\deg_{xy} X(x,y,t)$ は $X(x,y,t)$ の x と y に関する次数をあらわす．

   (b) 暗号化ステップで選ばれるモニックな既約多項式 $f(t) \in \mathbb{F}_p[t]$ の次数の下限として $\ell \in \mathbb{N}$ を選ぶ．
   セキュリティ上の理由から (詳細は [4] の 5.3 参照), $\deg_t X(x,y,t) < \ell$ を満たすように設定する．

   (c) $d \geq \max(\deg u_x(t), \deg u_y(t), \deg v_x(t), \deg v_y(t))$ を満たす $d \in \mathbb{N}$ を選ぶ．

ℓ もしくは d を大きくとることで，基礎体の標数 p を可能な限り小さく選ぶことができる (e.g. 最大 4 ビット)．鍵サイズの見積もりは [4]7 章を参照されたい．

[暗号化]

m を平文とする．m を $m = m_0 || m_1 || \cdots || m_{\ell-1}$ $(0 \leq m_i \leq p-1)$ なる小さなブロックに分割する．

1. m を次のように平文多項式に埋め込む： $m(t) = m_{\ell-1} t^{\ell-1} + \cdots + m_1 t + m_0$

2. セキュリティ上，次を満たすランダムな多項式 $s(x,y,t)$ を選ぶ (詳細は [4] の 5.3 参照)：
   $\alpha > \deg_x X(x,y,t)$ かつ $\beta > \deg_y X(x,y,t)$ を満たす項 $x^\alpha y^\beta$ を含み，さらに $(\deg_x s(x,y,t) +$

$\deg_y s(x,y,t))d+\deg_t s(x,y,t) < \ell$ を満たす. (この条件により, $\deg(s(u_x(t),u_y(t),t)-s(v_x(t),v_y(t),t)) < \ell$ が導かれ, 復号ステップにおいて, 因子 $f(t)$ を検出することができる)

3. $\deg_t r(x,y,t) < \ell$ を満たすランダムな多項式 $r(x,y,t)$ を選ぶ. (セキュリティ上必要な条件であり, 詳細は [4] の 5.3 を参照されたい)

4. $\deg f(t) \geq \ell$ なるモニックな既約多項式 $f(t)$ をランダムに選ぶ.

5. 暗号文である多項式 $F(x,y,t)$ を次で計算する: $F(x,y,t) = m(t)+f(t)s(x,y,t)+X(x,y,t)r(x,y,t)$.

[復号]

D_1, D_2 は X 上に存在するため, $X(u_x(t),u_y(t),t) = X(v_x(t),v_y(t),t) = 0$ を満たすことに注意されたい.

1. セクション D_1 および D_2 を $F(x,y,t)$ に代入する :
   $h_1(t) = F(u_x(t),u_y(t),t) = m(t) + f(t)s(u_x(t),u_y(t),t)$
   $h_2(t) = F(v_x(t),v_y(t),t) = m(t) + f(t)s(v_x(t),v_y(t),t)$

2. $h_1(t) - h_2(t)$ を計算する : $h_1(t) - h_2(t) = f(t)\left(s(u_x(t),u_y(t),t) - s(v_x(t),v_y(t),t)\right)$

3. $h_1(t) - h_2(t)$ を因数分解し, すべの因子の中で次数が最大のモニックな既約多項式 $f(t)$ を検出する. (この方法で $f(t)$ が検出される理由は次を参照されたい)

4. $h_1(t)$ の $f(t)$ に関する正規形を計算し, $m(t)$ を得る. ($\deg m(t) < \deg f(t)$.)

5. $m(t)$ から m を求める.

例 1 (鍵生成)

以後, 本稿の例では, 体 $\mathbb{F}_2$ を扱うものとする.

[秘密鍵] $\lambda_x(t)|\lambda_y(t)$ を満たすようにランダムに生成された多項式を $\lambda_x(t) := t^2+1$, $\lambda_y(t) := t(t^2+1)$, $u_x(t) := t^2+t$, $u_y(t) := t^3+t^2+t+1$ とする. そして $v_x(t) := u_x(t)-\lambda_x(t) = 1+t$, $v_y(t) := u_y(t)-\lambda_y(t) = 1+t^2$ を計算する. このとき, 秘密鍵は次のような異なる 2 つの曲線で定義される.

$D_1 : (u_x(t),u_y(t),t) = (t^2+t, t^3+t^2+t+1, t)$, $\quad D_2 : (v_x(t),v_y(t),t) = (1+t, 1+t^2, t)$.

[公開鍵] 2 つの曲線 (秘密鍵) を含む代数曲面 $X(x,y,t) = \sum_{i,j} c_{ij}(t)x^iy^j$ (公開鍵) を生成するために, ランダムに $c_{ij}(t)((i,j) \neq (0,0),(1,0))$ を生成し, $c_{10}(t)$ および $c_{00}(t) \in \mathbb{F}_2(t)$ を次で計算する.

$c_{10}(t) := -\sum_{(i,j)\neq(0,0),(1,0)} c_{i,j}(t)\left(u_x(t)^iu_y(t)^j - v_x(t)^iv_y(t)^j\right)/(u_x(t)-v_x(t))$

$c_{00}(t) := -\sum_{(i,j)\neq(0,0)} c_{i,j}(t)u_x(t)^iu_y(t)^j$.

例えば, 次のような $X_A(x,y,t)$ および $X_B(x,y,t)$ が生成される.

(以後, 紙面上で見やすくするために, 便宜上, x や y でくくることがある)

$X_A(x,y,t) := y^5+x^5+(t^6+t^4+t^3+t+1)x^2y+(t^{13}+t^{12}+t^{11}+t^{10}+t^7+t^5+t^3)x+(t^8+t^7+t^4+t+1)y+t^{14}+t^9+t^7+t^6+t^5+t^4+t^3+t$,

$X_B(x,y,t) := t^2+t^8+t^{12}+t^{14}+t^{21}+t^{22}+t^{23}+t^{24}+t^{26}+t^{27}+t^{28}+t^{29}+y+t^2y+y^2+t^3y^2+y^3+t^2y^3+t^3y^3+ty^4+t^2y^4+t^4y^4+t^5y^4+y^5+t^4y^5+x(t+t^3+t^5+t^{10}+t^{11}+t^{16}+t^{17}+t^{19}+t^{21}+t^{23}+t^{26}+t^{28}+t^3y+t^4y+y^2+ty^2+t^3y^2+y^3+ty^3+t^3y^3+t^5y^3+y^4+ty^4+t^2y^4+t^3y^4+t^4y^4+y^5+t^2y^5)+x^4(1+t^2+t^4+t^5+t^3y+t^4y+t^5y+y^2+ty^2+t^2y^2+t^3y^2+t^4y^2+ty^3+t^2y^3+t^4y^3+y^4+t^2y^4+t^3y^4+t^5y^4+y^5+t^4y^5)+x^3(t+t^3+t^4+t^5+y+ty+t^3y+t^5y+t^2y^2+t^4y^2+y^3+t^2y^3+t^3y^3+t^5y^3+t^2y^4+t^3y^4+y^5+t^5y^5)+x^2(t+t^5+t^2y+t^4y+y^2+ty^2+ty^3+t^2y^3+t^3y^3+t^4y^3+t^5y^3+y^4+ty^4+t^3y^4+t^4y^4+y^5+ty^5+t^5y^5)+x^5(1+t^3+ty+t^2y+t^3y+t^4y+t^4y^2+t^5y^2+ty^3+t^2y^3+t^4y^3+y^4+t^2y^4+t^4y^4+ty^5+t^2y^5+t^5y^5)$

$X_i(x,y,t)$ $(i = A,B)$ が 2 つの曲線を含むことは, $X_i(u_x(t),u_y(t),t) = X_i(v_x(t),v_y(t),t) = 0$ をチェックすることで確かめることができる.

注意 1

ここでは，辞書式順序を用いることとする．$X_A(x,y,t)$ を使用する場合，主項 $\mathrm{LT}(X_A)=x^5$ が**仮定 1**(**3** 章参照) を満たすため，内山-徳永の攻撃法で解読することができる．一方，$X_B(x,y,t)$ を使用する場合，主項 $\mathrm{LT}(X_B)=t(1+t+t^4)x^5y^5$ が**仮定 1** を満たさないため，内山-徳永の攻撃法が適用できない．それに対し，**4** 章の有理関数体上の多項式環への拡張による攻撃法，**5** 章のグレブナー基底のテクニックを用いた $\mathbb{F}_p$ 上の多項式環での攻撃法，**6** 章の代数曲面の零点を利用した新たな攻撃法は，全ての場合，すなわち $X_A(x,y,t)$ と $X_B(x,y,t)$ の両方に適用可能である．

例 2 (暗号化と復号)

[暗号化]

$m(t)$ (平文多項式), $f(t), s(x,y,t)$, そして $r(x,y,t)$ を次のように設定する．

$m(t) := 1+t+t^2+t^3+t^4+t^6+t^8+t^9+t^{14}+t^{17}+t^{19}+t^{20}+t^{23}+t^{26}+t^{28}+t^{29}+t^{30}+t^{32}+t^{34}+t^{35}+t^{36}+t^{37}+t^{39}$,

$f(t) := 1+t+t^2+t^4+t^7+t^9+t^{10}+t^{11}+t^{14}+t^{17}+t^{22}+t^{23}+t^{25}+t^{26}+t^{27}+t^{28}+t^{32}+t^{34}+t^{36}+t^{38}+t^{40}$,

$s(x,y,t) := t+t^3+x^3+y^2+x^6y^6$, $r(x,y,t) := 1+t^3+t^4+xy+y^2$.

$\mathbb{F}_2[x,y,t]$ で，暗号文 $F_A(x,y,t)$ は $X_A(x,y,t)$ を用いて次のように計算される．

$F_A(x,y,t) := m(t)+f(t)s(x,y,t)+X_A(x,y,t)r(x,y,t) = 1+t+t^6+t^{12}+t^{14}+t^{15}+t^{17}+t^{19}+t^{24}+t^{25}+t^{26}+t^{27}+t^{28}+t^{29}+t^{31}+t^{32}+t^{33}+t^{34}+t^{35}+t^{36}+t^{37}+t^{39}+t^{43}+y+ty+t^3y+t^4y+t^5y+t^{10}y+t^{12}y+y^2+t^2y^2+t^3y^2+t^5y^2+t^6y^2+t^{10}y^2+t^{11}y^2+t^{17}y^2+t^{22}y^2+t^{23}y^2+t^{25}y^2+t^{26}y^2+t^{27}y^2+t^{28}y^2+t^{32}y^2+t^{34}y^2+t^{36}y^2+t^{38}y^2+t^{40}y^2+y^3+ty^3+t^4y^3+t^7y^3+t^8y^3+y^5+t^3y^5+t^4y^5+y^7+x^5(1+t^3+t^4+y^2)+x^3(1+t+t^2+t^4+t^7+t^9+t^{10}+t^{11}+t^{14}+t^{17}+t^{22}+t^{23}+t^{25}+t^{26}+t^{27}+t^{28}+t^{32}+t^{34}+t^{36}+t^{38}+t^{40}+y^2+ty^2+t^3y^2+t^4y^2+t^6y^2)+x^2(y+ty+t^3y+t^4y+t^7y+t^8y+t^9y+t^{11}y+t^{12}y+t^{13}y+y^3+ty^3+t^3y^3+t^4y^3+t^6y^3)+x(t^3+t^5+t^6+t^8+t^9+t^{12}+t^{17}+ty+t^3y+t^4y+t^5y+t^6y+t^7y+t^9y+t^{14}y+y^2+ty^2+t^3y^2+t^4y^2+t^5y^2+t^8y^2+t^{10}y^2+t^{11}y^2+t^{12}y^2+t^{13}y^2+y^6)+x^6(y+y^6+ty^6+t^2y^6+t^4y^6+t^7y^6+t^9y^6+t^{10}y^6+t^{11}y^6+t^{14}y^6+t^{17}y^6+t^{22}y^6+t^{23}y^6+t^{25}y^6+t^{26}y^6+t^{27}y^6+t^{28}y^6+t^{32}y^6+t^{34}y^6+t^{36}y^6+t^{38}y^6+t^{40}y^6)$.

[復号]

$F_A(u_x(t),u_y(t),t)-F_A(v_x(t),v_y(t),t) = (t(1+t)^5(1+t^2+t^3)(1+t^2+t^6+t^8+t^9+t^{10}+t^{11}+t^{12}+t^{15}+t^{17}+t^{18}+t^{19}+t^{21})(1+t+t^2+t^4+t^7+t^9+t^{10}+t^{11}+t^{14}+t^{17}+t^{22}+t^{23}+t^{25}+t^{26}+t^{27}+t^{28}+t^{32}+t^{34}+t^{36}+t^{38}+t^{40})$.

ここで，最大の次数をもつ因子として $f(t)$ が検出される．最後に，$F(x,y,t)$ の $f(t)$ に関する正規形を計算し（次のように $\xrightarrow[f(t)]{*}$ を用いてあらわす），平文多項式を得る．

$$F_A(x,y,t) \xrightarrow[f(t)]{*} 1+t+t^2+t^3+t^4+t^6+t^8+t^9+t^{14}+t^{17}+t^{19}+t^{20}+t^{23}+t^{26}+t^{28}+t^{29}+t^{30}+t^{32}+t^{34}+t^{35}+t^{36}+t^{37}+t^{39} \ (=m(t))$$

例 3 (暗号化と復号)

$X_B(x,y,t)$ を公開鍵として使用した場合，同様に，対応する暗号文 $F_B(x,y,t)$ は次のように計算される．

$F_B(x,y,t) := m(t)+f(t)s(x,y,t)+X_B(x,y,t)r(x,y,t) = t^2+t^8+t^{12}+t^{14}+t^{21}+t^{22}+t^{23}+t^{24}+t^{26}+t^{27}+t^{28}+t^{29}+y+t^2y+y^2+t^3y^2+y^3+t^2y^3+t^3y^3+ty^4+t^2y^4+t^4y^4+t^5y^4+y^5+t^4y^5+x(t+t^3+t^5+t^{10}+t^{11}+t^{16}+t^{17}+t^{19}+t^{21}+t^{23}+t^{26}+t^{28}+t^3y+t^4y+y^2+ty^2+t^3y^2+y^3+ty^3+t^3y^3+t^5y^3+y^4+ty^4+t^2y^4+t^3y^4+t^4y^4+y^5+t^2y^5)+x^4(1+t^2+t^4+t^5+t^3y+t^4y+t^5y+y^2+ty^2+t^2y^2+t^3y^2+t^4y^2+ty^3+t^2y^3+t^4y^3+y^4+t^2y^4+t^3y^4+t^5y^4+y^5+t^4y^5)+x^3(t+t^3+t^4+t^5+y+ty+t^3y+t^5y+t^2y^2+t^4y^2+y^3+t^2y^3+t^3y^3+t^5y^3+t^2y^4+t^3y^4+y^5+t^5y^5)+x^2(t+t^5+t^2y+t^4y+y^2+ty^2+ty^3+t^2y^3+t^3y^3+t^4y^3+t^5y^3+y^4+ty^4+t^3y^4+t^4y^4+y^5+ty^5+t^5y^5)+x^5(1+t^3+ty+t^2y+t^3y+t^4y+t^4y^2+t^5y^2+ty^3+t^2y^3+t^4y^3+y^4+t^2y^4+t^4y^4+ty^5+t^2y^5+t^5y^5)$.

そして，**例 2** と同様に復号される．

3 内山-徳永の条件付き攻撃法 [5]

後章で全ての場合に適用可能な攻撃法を提案するために，まず，次の仮定を満たす場合のみに適用可能な内山-徳永の攻撃法を簡単にサーベイする．[5] では「割る」,「余り」,「先頭項」という表現を用いているところを，(同じ意味であるが) 後章への発展の都合上，それぞれ「正規化する (正規形になるまで簡約を繰り返す)」,「正規形」,「主項」という表現におきかえ，各因子の属するドメインも追記して引用している．

仮定 1
公開鍵となる代数曲面 X の定義方程式の，単項式順序 $\hat{R}$ に関する主項 $\mathrm{LT}(X)$ が $cx^{\alpha}y^{\beta}$ where $c \in \mathbb{F}_p$ $((\alpha,\beta) \neq (0,0))$ なる形をしている．

アルゴリズム 1 (内山-徳永の条件付き攻撃法)

入力 : **仮定 1** を満たす秋山-後藤代数曲面公開鍵暗号の公開鍵 $X(x,y,t) \in \mathbb{F}_p[x,y,t]$
暗号文 $F(x,y,t) \in \mathbb{F}_p[x,y,t]$.
出力 : 暗号文 $F(x,y,t)$ に対応する平文 m

1. $F(x,y,t)$ の $X(x,y,t)$ に関する正規形 $R_1(x,y,t) \in \mathbb{F}_p[x,y,t]$ を求める．
2. R_1 の項で x^iy^j $((i,j) \neq (0,0))$ の形をしたもので係数が $\mathbb{F}_p$ の要素でないものをランダムに選び，その係数を C とする．
3. C の因子となる $\mathbb{F}_p[t]$ の要素を求め，その中に含まれる次数 ℓ 以上の既約因子の集合を $\hat{G}$ とする．R_1 の $\hat{G}$ の要素 g に関する正規形 n が $\mathbb{F}_p[t]$ の要素となるものを選ぶ．
4. 多項式 $n(t) = n_{k-1}t^{k-1} + \cdots + n_1t + n_0 \in \mathbb{F}_p[t]$ とおき $m = n_0||n_1||\cdots||n_{k-1}$ を出力して終了．

注意 2
内山-徳永の実装では，*Step 2*, *3* で，*Step2* の条件を満たす 2 つの異なる R_1 の項を取り，それらの係数を C_1, C_2 として，最大公約因子 $\mathrm{GCD}(C_1, C_2)$ 計算を利用して検出している．

命題 2 (Proposition1 in pp.79-80 in [7])
Let $G = \{g_1, \cdots, g_t\}$ be a Gröbner basis for an ideal $I \subset k[x_1, \cdots, x_n]$ and let $f \in k[x_1, \cdots, x_n]$ (which denotes the polynomial ring over the field k where $x_1, \cdots, x_n$ are variables). Then there is a unique $r \in k[x_1, \cdots, x_n]$ with the following two properties:
(i) There is $g \in I$ such that $f = g + r$, (ii) No term of r is reduced by any of $\mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_t)$.
In particular, r is the normal form of the reduction of f by G no matter how the elements of G are listed when using the reduction algorithm.

定理 3 (Theorem1 in [5])
アルゴリズム 1 の中で生成される多項式 $g(t), n(t)$ は，秋山-後藤 代数曲面公開鍵暗号での暗号化/復号の際に用いられる多項式 $f(t)$，平文から得られる多項式 $m(t)$ にそれぞれ一致している．すなわち，出力された平文は正しいものである．

例 4 (内山-徳永の攻撃法が適用できない例 : 仮定を満たさない公開鍵を使用した例 3 に対する検証)
$F_B(x,y,t)$ の $X_B(x,y,t)$ に関する正規形を計算する．いま，$\mathrm{LT}(X_B) = t(1+t+t^4)x^5y^5$ であるから，求める正規形を得ようとすると，**アルゴリズム 1** における $\mathbb{F}_p[x,y,t]$ での演算では簡約が進まない．そこで，

有理関数体 $\mathbb{F}_p(t)$ 上の多項式環 $\mathbb{F}_p(t)[x,y]$ に拡張して正規形を計算してみると，次が得られる．ここで，分母因子 $t(1+t+t^4)$ は $\mathrm{LT}(X_B)=t(1+t+t^4)x^5y^5$ により生じていることに注意されたい．
$R_B(x,y,t) := (1+t^3+t^7+\cdots+t^{44}y^{16}+t^{46}y^{16}+t^{48}y^{16}+x^2(t^4y^6+t^8y^6+t^{12}y^6+\cdots+t^{42}y^{16}+t^{45}y^{16}+t^{49}y^{16})+x(ty^6+t^4y^6+t^5y^6+\cdots+t^{45}y^{16}+t^{47}y^{16}+t^{49}y^{16})+x^4(t^6+t^4y^6+t^6y^6+\cdots+t^{46}y^{16}+t^47y^{16}+t^{50y^{16}})+x^3(1+t+t^2+\cdots+t^{48}y^{16}+t^{49}y^{16}+t^{50}y^{16}))/(1+t^3+ty+t^2y+t^3y+t^4y+t^4y^2+t^5y^2+ty^3+t^2y^3+t^4y^3+y^4+t^2y^4+t^4y^4+ty^5+t^2y^5+t^5y^5)^2$．しかし，分子に着目して $c_{00}(t)$ を除く非零な $c_{ij}(t)$ の GCD を計算しても 1 となり，$f(t)$ が検出できない．簡約の途中で，主項 $\mathrm{LT}(X_B)$ の主係数 $t(1+t+t^4)$ の影響で低次の項の次数が上がり，余分に簡約が行われ，検出に必要な低次項の形を壊しているからである．

4 全ての場合に適用可能な有理関数体上の多項式環での攻撃法 (岩見 [8])

$F(x,y,t)$ の $X(x,y,t)$ に関する正規形を $R_1(x,y,t)$, $s(x,y,t)$ の $X(x,y,t)$ に関する正規形を $R_2(x,y,t)$ とする．このとき，$F=G_1X+R_1$, $s=G_2X+R_2$, (G_1,G_2,R_1,R_2 は一意的) とかける．暗号文 $F=m(t)+f(t)s(x,y,t)+X(x,y,t)r(x,y,t)$ に代入すると

$$F(x,y,t)=m(t)+f(t)R_2(x,y,t)+X(x,y,t)(f(t)G_2(x,y,t)+r(x,y,t))$$

となり，実は $R_1(x,y,t)=m(t)+f(t)R_2(x,y,t)$ が成り立つため，X の主係数が定数のときには，F の X に関する正規形として $R_1(x,y,t)=m(t)+f(t)R_2(x,y,t)$ が得られ，$f(t)$ を検出してから，さらに $R_1(x,y,t)$ の $f(t)$ に関する正規形を計算することで $m(t)$ を求めることに成功した．しかし，**例 4** に見られるように，主項 $\mathrm{LT}(X)=c_\beta(t)x^\alpha y^\beta$ における $c_{\alpha\beta}(t)$ が定数でない場合 (t を含む場合)，$F(x,y,t)$ を $X(x,y,t)$ に関して正規化すると，必ずしも望まれる形 $F \xrightarrow[X]{} m(t)+f(t)R_2(x,y,t)$ で簡約が止まるとは限らない．簡約の途中で，主係数がかけあわされて剰余の t の次数が上がり，X の主項の項順序よりも高くなってしまい，望ましくない簡約が引き起こされることがある．その結果，$m(t)+f(t)R_2(x,y,t)$ の形が余分な簡約で崩れ，$f(t)$ の検出に失敗する．

本章では，すべての公開鍵の形に適用可能な攻撃法を提案する．主なアイディアは，$f(t)$ の検出を難しくする原因である主係数 $\mathrm{LC}(X)\in\mathbf{F}_p[t]$ をなくすこと，すなわち，公開鍵 $X(x,y,t)$ を x と y に関してモニックに変換してから，有理関数体 $\mathbb{F}_p(t)$ 上の多項式環 $\mathbb{F}_p(t)[x,y]$ で簡約を繰返し，正規形を計算することである．

アルゴリズム 2 (有理関数体上の多項式環での攻撃 [8])

入力 : 秋山-後藤代数曲面公開鍵暗号の公開鍵 $X(x,y,t)\in\mathbb{F}_p[x,y,t]$,
暗号文 $F(x,y,t)\in\mathbb{F}_p[x,y,t]$.
出力 : 暗号文 $F(x,y,t)$ に対応する平文 m.

0. 公開鍵 X を，$\tilde{X}:=X/\mathrm{LC}(X)\in\mathbb{F}_p(t)[x,y]$ でモニックに変換する．

1. F の $\tilde{X}$ に関する正規形 $R_1(x,y,t)\in\mathbb{F}_p(t)[x,y]$ を求める．

2. R_1 の項のうち，$c_{ij}(t)x^iy^j$ ($(i,j)\neq(0,0)$) の形をしたもので $c_{ij}(t)$ が $\mathbb{F}_p$ の要素でないものをランダムに選び，$c_{ij}(t)$ を通分し，その分子を $C(\in\mathbb{F}_p[t])$ とする．

3. C を $\mathbb{F}_p[t]$ で因数分解し，t の次数が ℓ 以上の既約因子の集合を $\hat{G}$ とする．R_1 の $\hat{G}$ の要素 g に関する正規形 n が，$\mathbb{F}_p[t]$ の要素となるものを選ぶ．

4. 多項式 $n(t)=n_{k-1}t^{k-1}+\cdots+n_1t+n_0\in\mathbb{F}_p[t]$ とおき $m=n_0||n_1||\cdots||n_{k-1}$ を出力して終了.

$m(t)$ を $\mathbb{F}_p(t)[x,y]$ の表現ではなく，$\mathbb{F}_p[x,y,t]$ で一意的に求めるためには，各簡約ステップで生じる有理式と，暗号文 F の t に関する多項式部分を，通分でまとめてしまうことなく処理を進める必要がある.

定理 4
アルゴリズム 2 の中で生成される多項式 $g(t),n(t)$ は，秋山-後藤代数曲面公開鍵暗号での暗号化/復号の際に用いられる多項式 $f(t)$，平文から得られる多項式 $m(t)$ にそれぞれ一致している．すなわち，出力された平文は正しいものである.

例 5
主係数が $\mathrm{LC}(X_B)=t(1+t+t^4)$ であるから，モニックにするための変換 $\tilde{X}_B(x,y,t):=X_B(x,y,t)/\mathrm{LC}(X_B)$ を施す．ここで，アルゴリズムは $\mathbb{F}_p(t)[x,y]$ (t に関する有理式体上の x,y に関する多項式環．この例では $p=2$) で実行されることに注意されたい．次の $R_1(x,y,t)$ の分母には $t^2(1+t+t^4)^3$ があらわれている.

$$F_B(x,y,t)\xrightarrow[\tilde{X}_B(x,y,t)]{*}R_1(x,y,t)(\in\mathbb{F}_2(t)[x,y])$$

次のリストは，$R_1(x,y,t)$ の非零の項 $c_{ij}x^iy^j$ における c_{ij} の集合の各要素をそれぞれ通分して $\mathbb{F}_2$ 上で因数分解して分子のみ取り出した集合である．最初の要素は c_{00} の分子である.

$t(1+t+t^2)(1+t+t^4)(1+t^2+t^3+t^4+t^5)(1+t^3+t^4+t^6+t^7+t^8+t^9+t^{10}+t^{11}+t^{12}+t^{13}+t^{14}+t^{15})(1+t^2+t^3+t^4+t^8+t^9+t^{11}+t^{13}+t^{17}+t^{20}+t^{22}+t^{23}+t^{24}+t^{25}+t^{27}+t^{29}+t^{30}+t^{31}+t^{36}+t^{37}+t^{38}+t^{39}+t^{40}+t^{41}+t^{43}+t^{47}+t^{49})$, $(1+t)^5(1+t+t^2)(1+t+t^4)(1+t^3+t^4+t^5+t^6+t^7+t^8+t^{10}+t^{12})(1+t^2+t^3+t^4+t^5+t^6+t^8+t^9+t^{11}+t^{13}+t^{14})(1+t+t^2+t^4+t^7+t^9+t^{10}+t^{11}+t^{14}+t^{17}+t^{22}+t^{23}+t^{25}+t^{26}+t^{27}+t^{28}+t^{32}+t^{34}+t^{36}+t^{38}+t^{40})$, $t^2(1+t+t^4)(1+t^3+t^4)^2(1+t+t^2+t^4+t^7+t^9+t^{10}+t^{11}+t^{14}+t^{17}+t^{22}+t^{23}+t^{25}+t^{26}+t^{27}+t^{28}+t^{32}+t^{34}+t^{36}+t^{38}+t^{40})$, $\cdots\cdots\cdots\cdots$, $(1+t+t^2+t^6+t^7+t^8+t^9)(1+t+t^2+t^4+t^7+t^9+t^{10}+t^{11}+t^{14}+t^{17}+t^{22}+t^{23}+t^{25}+t^{26}+t^{27}+t^{28}+t^{32}+t^{34}+t^{36}+t^{38}+t^{40})$, $(1+t)(1+t+t^5+t^6+t^8)(1+t+t^2+t^4+t^7+t^9+t^{10}+t^{11}+t^{14}+t^{17}+t^{22}+t^{23}+t^{25}+t^{26}+t^{27}+t^{28}+t^{32}+t^{34}+t^{36}+t^{38}+t^{40})\}$.

最初の要素 c_{00} を除く全ての要素が，共通する因子 $1+t+t^2+t^4+t^7+t^9+t^{10}+t^{11}+t^{14}+t^{17}+t^{22}+t^{23}+t^{25}+t^{26}+t^{27}+t^{28}+t^{32}+t^{34}+t^{36}+t^{38}+t^{40}):=g(t)$ をもつことがわかる．(すなわち $f(t)$ を検出することができた). 実際の計算では，最初の要素以外から任意の 2 つの要素を選んで GCD を計算するだけでよい．最後に，$R(x,y,t)$ の $g(t)(=f(t))$ に関する正規形を計算して平文 $m(t)$ を得る.

5 全ての場合に適用可能なグレブナー基底を用いた攻撃法 (岩見 [10])

ここでは，新たなパラメータを導入し，グレブナー基底のテクニックを用いる．このアルゴリズムでは，有理関数体上の多項式環を経由することなく，体 $\mathbb{F}_p$ 上の多項式環で計算することができる.

系 5 (Corollary2 in pp.80 in [7])
Let $G=\{g_1,\cdots,g_t\}$ be a Gröbner basis for an ideal $I\subset k[x_1,\cdots,x_n]$ and let $f\in k[x_1,\cdots,x_n]$. Then $f\in I$ if and only if the normalform of the reduction of f by G is zero.

アルゴリズム 3 (グレブナー基底を利用した多項式環での攻撃法)

入力 : 秋山-後藤代数曲面公開鍵暗号の公開鍵 $X(x,y,t) \in \mathbb{F}_p[x,y,t]$,
暗号文 $F(x,y,t) \in \mathbb{F}_p[x,y,t]$.
出力 : 暗号文 $F(x,y,t)$ に対応する平文 m.

0. 新たなパラメータ $\mathcal{A}$ を導入し，イデアル $I_X := \langle \mathcal{A}\cdot X(x,y,t), \mathcal{A}\cdot \mathrm{LC}(X)-1\rangle \subset \mathbb{F}_p[x,y,t,\mathcal{A}]$ のグレブナー基底 GB_X を，$\mathbb{F}_p[x,y,t,\mathcal{A}]$ で，変数順序 $x \succ y \succ \mathcal{A} \succ t$ で計算する.

1. $F(x,y,t)$ の GB_X に関する正規形 $R(x,y,t,\mathcal{A}) \in \mathbb{F}_p[x,y,t,\mathcal{A}]$ を計算する.

2. $R(x,y,t,\mathcal{A})$ の項のうち，$c_{ij}(t,\mathcal{A})x^iy^j$ $((i,j)\neq(0,0))$ の形をしたもので，$c_{ij}(t,\mathcal{A})$ が $\mathbb{F}_p$ の要素でないものをランダムに選び，$c_{ij}(t,\mathcal{A})$ を C とする.

3. C の各項を，$\mathcal{A}\cdot\mathrm{LC}(X)=1$ であることを用いて，$\mathcal{A}^0 \mapsto (\mathcal{A}\cdot\mathrm{LC}(X))^2 = \mathcal{A}^2\cdot\mathrm{LC}(X)^2, \mathcal{A}^1 \mapsto \mathcal{A}(\mathcal{A}\cdot\mathrm{LC}(X))^1 = \mathcal{A}^2\cdot\mathrm{LC}(X), \cdots$, と変換し，$C$ の各項の $\mathcal{A}$ のべきが等しくなるようにして，$\mathcal{A}$ のべきをくくり出す．そして $\mathbb{F}_p[t,\mathcal{A}]$ で因数分解し，t の次数が ℓ 以上の既約因子の集合を $\hat{G}$ とし，$g(t)\in\hat{G}$ なる要素を選び，イデアル $I_g := \langle g(t), \mathcal{A}\cdot\mathrm{LC}(X)-1\rangle \subset \mathbb{F}_p[t,\mathcal{A}]$ のグレブナー基底 GB_g を計算する．そして，$R(0,0,t,\mathcal{A})$ の GB_g に関する正規形 $n\in\mathbb{F}_p[t]$ を計算する.

4. 多項式 $n(t) = n_{k-1}t^{k-1}+\cdots+n_1t+n_0 \in \mathbb{F}_p[t]$ を計算し，$m = n_0||n_1||\cdots||n_{k-1}$ を出力して終了.

定理 6
アルゴリズム 3 の中で生成される多項式 $g(t)$ と $n(t)$ は，秋山-後藤代数曲面公開鍵暗号での暗号化/復号の際に用いられる多項式 $f(t)$，平文から得られる多項式 $m(t)$ にそれぞれ一致している．すなわち，出力された平文は正しいものである.

例 6
アルゴリズム 3 を，$\mathbb{F}_2[x,y,t,\mathcal{A}]$ で，変数順序 $x\succ y\succ\mathcal{A}\succ t$ で用いることで，暗号文 $F_B(x,y,t)$ から平文 m を求める．イデアル $I_X := \langle \mathcal{A}\cdot X(x,y,t), \mathcal{A}\cdot\mathrm{LC}(X)-1\rangle$ のグレブナー基底 GB_X を計算し，次を得る.
$\mathrm{GB}_X = \{1+\mathcal{A}t+\mathcal{A}t^2+\mathcal{A}t^5, 1+\mathcal{A}t+t^2+t^3+\mathcal{A}t^3+t^6+t^7+t^8+t^9+t^{12}+t^{13}+t^{14}+t^{15}+t^{17}+t^{19}+t^{22}+t^{23}+t^{24}+\mathcal{A}tx+\mathcal{A}t^3x+t^4x+t^5x+t^6x+t^7x+t^{11}x+t^{12}x+t^{13}x+t^{14}x+t^{15}x+t^{16}x+t^{19}x+t^{20}x+t^{21}x+t^{23}x+x^2+\mathcal{A}t^2x^2+x^3+\mathcal{A}t^2x^3+\mathcal{A}t^3x^3+\mathcal{A}t^4x^3+x^4+\mathcal{A}x^4+\mathcal{A}tx^4+\mathcal{A}t^4x^4+\mathcal{A}x^5+\mathcal{A}t^3x^5+\mathcal{A}y+\mathcal{A}t^2y+\mathcal{A}t^3xy+\mathcal{A}t^4xy+\mathcal{A}t^2x^2y+\mathcal{A}t^4x^2y+x^3y+\mathcal{A}x^3y+\mathcal{A}t^2x^3y+\mathcal{A}t^3x^3y+x^4y+\mathcal{A}tx^4y+\mathcal{A}t^2x^4y+\mathcal{A}t^3x^4y+\mathcal{A}t^4x^4y+\mathcal{A}tx^5y+\mathcal{A}t^2x^5y+\mathcal{A}t^3x^5y+\mathcal{A}t^4x^5y+\mathcal{A}y^2+\mathcal{A}t^3y^2+\mathcal{A}xy^2+\mathcal{A}txy^2+\mathcal{A}t^3xy^2+\mathcal{A}x^2y^2+\mathcal{A}tx^2y^2+\mathcal{A}t^2x^3y^2+\mathcal{A}t^4x^3y^2+\mathcal{A}x^4y^2+\mathcal{A}tx^4y^2+\mathcal{A}t^2x^4y^2+\mathcal{A}t^3x^4y^2+\mathcal{A}t^4x^4y^2+x^5y^2+\mathcal{A}tx^5y^2+\mathcal{A}t^2x^5y^2+\mathcal{A}t^4x^5y^2+\mathcal{A}y^3+\mathcal{A}t^2y^3+\mathcal{A}t^3y^3+xy^3+\mathcal{A}xy^3+\mathcal{A}t^2xy^3+\mathcal{A}t^3xy^3+x^2y^3+\mathcal{A}t^3x^2y^3+\mathcal{A}t^4x^2y^3+x^3y^3+\mathcal{A}x^3y^3+\mathcal{A}tx^3y^3+\mathcal{A}t^3x^3y^3+\mathcal{A}tx^4y^3+\mathcal{A}t^2x^4y^3+\mathcal{A}t^4x^4y^3+\mathcal{A}tx^5y^3+\mathcal{A}t^2x^5y^3+\mathcal{A}t^4x^5y^3+y^4+\mathcal{A}t^4y^4+\mathcal{A}xy^4+\mathcal{A}txy^4+\mathcal{A}t^2xy^4+\mathcal{A}t^3xy^4+\mathcal{A}t^4xy^4+\mathcal{A}x^2y^4+\mathcal{A}tx^2y^4+\mathcal{A}t^3x^2y^4+\mathcal{A}t^4x^2y^4+\mathcal{A}t^2x^3y^4+\mathcal{A}t^3x^3y^4+x^4y^4+\mathcal{A}x^4y^4+\mathcal{A}tx^4y^4+\mathcal{A}t^3x^4y^4+\mathcal{A}x^5y^4+\cdots\cdots+\mathcal{A}t^2xy^5+x^2y^5+\mathcal{A}x^2y^5+\mathcal{A}t^2x^2y^5+x^3y^5+\mathcal{A}x^3y^5+\mathcal{A}tx^3y^5+\mathcal{A}t^2x^3y^5\mathcal{A}x^4y^5+\mathcal{A}t^4x^4y^5+x^5y^5\}$
$F_B(x,y,t)$ の GB_X に関する正規形を計算し，$R(x,y,t,\mathcal{A}) = \sum c_{ij}(t,\mathcal{A})x^iy^j \in \mathbb{F}_2[x,y,t,\mathcal{A}]$ を得る.
$c_{ij}(t,\mathcal{A})x^iy^j$ から c_{00} 以外の項を 2 つ選び，$\mathcal{A}\cdot\mathrm{LT}=1$ を利用して $\mathcal{A}$ のべきをくくり出してから，$\{c_{ij}(t,\mathcal{A})\}$ の GCD を計算する．例えば，$1+t+t^2+\mathcal{A}t^2+t^3+\mathcal{A}^2t^3+t^6+t^9+t^{11}+t^{12}+t^{14}+t^{18}+t^{20}+t^{27}+t^{28}+t^{34}+t^{40}$ であれば，$\mathcal{A}^2$ をくくり出すために，$\mathcal{A}^0\to(\mathcal{A}\cdot\mathrm{LC})^2 = \mathcal{A}^2\cdot\mathrm{LC}^2$, $\mathcal{A}^1\to\mathcal{A}(\mathcal{A}\cdot\mathrm{LC})^1 = \mathcal{A}^2\cdot\mathrm{LC}$ を用いて変換することで，$\mathcal{A}^2(t^2(1+t^3+t^4)^2(1+t+t^2+t^4+t^7+t^9+t^{10}+t^{11}+t^{14}+t^{17}+t^{22}+t^{23}+t^{25}+t^{26}+t^{27}+t^{28}+t^{32}+t^{34}+t^{36}+t^{38}+t^{40})$ を得る．そして，最大次数をもつ因子として $f(t)$ を検出する．最後に，$R(0,0,t,\mathcal{A})$ の GB_f に関する正規形を次のように計算する.

$R(0,0,t,\mathcal{A}) = 1+\mathcal{A}+\mathcal{A}^2t+\mathcal{A}t^3+\mathcal{A}^2t^3+\mathcal{A}t^4+\mathcal{A}^2t^4+t^5+t^6+t^7+t^{13}+t^{15}+t^{16}+t^{18}+t^{19}+t^{22}+t^{23}+t^{25}+t^{30}+t^{33}+t^{34}+t^{37}+t^{40}+t^{41}+t^{44}+t^{46}+t^{58}+t^{60}+t^{62}+t^{63}+t^{64}$, $\mathrm{GB}_f = \{1+t+t^2+t^4+t^7+t^9+t^{10}+t^{11}+t^{14}+t^{17}+t^{22}+t^{23}+t^{25}+t^{26}+t^{27}+t^{28}+t^{32}+t^{34}+t^{36}+t^{38}+t^{40}, A+t+t^2+t^5+t^6+t^7+t^8+t^{10}+t^{12}+t^{13}+t^{15}+t^{16}+t^{18}+t^{21}+t^{27}+t^{30}+t^{32}+t^{33}+t^{34}+t^{39}\}$,
$R(0,0,t,\mathcal{A}) \underset{\mathrm{GB}_f}{\longrightarrow} m(t)$ (平文を得ることができる)

6 脆弱性のない代数曲面公開鍵暗号にむけて
— 全ての場合に適用可能な代数曲面の零点を利用した攻撃法 —

上述の攻撃手法に対して脆弱性のない代数曲面公開鍵暗号にむけて，暗号文の構成方法について再考する．ここで，$F(x,y,t)$ の $X(x,y,t)$ に関する正規形を $R_1(x,y,t)$, $s(x,y,t)$ の $X(x,y,t)$ に関する正規形を $R_2(x,y,t)$ とすると，$F = G_1X + R_1$, $s = G_2X + R_2$, (G_1, G_2, R_1, R_2 は一意的) とかけるため，次のように計算できる．

$$\begin{aligned} F(x,y,t) &= m(t) + f(t)s(x,y,t) + X(x,y,t)r(x,y,t) \\ &= m(t) + f(t)\left(G_2(x,y,t)X(x,y,t) + R_2(x,y,t)\right) + X(x,y,t)r(x,y,t) \\ &= m(t) + f(t)R_2(x,y,t) + X(x,y,t)\left(f(t)G_2(x,y,t) + r(x,y,t)\right) \end{aligned}$$

$F(t)[x,y]$ (あるいは $F[x,y,t,\mathcal{A}]$) で簡約できないようにするためには，あるいは $f(t)$ の検出を失敗させるためには，どのようにすればよいのだろうか．大筋をかえない方針で，暗号文の構成法を少し変形して作ることができないか，いろいろと試してみたが，簡約して攻撃されないようにすると復号できなくなり，復号できるようにすると簡約して攻撃できなくなる等，うまくいかない．

そこで，次のような違った視点で考える．まず，公開鍵である代数曲面 $X(x,y,t) = 0$ に対して，主変数 x に関する根を 2 つ求める．一般ヘンゼル構成，拡張ヘンゼル構成等を用いれば，どのような場合でも，$X(x,y,t) = 0$ から $\prod_{i=1}^{d}(x-\eta_i(y,t)) = 0$ なる x に関する根 $\eta_i(y,t)(i = 1,\cdots,d$, ここで d は $X(x,y,t)$ の x の次数) を求めることができることに注意されたい．ここで，一般性を失うことなく，異なる 2 つの x に関する根を $\eta_1(y,t)$, $\eta_2(y,t)$ とし，暗号文 $F(x,y,t)$ に $X(x,y,t) = 0$ の異なる零点である $(\eta_1(y,t),y,t)$ と $(\eta_2(y,t),y,t)$ を代入し，次を得る．

$$\begin{aligned} F(\eta_1(y,t),y,t) &= m(t) + f(t)p(\eta_1(y,t),y,t) + X(\eta_1(y,t),y,t)q(x,y,t) \\ F(\eta_2(y,t),y,t) &= m(t) + f(t)p(\eta_2(y,t),y,t) + X(\eta_2(y,t),y,t)q(x,y,t) \end{aligned}$$

ここで，第 1 式右辺から第 2 式右辺を引くと，$m(t)$ はキャンセルし，$X(\eta_1(y,t),y,t)$ と $X(\eta_1(y,t),y,t)$ は高次項以外ゼロとなるため，適当な次数で高次項を打ち切ることで，

$$f(t)\left(p(\eta_1(y,t),y,t) - p(\eta_2(y,t),y,t)\right)$$

が残り，これを因数分解することで，$f(t)$ を検出することができる．$f(t)$ が検出できれば，$m(t)$ も計算することができる．

つまり，脆弱性のない代数曲面公開鍵暗号をつくる上で，簡約されてしまうことが問題というよりは，むしろ，代数曲面を利用している特性上，$X(x,y,t)$ に x に関する根を計算し

を代入すると消えてしまうため，ランダムな多項式を併用して平文 $m(t)$ を隠して伝送したとしても，2 つの曲線を代入して復号する方法とあわせている限り，攻撃者も同様の式を得ることが可能であるということが，問題の核心であることがわかる．

7 まとめ

秋山-後藤代数曲面公開鍵暗号に対する内山-徳永の攻撃手法とは，公開鍵がある条件を満たすとき，公開鍵と暗号文から，$\mathbb{F}_p[x,y,t]$ での簡約を利用して平文を得ることができるというものであった．筆者はそれを，$\mathbb{F}_p(t)[x,y]$ で行なうことができるように拡張することで，任意の公開鍵に対して適用可能な攻撃手法を提案していたが，さらに，新たなパラメータ $\mathcal{A}$ を導入してグレブナー基底を用いることで，任意の公開鍵に対して適用可能な，$\mathbb{F}_p[x,y,t,\mathcal{A}]$ での攻撃手法を提案した．証明等の詳細は，[9] を参照されたい．

よって，今後，脆弱性のない新しい代数曲面公開鍵暗号の提案が必要である．本稿では，これまでの簡約を利用した攻撃法の他に，代数曲面の零点（必ず計算することが可能）を利用した攻撃法も存在することを述べ，そのことから，大筋をかえない方向のままでは，安全な新しい代数曲面公開暗号の提案は難しく，発想を変える必要があることを述べた．

今後，その背景にある，もう少し歴史のある多次多変数公開鍵暗号やHFEの進化の歴史，それらを強化する持ち駒行列について，そこで多変数がどのように扱われてきたのかを調査した上で，再挑戦したい．

参 考 文 献

[1] A. Akiyama, Y. Goto : A Construction of an Algebraic Surface Public-key Cryptosystem. CD-ROM 2E4-3, pp.925-930 Symposium on Cryptography and Information Security (SCIS2005) January 2005.

[2] Algebraic surface public key cryptosystem, opened to the general public at website, February 2005 : About Toshiba > Technologies > Corporate Research & Development Center > Research and Development > Research News
http://www.toshiba.co.jp/rdc/rd/topics_e_05.htm#050206
http://www.toshiba.co.jp/rdc/rd/detail_j/0502_06.htm

[3] A. Akiyama, Y. Goto : A Security Analysis for a Public-key Cryptosystem using Algebraic Surfaces. CD-ROM 2A3-1, Symposium on Cryptography and Information Security (SCIS2006) January 2006.

[4] K. Akiyama, Y. Goto : A Public-key Cryptosystem using Algebraic Surfaces. Workshop Record of the International Workshop on Post-Quantum Cryptography (PQCrypto2006), pp.119-138, May 2006.

[5] S. Uchiyama, H. Tokunaga : 代数曲面を用いた公開鍵暗号の安全性について．CD-ROM 2C1-2, Symposium on Cryptography and Information Security (SCIS2007), January 2007.

[6] Cryptography Research and Evaluation Committees(CRYPTREC) : CRYPTREC Report 2006; Report of the Cryptographic Technique Monitoring Subcommittee, March 2007.
http://www.ipa.go.jp/security/enc/CRYPTREC/fy18/documents/c06_wat_final.pdf
Appendix3, "list of papers" (3)algorithm of public-key cryptosystem pp.87-88

[7] D. Cox, J. Little and D. O'Shea: Ideals, Varieties, and Algoriths: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Second Edition, Springer-Verlag.

[8] 岩見 真希：代数曲面公開鍵暗号に対する簡約を利用した攻撃法．京都大学数理解析研究所講究録 1572, pp.114-123, 2007年11月.

[9] M. Iwami : A Reduction Attack on Algebraic Surface Public-Key Cryptosystems. CD-ROM pp.214-221 (ポスター発表の論文版), The Asian Symposium on Computer Mathematics (ASCM) 2007, December 2007. 後に，LNAI Proc. of the ASCM 2007, Volume No. 5081, Springer に受理され掲載決定.

[10] 岩見真希：秋山-後藤代数曲面公開鍵暗号に対するグレブナー基底を用いた攻撃法の提案．大阪経済法科大学総合科学研究所年報第27号，pp.93-103，2008年3月.