数理解析研究所講究録
第 1759 巻 2011 年 105-114

An improvement of Voloch's rational point attack on improved algebraic surface cryptosystem

岩見 真希
MAKI IWAMI
大阪経済法科大学
OSAKA UNIVERSITY OF ECONOMICS AND LAW *

Abstract

There are trials to attack on improved algebraic surface cryptosystem (ASC07) such as rational point attack by Voloch and substitution of series solution by Iwami, but they are not effective because a certain polynomial have too many candidates and cannot be determined uniquely in the realistic calculation. In this paper, we try to improve these attacks. The idea is that performing monomial reduction increases the number of the system of equations and it decreases the number of candidates of a certain polynomial. It can be reduced to the combinatorial optimization problem by lattice basis reduction. Unfortunately, after further investigation, it was found that we couldn't improve these attacks by the suggested algorithm because ASC07 has some conditional equations w.r.t. degrees in the public key and encryption step, and the restrictions prevent the suggested algorithm from increasing the number of the system of equations and decreasing the the number of candidates of a certain polynomial. However, we can say that the suggested algorithm in this paper would be useful if there weren't such a degree ristriction in ASC07. [1)]

1 Introduction

An improved algebraic surface cryptosystem (ASC07) [6] is a public key cryptosystem whose original version is an algebraic surface cryptosystem (ASC04) [1](See **section 2**). Ivanov and Voloch suggested the guideline of substitution attack briefly on ASC07 in [7], but the practical algorithm was not given. So, strategy of Voloch's rational point attack introduced in [6] is in **section 3.1**. After that the author suggested substitution of series solution attack in [9](See **section 3.2**), but it is no different than one obtained in Voloch's rational point attack in the sense that a certain polynomial have too many candidates and cannot be determined uniquely in the realistic calculation (See **section 3.3**).

In this paper, we try to improve these attacks. In the presentation, the author talked that performing monomial reduction increases the number of the system of equations and it decreases the number of candidates of a certain polynomial. It can be reduced to the combinatorial optimization problem by lattice basis reduction.

Unfortunately, after further investigation, the author realized that some conditional equations w.r.t. degrees in the public key and encryption step of ASC07 were missing. These restrictions prevent the suggested algorithm from increasing the number of the system of equations and decreasing the the number of candidates of a certain polynomial, therefore we cannot improve them.

However, we can say that the suggested algorithm in this paper would be useful if there weren't such a degree ristriction in ASC07 (See **section 4**).

*maki@keiho-u.ac.jp

1) A part of this work is supported by Grant-in-Aid for Young Scientists (B).

2 Improved Algebraic Surface Cryptosystem (ASC07)

[Key generation of ASC07]

1. Secret key
   $D : (x, y, t) = (u_x(t), u_y(t), t)$: a section of X

2. Public key

   (a) $X(x, y, t) = 0$: a defining equation of a surface X with fibration.

   (b) $m(x, y, t) = \sum_{(i,j)\in\Lambda_m} m_{ij}(t)x^i y^j$:form of a plaintext polynomial, $m_{ij}(t)$ is unknown except for its degree.

   (c) $f(x, y, t) = \sum_{(i,j)\in\Lambda_f} f_{ij}(t)x^i y^j$:form of a divisor polynomial. $f_{ij}(t)$ is unknown except for its degree.

   Here Λ_A denotes the set of exponents of nonzero $x^i y^j$ terms in $A(x, y, t)$. $m(x, y, t)$ and $f(x, y, t)$ are chosen so as to satisfying $\Lambda_m \subset \Lambda_f \Lambda_X$ where $\Lambda_A \Lambda_B = \{(i_a + i_b, j_a + j_b)|(i_a, j_a) \in \Lambda_A, (i_b, j_b) \in \Lambda_B\}$. The decryption process requires that these keys satisfy the following condition:
   $\deg_x X(x, y, t) < \deg_x m(x, y, t) < \deg_x f(x, y, t)$,
   $\deg_y X(x, y, t) < \deg_y m(x, y, t) < \deg_y f(x, y, t)$,
   $\deg_t X(x, y, t) < \deg_t m(x, y, t) < \deg_t f(x, y, t)$,
   and
   $(\deg_x m(x, y, t), \deg_y m(x, y, t), \deg_t m(x, y, t)) \in \Gamma_m$,
   $(\deg_x f(x, y, t), \deg_y f(x, y, t), \deg_t f(x, y, t)) \in \Gamma_f$,
   where $\Gamma_m = \{(i, j, k) \in \mathbb{N}^3 | c_{ijk} \neq 0\}$ denotes the set of exponents of nonzero $x^i y^j t^k$ terms in $m(x, y, t)$, so that $m(x, y, t) = \Sigma_{(i,j,k)\in\Gamma_m} c_{ijk} x^i y^j t^k$.

[Encryption of ASC07]
Let m be a plain text, and divide m into small blocks as $m = m_{00}|| \cdots ||m_{ij}|| \cdots ||m_{IJ}$ where $\forall(i, j) \in \Lambda_m$, $|m_{ij}| \leq (|p| - 1)(\deg m_{ij}(t) + 1)$. Further, write $\ell_{ij} := \deg m_{ij}(t)$ and divide m_{ij} into $\ell_{ij} + 1$ blocks each of which is of $(|p| - 1)$ bits: $m_{ij} = m_{ij0}||m_{ij1}|| \cdots ||m_{ij\ell_{ij}}$.

1. Embed m into a plain text polynomial as $m(x, y, t) = \sum_{(i,j)\in\Lambda_m} m_{ij}(t)x^i y^j$ where $m_{ij}(t)$ is given as $m_{ij}(t) = \sum_{k=0}^{\deg m_{ij}(t)} m_{ijk} t^k$

2. Choose a random divisor polynomial $f(x, y, t)$ in accordance with the condition of $f(x, y, t)$.

3. Choose a random polynomials $r_1(x, y, t)$ and $r_2(x, y, t)$ that have the same form as $f(x, y, t)$; i.e. they have $\Lambda_r = \Lambda_f$ and $\deg r_{ij}(t) = \deg f_{ij}(t)$ for $(i, j) \in \Lambda_f$ as polynomials in x and y over $k[t]$.

4. Choose a random polynomials $s_0(x, y, t)$ and $s_1(x, y, t)$ that have the same form as $X(x, y, t)$; i.e. they have $\Lambda_s = \Lambda_X$ and $\deg s_{ij}(t) = \deg c_{ij}(t)$ for $(i, j) \in \Lambda_X$ as polynomials in x and y over $k[t]$.

5. Construct the cipher polynomials by
   $F_1(x, y, t) = m(x, y, t) + f(x, y, t)s_1(x, y, t) + X(x, y, t)r_1(x, y, t)$,
   $F_2(x, y, t) = m(x, y, t) + f(x, y, t)s_2(x, y, t) + X(x, y, t)r_2(x, y, t)$.

[Decryption of ASC07] The section $D : (u_x(t), u_y(t), t)$ satisfies $X(u_x(t), u_y(t), t) = 0$ as they are on $X(x, y, t)$.

1. Substitute D into F_i ; $h_i(t) = F_i(u_x(t), u_y(t), t) = m(u_x(t), u_y(t), t) + f(u_x(t), u_y(t), t)s_i(u_x(t), u_y(t), t)$
2. Compute $h_1(t) - h_2(t) = f(u_x(t), u_y(t), t)\{s_1(u_x(t), u_y(t), t) - s_2(u_x(t), u_y(t), t)\}$.
3. Factorize $h_1(t) - h_2(t)$.
4. Find the factor $f(u_x(t), u_y(t), t)$ as a polynomial of the degree calculated from the form of $f(x, y, t)$ initially.
5. $h_1(t) \equiv m(u_x(t), u_y(t), t) \pmod{f(u_x(t), u_y(t), t)}$
6. Extract the coefficient $m_{ij}(t)$ from $m(x, y, t)$ by solving linear equations.
   Let $m(x, y, t) = \sum_{(i,j,k)\in\Gamma_m} m_{ijk}x^iy^jt^k$, where m_{ijk}'s are variables. Construct the linear equations by comparing the coefficients of t in $m(u_x(t), u_y(t), t) = \sum_{(i,j,k)\in\Gamma_m} m_{ijk}u_x(t)^iu_y(t)^jt^k$. The left-hand side is given in the step 5.
7. Extract m form $m_{ij}(t)$ and authenticate the MAC of m. We can make certain of the plaintext m, if MAC is authenticated, Otherwise, return step 4.

Note that the differences between ASC04 and ASC07 are as follows:

(1) Plain text and random polynomial are modified to be multivariate from $m(t)$ and $f(t)$ to $m(x, y, t)$ and $f(x, y, t)$.

(2) To avoid reduction attack, the order is modified to be $X(x, y, t) \prec m(x, y, t) \prec f(x, y, t)$ i.e. it becomes difficult to find $m(x, y, t)$ and $f(x, y, t)$ because they are reduced by $X(x, y, t)$ and lost their original form.

(3) To decrypt ciphertexts, two cipher polynomials $F_1(x, y, t), F_2(x, y, t)$ are given.

3 Strategy of Rational Point Attack and Substitution of Series Solution Attack

3.1 Rational Point Attack (by Voloch)

The algorithm of attack on ASC07 by rational point attack is as follows.

Algorithm 1 (rational point attack by Voloch)

1. *Let* $F(x, y, t) = F_1(x, y, t) - F_2(x, y, t)$ *i.e.*
   $F(x, y, t) = f(x, y, t)(s_1(x, y, t) - s_2(x, y, t)) + X(x, y, t)(r_1(x, y, t) - r_2(x, y, t))$.
2. *Let* $g(x, y, t) = f(x, y, t)(s_1(x, y, t) - s_2(x, y, t))$ *and write* $g(x, y, t) = \Sigma_{(i,j)\in\Gamma_g} g_{ijk}x^iy^jt^k$ *where* $\Gamma_g = \{(i, j, k) \in \mathbb{N}^3 | g_{ijk} \neq 0\}$ *denotes the set of exponents of nonzero* $x^iy^jt^k$ *terms in* $g(x, y, t)$.
3. *Find a large number of rational points* (x_ℓ, y_ℓ, t_ℓ) *on* $X(x, y, t) = 0$ *and substitute them into* $F(x, y, t)$ *to obtain a system of linear equations in* $g_{ijk} \in \mathbb{F}_p$: $g(x_\ell, y_\ell, t_\ell) = F(x_\ell, y_\ell, t_\ell)$ $(\ell = 1, \cdots, n)$.
4. *Solve this system for* g_{ijk} *and factor* $g(x, y, t)$ *to find* $f(x, y, t)$.

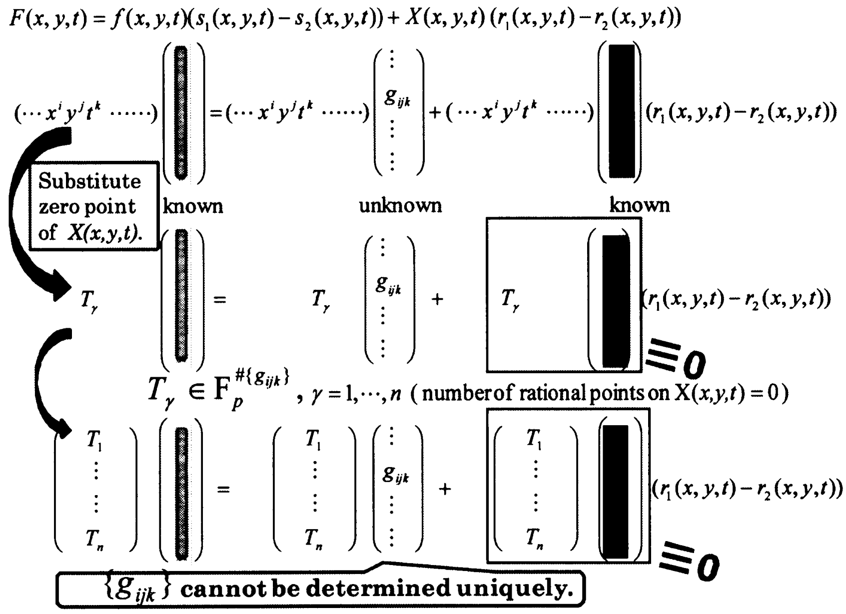

Figure 1: Voloch's rational point attack

5. *Finally, substitute rational points of* $X(x,y,t)=0$ *into*

$$F_1(x,y,t) = m(x,y,t) + f(x,y,t)s_1(x,y,t) + X(x,y,t)r_1(x,y,t)$$

to construct a system of linear equations in the coefficients of $m(x,y,t)$ *and* $s_1(x,y,t)$. *A solution to this system gives* $m(x,y,t)$.

Note that this attack requires many rational points on $X(x,y,t)=0$, which can be obtained by raising the field of definition for $X(x,y,t)=0$. But no matter how many rational points we use, the polynomial $g(x,y,t)$ (and so $f(x,y,t)$ and $m(x,y,t)$) cannot be determined uniquely.

3.2 Substitution of Series Solution Attack (by Iwami: Jssac2009)

The algorithm of attack on ASC07 by substitution of series solution is as follows.

Algorithm 2 (substitution of series solution attack by Iwami)

1. *Let* $F(x,y,t) = F_1(x,y,t) - F_2(x,y,t)$ *i.e.*
   $F(x,y,t) = f(x,y,t)(s_1(x,y,t) - s_2(x,y,t)) + X(x,y,t)(r_1(x,y,t) - r_2(x,y,t))$.

2. *Let* $g(x,y,t) = f(x,y,t)(s_1(x,y,t) - s_2(x,y,t))$ *and write*

$$g(x,y,t) = \Sigma_{(i,j)\in\Gamma_g} g_{ijk}x^iy^jt^k$$

   where $\{g_{ijk}\}$ *are unknown elements in* $\mathbb{F}_p$ *and* $\Gamma_g = \{(i,j,k)\in\mathbb{N}^3 | g_{ijk}\neq 0\}$ *denotes the set of exponents of nonzero* $x^iy^jt^k$ *terms in* $g(x,y,t)$.

3. *Calculate a series solution of* $X(x,y,t)=0$ *and let it be* $x=\eta(y,t)$. *Substitute it into* $F(x,y,t)$ *and let it be* $F(\eta(y,t),y,t) := \sum \widetilde{g_{\alpha\beta}}y^\alpha t^\beta$ *where* $\{\widetilde{g_{\alpha\beta}}\}$ *are known elements in* $\mathbb{F}_p$, *whereas,*

$$
\begin{aligned}
F(\eta(y,t),y,t) &= f(\eta(y,t),y,t)(s_1(\eta(y,t),y,t) - s_2(\eta(y,t),y,t)) \\
&\quad + X(\eta(y,t),y,t)(r_1(\eta(y,t),y,t) - r_2(\eta(y,t),y,t)) \\
&\equiv f(\eta(y,t),y,t)(s_1(\eta(y,t),y,t) - s_2(\eta(y,t),y,t)) \bmod S^e \\
&\equiv g(\eta(y,t),y,t) \bmod S^e \\
&\equiv \sum g_{ijk}\eta(y,t)^i y^j t^k \bmod S^e \\
&:= \textstyle\sum_{\alpha,\beta}(\sum_{(i,j,k)} \eta_{\alpha\beta ijk} g_{ijk}) y^\alpha t^\beta
\end{aligned}
$$

where S^e is a polynomial ideal as $X(\eta(y,t),y,t)$ becomes 0 by truncation, $\{\eta_{\alpha\beta ijk}\}$ are known elements in $\mathbb{F}_p$. Now we obtain the system of linear equations by comparing the coefficients w.r.t. $y^\alpha t^\beta$ as $\widetilde{g_{\alpha\beta}} = \sum_{(i,j,k)} \eta_{\alpha\beta ijk} g_{ijk}$.

4. *Solve this system for g_{ijk} and factor $g(x,y,t)$ to find $f(x,y,t)$.*

5. *Finally, substitute series solution of $X(x,y,t) = 0$ into*

$$F_1(x,y,t) = m(x,y,t) + f(x,y,t)s_1(x,y,t) + X(x,y,t)r_1(x,y,t)$$

to construct a system of linear equations in the coefficients of $m(x,y,t)$ and $s_1(x,y,t)$ w.r.t. $y^\alpha t^\beta$. A solution to this system gives $m(x,y,t)$. (As for this step, we may use **step 5** *in Voloch's rational point attack.)*

But $\{g_{ijk}\}$ cannot be determined uniquely because of the freedom of degree as is shown in Figure 2 and Figure 4. Note that we can also obtain more equations by raising the field of definition for $X(x,y,t) = 0$. But the polynomial $g(x,y,t)$ (and so $f(x,y,t)$ and $m(x,y,t)$) cannot be determined uniquely.

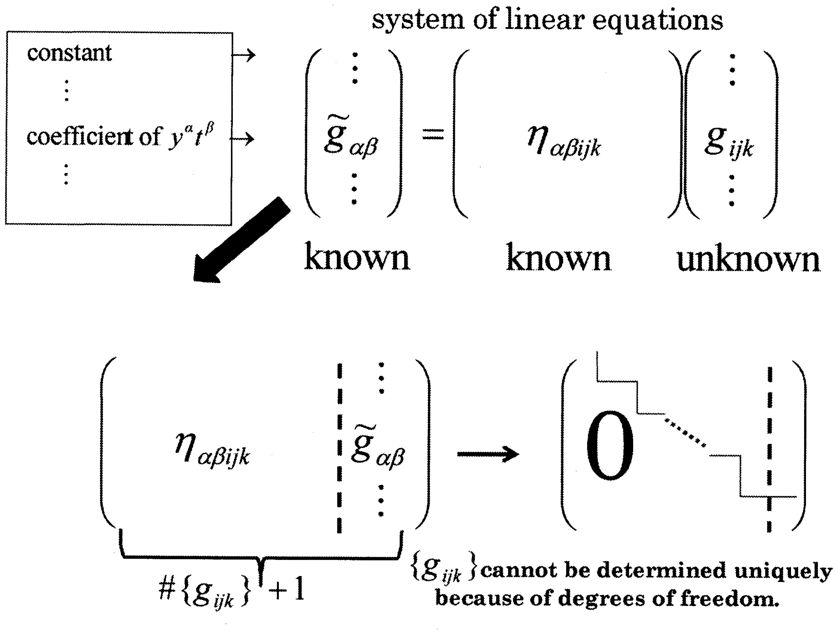

Figure 2: substitution of series solution attack

3.3 Comparison between Substitution of Series Solution Attack and Rational Point Attack

We compare two methods, i.e. substitution of "series solutions" by the author and "rational point" by Voloch with simple example as follows.

Example 1

characteristic : $p = 17$,
public-key : $X(x,y,t) = 12 + 5t + 7t^2 + 3t^4 + 7t^5 + 5t^6 + 13t^7 + 4xy + 7txy + 10x^2y + 3tx^2y$,
plain text polynomial : $m(x,y,t) = 11+3t+15t^2+2t^3+5t^4+10t^5+2t^6+2t^7+13t^8+(2+11t+12t^7)x^3y^2$,
randomly chosen polynomials :
$s_1 = (4t+2)x^2y + (9t+4)xy + 12t^7 + 14t^6 + 13t^3 + 14t + 4$,
$s_2 = (7t+11)x^2y + (3t+3)xy + 12t^7 + t^6 + 7t^5 + t^4 + 4t^3 + 2t + 1$,
$r_1 = (10t^9 + 8t^8 + 16t^6 + t^3 + 16t + 2)x^4y^3 + (14t^9 + 10t^8 + 13t^5 + 6t^4 + 10t^2 + 15)xy^2 + 8t^9 + 3t^8 + 3t^7 + 9t^3 + 7t^2 + t + 15$,
$r_2 = (4t^9 + 8t^8 + 13t^5 + 12t^4 + 4t + 16)x^4y^3 + (2t^9 + t^8 + 2t^6 + 4t^4 + 13t^3 + 2t + 8)xy^2 + 16t^9 + 4t^8 + 2t^7 + 3t^5 + 13t^3 + 8t + 16$,
$f(x,y,t) = (8t^9 + 11t^8 + 10t^7 + 7t^6 + 8t^5 + 16t^4 + 10t^3 + 12t^2 + 7t + 16)x^4y^3 + (16t^9 + 16t^8 + 2t^7 + 4t^6 + 4t^5 + 9t^4 + 9t^3 + t^2 + 7t + 14)xy^2 + 5t^9 + 14t + 11$ *where* $\deg(X(x,y,t)) < \deg(m(x,y,t)) < \deg(f(x,y,t))$.
cipher-text polynomials :
$F_1 = m(x,y,t) + f(x,y,t)s_1(x,y,t) + X(x,y,t)r_1(x,y,t)$,
$F_2 = m(x,y,t) + f(x,y,t)s_2(x,y,t) + X(x,y,t)r_2(x,y,t)$, *ideal* $S_k (k = 0, 1, \cdots 20)$.

Let $g(x,y,t) = \sum_{(ijk)x^iy^jt^k} x^iy^jt^k (= f(x,y,t)(s_1(x,y,t) - s_2(x,y,t)))$ *where* $\{g_{ijk}\}$ *are unknowns in* $\mathbb{F}_{17}$. *We can see that the number of nonzero terms of* $g(x,y,t)$ *is* $(\#g_{ijk} =)117$ *by the conditions of* Λ_f *and* $\Lambda_s (= \Lambda_X)$, *and the number of rational points of* $X(x,y,t) = 0$ *is 325 if we don't raise the field of definitions for* $X(x,y,t)$. *So we can construct the system of equations and obtain* rank $= 87$ *as is shown in Figure 3 and Figure 4. So, the dimension of the solution space is* $30 (= 117 - 87)$ *and the candidate of* $g(x,y,t)$ *is* $17^{30} (= p^{30})$ *therefore* $g(x,y,t)$ *cannot be determined uniquely.*

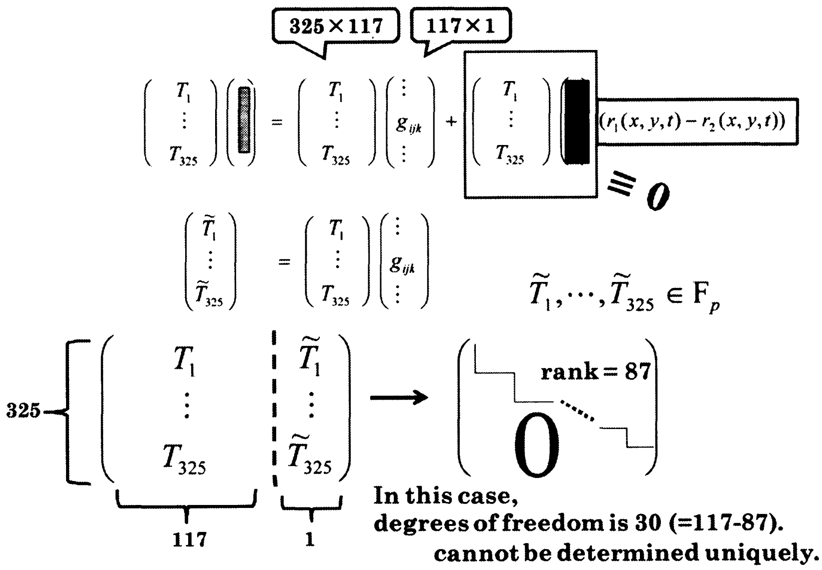

Figure 3: Example of Voloch's rational point attack

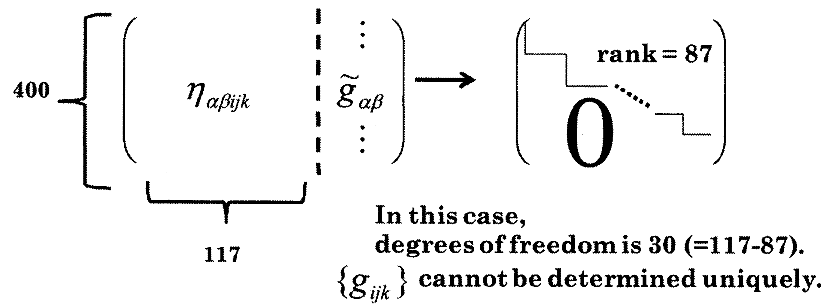

Figure 4: Example of substitution of series solutions attack

Note that we can obtain more equations by raising the field of definition for $X(x, y, t) = 0$, but both method result in the same situation.

4 Improvement

4.1 Algorithm for improvement

After performing Voloch's rational point attack (or Iwami's substitution of series solutions attack), we try to obtain more equations and decrease the candidate of the solution as follows.

Let $\vec{g}$ be a coefficient vector of $g(x, y, t)$ obtained by Voloch's rational point attack (step 4. in **Algorithm 1**) or Iwami's substitution of series solutions attack (step 4. in **Algorithm 2**)).Then we can express $\vec{g}$ as

$$\vec{g} = \vec{g_s} + \sum c_i \vec{b_i}$$

where c_i is an unknown element in $\mathbb{F}_p$, $\vec{g_s}$ is a general solution and $\{\vec{b_i}\}$ are fundamental solutions of $\vec{g}$. Let $\vec{F_1} - \vec{F_2}$ be a coefficient vector of $F_1 - F_2 (= g(x, y, t) + X(x, y, t)(r_1(x, y, t) - r_2(x, y, t)))$ then we can express $\vec{F_1} - \vec{F_2} - \vec{g}$ by performing monomial reduction as

$$\vec{F_1} - \vec{F_2} - \vec{g} = \Sigma d_i \overrightarrow{p_i X}$$

where d_i is unknown in $\mathbb{F}_p$, p_i is monomial and $\overrightarrow{p_i X}$ is a coefficient vector of $p_i X$. Therefore the problem results in combinatorial optimization problem calculating c_i and d_i satisfying

$$\vec{F_1} - \vec{F_2} = \vec{g_s} + \Sigma c_i \vec{b_i} + \Sigma d_i \overrightarrow{p_i X}.$$

Algorithm 3 (Calculation of c_i, d_i and $\vec{g}$ satisfying $\vec{g} = \vec{g_s} + \Sigma c_i \vec{b_i}$ and $\vec{F_1} - \vec{F_2} = \vec{g} + \Sigma d_i \overrightarrow{p_i X}$)

1. *Let $\vec{g}$ be a coefficient vector of $g(x, y, t)$ obtained by step 4. in* **Algorithm 1** *or step 4. in* **Algorithm 2**, *and express $\vec{g}$ as $\vec{g} = \vec{g_s} + \sum c_i \vec{b_i}$ where c_i is an unknown element in $\mathbb{F}_p$, $\vec{g_s}$ is a general solution and $\{\vec{b_i}\}$ are fundamental solutions of $\vec{g}$. And calculate $\vec{F_1} - \vec{F_2} - \vec{g_s}$.*

2. *Let $p_1, \cdots, p_r$ be monimials which are the support of $r_1(x, y, t) - r_2(x, y, t)$ calculated by the conditions of the public key. Then calculate coefficient vector of $p_i X$ and let it be $\overrightarrow{p_i X}$ $(i = 1, \cdots, r)$.*

3. *Construct the following matrix and calculate the reduced rattice basis where a is a scaling factor.*

$$\begin{array}{cc}
\left(\begin{array}{c|c}
\mathbf{E}_{1+v+r} & \begin{array}{c} a(\vec{F}_1-\vec{F}_2-\vec{g}_s) \\ \hline a\vec{b}_1 \\ \vdots \\ a\vec{b}_v \\ \hline a\,\overrightarrow{p_1X} \\ \vdots \\ a\,\overrightarrow{p_rX} \end{array} \\ \hline
\mathbf{0} & ap\mathbf{E}_{\#\{g_{ijk}\}}
\end{array}\right) &
\begin{array}{l} \}\ 1 \\ \}\ v \\ \}\ r \\ \}\ \#\{g_{ijk}\} \end{array} \\
\underbrace{\qquad\qquad\qquad}_{1+v+r}\ \underbrace{\qquad\qquad\qquad}_{\#\{g_{ijk}\}} &
\end{array}$$

Figure 5: The matrix for calculating reduced lattice basis.

4. *By the short vector, we obtain c_i, d_i satisfying*

$$\vec{F_1} - \vec{F_2} = \vec{g_s} + \Sigma c_i \vec{b_i} + \Sigma d_i \overrightarrow{p_i X},$$

and then we obtain

$$\vec{g} = \vec{g_s} + \Sigma c_i \vec{b_i}.$$

(proof) The problem is to obtain c_i and d_i satisfying $\vec{F_1} - \vec{F_2} - \vec{g_s} = \Sigma c_i \vec{b_i} + \Sigma d_i \overrightarrow{p_i X}$, so it is obvious from the theory of combinatorial optimization problem using lattice basis reduction.

4.2 Analysis

As is shown in the previous section, the strategy is to decrease the number of candidates of $g(x, y, t)$ by increasing the system of equations by monomial reduction which is reduced to a problem of combinatorial optimization problem using lattice basis reduction. In this section, we see a simple example of **Algorithm 3**, and analyze it.

Example 2 (Applying Algorithm 3 to Example 1)
In **Example 1**, *the number of candidates of $g(x, y, t)$ is 17^{30}. Here, we try to decrease it by applying* **Algorithm 3** *to* **Example 1**. *We construct the following matrix (***Figure 6***) and calculate the reduced rattice basis with scaling factor $a = 10^7$.*
The rank of the matrix is 31 i.e. the number of unknown c_i and d_i satisfying $\vec{F_1} - \vec{F_2} = \vec{g_s} + \Sigma c_i \vec{b_i} + \Sigma d_i \overrightarrow{p_i X}$ is 30, therefore the number of candidates of $g(x, y, t)$ is 17^{30} which is the same result obtained in **Example 1**.

In the presentation, some conditional equations w.r.t. degrees between r_1, r_2 and $f(x, y, t)$, s_1, s_2 and $X(x, y, t)$ in the public key and encryption step of ASC07 were missing, and it allowed us to success in

$$
\begin{array}{cc}
\left(\begin{array}{c|c}
\mathbf{E}_{61} & \begin{array}{c} 10^7\,(\vec{F}_1-\vec{F}_2-\vec{g}_s) \\ \hline 10^7\,\vec{b}_1 \\ \vdots \\ 10^7\,\vec{b}_{30} \\ \hline 10^7\,\overrightarrow{p_1X} \\ \vdots \\ 10^7\,\overrightarrow{p_{30}X} \end{array} \\ \hline
\mathbf{0} & 10^7\times 17\times \mathbf{E}_{117}
\end{array}\right)
&
\begin{array}{l} \}\,1 \\ \}\,30 \\ \}\,30 \\ \}\,117 \end{array} \\
\begin{array}{cc} \underbrace{\qquad\qquad}_{61} & \underbrace{\qquad\qquad}_{117} \end{array} &
\end{array}
$$

Figure 6: Example of the matrix for calculating reduced lattice basis.

improvement. However, as is shown in the above example, ASC07 has the degree condition, so we cannot improve them. We can see the details in the following theorems and their proofs.

Theorem 1
As for $\vec{F_1} - \vec{F_2} = \vec{g_s} + \Sigma_{i=1}^{v} c_i \vec{b_i} + \Sigma_{i=1}^{r} d_i \overrightarrow{p_i X}$ *in* **Algorithm 3**, *the equation* $v = r$ *holds true.*

(proof) v is the dimension of the solution space of $g(x, y, t)$ obtained by **Algorithm 1** or **Algorithm 2**, and the number of candidates of $g(x, y, t)$ is p^v. r is the number of monomials of $r_1(x, y, t) - r_2(x, y, t)$ estimated by the condition of $f(x, y, t)$ because $f(x, y, t)(= \Sigma_{(i,j)\in\Lambda_f} f_{ij}(t)x^i y^j)$ is unknown but Λ_f and $\deg_t f_{ij}(t)$ is opened as a part of the public key, and by the encryption algorithm, we know that $\Lambda_f = \Lambda_r$ and $\deg r_{ij}(t) = \deg f_{ij}(t)$ for $(i, j) \in \Lambda_f$ as polynomials in x and y over $k[t]$. Moreover, $\Lambda_X = \Lambda_s$ and $\deg X_{ij}(t) = \deg s_{ij}(t)$ for $(i, j) \in \Lambda_X$ as polynomials in x and y over $k[t]$, and $F_1 - F_2 = f(s_1 - s_2) + X(r_1 - r_2) = g + X(r_1 - r_2) = g_s + \Sigma_{i=i}^{v} c_i b_i + X(r_1 - r_2)$. Now the number of candidates of $r_1 - r_2$ is p^r, then the number of candidates of $g(= g_s + \Sigma_{i=i}^{v} c_i b_i)$ is also p^r, therefore we obtain $v = r$.

Theorem 2
The rank of the matrix for calculating reduced lattice basis in Figure 5 *is* $1 + v$, *therefore, the dimension of the solution space of* $g(x, y, t)$ *still remains* v.

(proof) As we can see in the proof of **Theorem 4.2**, from some conditions in the public key and encryption algorithm, the number of candidates of $r_1 - r_2$ *i.e.* the number of monomials $p_1, \cdots, p_r$ is equals to the dimension of the solution space of $g(x, y, t)$. Therefore, the rank of the matrix becomes $1 + v(= 1 + r)$.

From **Theorem 2**, the number of candidates of $g(x, y, t)$ doesn't decrease and still remains p^v, *i.e.* the trial of the improvement of **Algorithm 1** and **Algorithm 2** failed.

5 Conclusion

In the presentation, the author talked that performing monomial reduction increases the number of the system of equations and it decreases the dimension of the solution space of $g(x, y, t)$. But after further investigation, the author realized that some conditional equations w.r.t. degrees in the public key and encryption step of ASC07 were missing. These restrictions keep the supports of $f(s_1 - s_2)$ and $X(r_1 - r_2)$ in the same form, and prevent the suggested algorithm from increasing the number of the system of equations and decreasing the the number of candidates of a certain polynomial, therefore the result of the suggested method is the same as Voloch's method.

Assume that there weren't such a degree ristriction in ASC07 then increasing the degrees and the number of terms seem to make it more complicated and secure, but we can say that the suggested algorithm (**Algorithm 2**) in this paper would be useful.

References

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

[2] S. Uchiyama, H. Tokunaga : On the Security of the Algebraic Surface Public-Key Cryptosystems, *Symposium on Cryptography and Information Security (SCIS2007)*, January 2007, CD-ROM 2C1-2.

[3] M. Iwami: A Reduction Attack on Algebraic Surface Public-Key Cryptosystems, *Workshop of Research Institute for Mathematical Sciences Kyoto University, New development of research on Computer Algebra, RIMS Kokyuroku* **1572**, November 2007, 114–123.

[4] M. Iwami : A Reduction Attack on Algebraic Surface Public-Key Cryptosystems, *Computer Mathematics, 8th Asian Symposium, ASCM 2007, Singapore, December 15-17, 2007, Revised and Invited Papers*, LNAI **5081**, Springer, 2008, 323–332.

[5] M Iwami : A Proposal for an Attack on Akiyama-Goto Algebraic Surface Public-Key Cryptosystems Utilizing Gröbner Bases, *Osaka Annals of the General Sciences Institute, Osaka University of Economics and Law* **27**, March 2008, 93–103.

[6] K. Akiyama, Y. Goto, H. Miyake : An algebraic Surface Cryptosystem, *Public Key Cryptography -PKC2009*, LNCS **5443**, Springer, 2009, 425–442.

[7] P. Ivanov and J. F. Voloch : Breaking the Akiyama-Goto cryptosystem, *preprint (opened on the Internet)*.

[8] M Iwami : Breaking the Improved Akiyama-Goto Algebraic Surface Public-key Cryptosystem, *Journal of the Japan Society for Symbolic and Algebraic Computation* Vol.15, No.2, pp.124-127, December 2008.

[9] M Iwami : Series Solution and Cryptography, *Journal of the Japan Society for Symbolic and Algebraic Computation* Vol.16, No.2, pp.127-130, December 2009.