Computer Algebra Techniques in the Development of Public-Key Cryptosystems using Multivariate Polynomials

Maki IWAMI
Osaka University of Economics and Law, Japan
maki@keiho-u.ac.jp

Abstract. In this paper, we give a brief survey of multivariate public-key cryptography (MPKC) whose security depends on the difficulty of solving a set of multivariate polynomial equations, focusing attention on the interactions between MPKC and computer algebra techniques which cause the improvement of their algorithms and various types of cryptosystems. Especially, we survey interactions between the development of algebraic surface cryptosystem and various trials to attack using computer algebra techniques such as reduction, application of Gröbner basis, reduced lattice basis, parametrization, substitution of series solutions or rational points, and ideal decomposition.

1 Introduction

Public-key cryptography is wildely used nowadays, but once a quantum computer is available, RSA, ElGamal and elliptic curve cryptography become insecure because there are polynomial time algorithms for integer factorization and discrete logarithm problems for a quantum computer. Therefore, multivariate cryptography, lattice-based cryptography and code-based cryptography whose security depend on the difficulty of solving other mathematical problems (NP-hard) have received attention as a post-quantum cryptography. In this paper, we focus attention on multivariate public-key cryptography (MPKC) whose security depends on the difficulty of solving a set of multivariate polynomial equations.

There are many MPKCs such as Matsumoto-Imai cryptosystem (MI), the Hidden Field Equations cryptosystem (HFE), the Oil-Vineger signature scheme, the Tamed Transformation Method cryptosystem (TTM), cryptosystem derived from internal perturbation, moon letter cryptosystem, Random Simultaneous Equations of degree 2 PKC (RSE(2)PKC), piece in hand matrix, Algebraic Surface Cryptosystem (ASC), etc. Then, the computer algebra techniques are essential to the development of the cryptosystems and several major mothods have been developed to attack on them such as Gröbner basis mothod, its improvements (F_4, F_5), the differential attack, etc.

In section 2, we see a brief survey of multivariate public-key cryptosystems. And in section 3, we see interactions between algebraic surface public-key cryptosystems and various types of computer algebra techniques.

2 A Brief Survey of Multivariate Public-Key Cryptosystems

2.1 Matsumoto-Imai Cryptosystem

In this subsection, we see a brief survey of Matsumoto-Imai Cryptosystem (MI) [18] which was proposed by Matsumoto and Imai in 1988, and a related attack.

Let k be a finite field of characteristic two and cardinality q, and take $g(x) \in k[x]$ to be any irreducible polynomial of degree n. Define the field $K = k[x]/g(x)$, a degree n extension of k.

Let $\Phi : K \longrightarrow k^n$ be the standard k-linear isomorphism between K and k^n given by

$$\Phi(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) = (a_0, a_1, \cdots, a_{n-1}).$$

The subfield k of K is embedded in k^n by $\Phi(a) = (a, 0, \cdots, 0), \forall a \in k$.

Note that here Φ is a k-linear map if we treat k as a subfield in K.

Choose θ so that $0 < \theta < n$ and gcd $(q^\theta + 1, q^\theta - 1) = 1$, and define the map $\widetilde{F}$ over K by $\widetilde{F} = X^{1+q^\theta}$. The conditions on θ insure that $\widetilde{F}$ is an invertible

map; indeed, if t is an integer such that $t(1+q^\theta) \equiv 1 \bmod (q^n-1)$, then $\widetilde{F}^{-1}$ is simply $\widetilde{F}^{-1}(X) = X^t$.

Now let F be the map over k^n defined by

$$F(x_1, \cdots, x_n) = \Phi \circ \widetilde{F} \circ \Phi^{-1}(x_1, \cdots, x_n) = (f_1, \cdots, f_n),$$

where $f_1, \cdots, f_n \in k[x_1, \cdots, x_n]$. And define the map over k^n by

$$\overline{F}(x_1, \cdots, x_n) = L_1 \circ F \circ L_2(x_1, \cdots, x_n) = (\overline{f_1}, \cdots, \overline{f_n}),$$

where L_1 and L_2 be two invertible transformations over k^n, and $\overline{f_1}, \cdots, \overline{f_n} \in k[x_1, \cdots, x_n]$. See Fig.1.

Public-key : The field k and degree 2 polynomials $\overline{f_1}, \cdots, \overline{f_n} \in k[x_1, \cdots, x_n]$

Private-key : Two invertible affine transformations L_1 and L_2.
(θ can be kept private, but it is not critical.)

Encryption : Given a plaintext message $(x_1', \cdots, x_n')$,
the associated ciphertext is $(y_1', \cdots, y_n')$,
where $y_i' = \overline{f_i}(x_1', \cdots, x_n')$ for $i = 1, \cdots, n$.

Decryption : We can decrypt the ciphertext $(y_1', \cdots, y_n')$ by computing

$$\begin{aligned}
\overline{F}^{-1}(y_1', \cdots, y_n') &= L_2^{-1} \circ F^{-1} \circ L_1^{-1}(y_1', \cdots, y_n') \\
&= L_2^{-1} \circ \Phi \circ \widetilde{F}^{-1} \circ \Phi^{-1} \circ L_1^{-1}(y_1', \cdots, y_n') \\
&= L_2^{-1} \circ \Phi \circ \widetilde{F}^{-1} \circ \Phi^{-1}(z_1', \cdots, z_n') \\
&= L_2^{-1}(\overline{z}_1, \cdots, \overline{z}_n) \\
&= (x_1', \cdots, x_n')
\end{aligned}$$

Moreover, a multi-branch MI is composed of (single-branch) MI as described above. For detail, see [16, 18].

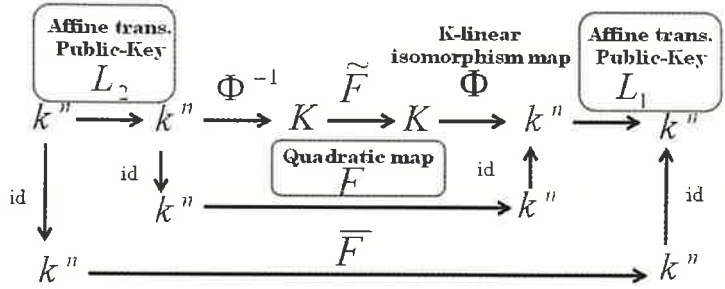

Fig. 1. Composition of maps in the construction of MI.

2.2 Attack on Matsumoto-Imai Cryptosystem

Patarin attacked MI by algebraic attack via linearization equations in 1955 [19]. The linearization equations are constructed as follows. Let $X, Y \in K$ s.t. $Y = \widetilde{F}(X) = X^{q^\theta+1}$, then we have $Y^{q^\theta-1} = (X^{q^\theta+1})^{q^\theta-1} = X^{q^{2\theta}-1}$. If we multiply both sides by XY and move right-hand side to left, we have $XY^{q^\theta} - X^{q^{2\theta}}Y = 0$. Define $\widetilde{R}(X,Y) = XY^{q^\theta} - X^{q^{2\theta}}Y \in K[X,Y]$ and $R = \Phi \circ \widetilde{R} \circ (\Phi^{-1} \times \Phi^{-1})$. The n components of $R(x_1, \cdots, x_n, y_1, \cdots, y_n)$ are of the form $\sum_{i=1}^n \sum_{j=1}^n a_{ij}x_iy_j + \sum_{i=1}^n b_ix_i + \sum_{j=1}^n c_jy_j + d$, then we obtain n linearization equations as

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_if_j + \sum_{i=1}^{n} b_ix_i + \sum_{j=1}^{n} c_jf_j + d = 0.$$

Actually, to solve linear equations, one of the ways is to substitute plaintext-ciphertext pairs which can be generated using public-key. And the linearization attack can also be applied to the multiple-branch MI.

2.3 Others

Even though the MI system was broken, various types of cryptosystems have been proposed to avoid the system's weakness, such as the Hidden Field Equations cryptosystem (HFE), the Oil-Vineger signature scheme, the Tamed Transformation Method cryptosystem (TTM), cryptosystem derived

from internal perturbation, moon letter cryptosystem, Random Simultaneous Equations of degree 2 PKC (RSE(2)PKC), piece in hand matrix, Algebraic Surface Cryptosystem (ASC), etc. Then, the computer algebra techniques are essential to the development of the cryptosystems.

In the next section, we see the interaction of development of algebraic surface public-key cryptosystem and attacks with computer algebra techniques.

3 Computer Algebra Techniques in the Development of Algebraic Surface Public-Key Cryptosystems

3.1 Algebraic Surface Public-Key Cryptosystems (ASC06)

Akiyama and Goto suggested algebraic surface public-key cryptosystems (ASC06, [1, 2, 3]) whose public-key is the defining equations of an algebraic surface, and secret-key is the algebraic curves on it.

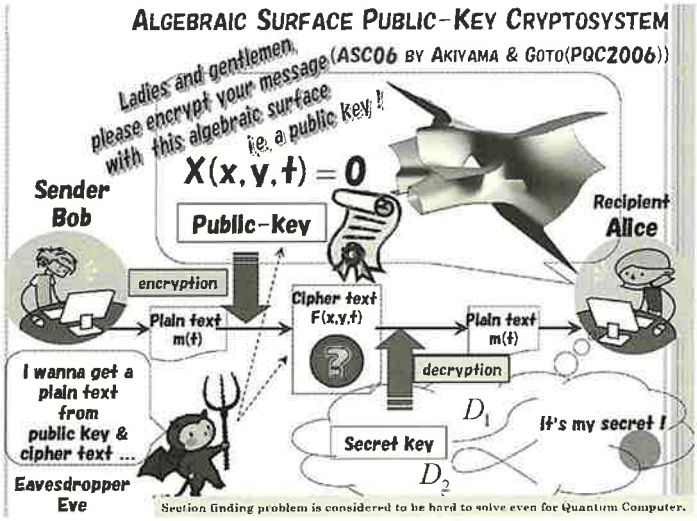

Fig. 2. algebraic surface cryptosystem

[Key generation of ASC06]

Secret key: Choose two distinct curves of the form $D_1 : (x, y, t) = (u_x(t), u_y(t), t)$, $D_2 : (x, y, t) = (v_x(t), v_y(t), t)$ satisfying $\deg u_x(t) \neq \deg v_x(t)$ or $\deg u_y(t) \neq \deg v_y(t)$ for the uniqueness of decryption, and satisfying $(u_x(t) - v_x(t))|(u_y(t) - v_y(t))$ for $c_{10}(t) \in \mathbb{F}_p[t]$ (not $\mathbb{F}_p(t)$) in step (a) in Pulic-key generation.

Public key:

(a) Construct algebraic surface (public key) $X(x, y, t) = \sum_{i,j} c_{ij}(t)x^i y^j = 0$ over $\mathbb{F}_p$ containing two curves (secret key), i.e. it satisfies $X(u_x(t), u_y(t), t) = X(v_x(t), v_y(t), t) = 0$. First, ramdomly choose $c_{ij}(t)$ with $(i, j) \neq (0, 0), (1, 0)$ and then calculate $c_{10}(t)$ and $c_{00}(t) \in \mathbb{F}_p(t)$ as follows.

$c_{10}(t) := -\sum_{(i,j)\neq(0,0),(1,0)} c_{i,j}(t)\{u_x(t)^i u_y(t)^j - v_x(t)^i v_y(t)^j\}/(u_x(t) - v_x(t))$

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

(b) Choose $\ell \in \mathbb{N}$ as a lower bound for the degree of a monic irreducible polynomial $f(t) \in \mathbb{F}_p[t]$ chosen in the encryption step. For reasons of security (see 5.3 in [3]), we impose $\deg_t X(x, y, t) < \ell$.

(c) Choose $d \in \mathbb{N}$ satisfying $d \geq \max\{\deg u_x(t), \deg u_y(t), \deg v_x(t), \deg v_y(t)\}$.

By taking a large ℓ or d, the characteristic p of the ground field can be chosen as small as possible (e.g. at most 4 bits). The estimation of the key size is discussed in section 7 in [3].

[Encryption of ASC06]

Let m be a plain text, and divide m into small blocks as $m = m_0||m_1||\cdots||m_{\ell-1}$ where each m_i is chosen $0 \leq m_i \leq p - 1$.

1. Embed m into a plain text polynomial as $m(t) = m_{\ell-1}t^{\ell-1} + \cdots + m_1 t + m_0$
2. Choose a random polynomial $s(x, y, t)$ containing a term $x^\alpha y^\beta$ with $\alpha > \deg_x X(x, y, t)$ and $\beta > \deg_y X(x, y, t)$ and satisfying $(\deg_x s(x, y, t) + \deg_y s(x, y, t))d + \deg_t s(x, y, t) < \ell$. (This implies $\deg(s(u_x(t), u_y(t), t) - s(v_x(t), v_y(t), t)) < \ell$, therefore we can extract $f(t)$ in the decryption step.)
3. Choose a random polynomial $r(x, y, t)$ satisfying $\deg_t r(x, y, t) < \ell$, and a random monic irreducible polynomial $f(t)$ with $\deg f(t) \geqq \ell$

4. Compute the cipher polynomial

$$F(x,y,t) = m(t) + f(t)s(x,y,t) + X(x,y,t)r(x,y,t).$$

[Decryption of ASC06]

As D_1, D_2 are on X, $X(u_x(t), u_y(t), t) = X(v_x(t), v_y(t), t) = 0$.

1. Substitute sections D_1 and D_2 into $F(x,y,t)$:

   $h_1(t) = F(u_x(t), u_y(t), t) = m(t) + f(t)s(u_x(t), u_y(t), t)$

   $h_2(t) = F(v_x(t), v_y(t), t) = m(t) + f(t)s(v_x(t), v_y(t), t)$
2. Compute $h_1(t) - h_2(t) (= f(t)\{s(u_x(t), u_y(t), t) - s(v_x(t), v_y(t), t))\}$.
3. Factorize and find $f(t)$ as a monic irreducible polynomial with maximum degree.
4. Compute $m(t)$ by reducing $h_1(t)$ by $f(t)$. ($\deg m(t) < \deg f(t)$.)
5. Extract m from $m(t)$.

3.2 Attacks on ASC06

To attack ASC06, the following algorithms are suggested.

Assumption 1. For the defining equation of the algebraic surface X which will be used as the public key, the leading term is in the form as $\mathrm{LT}(X)cx^{\alpha}y^{\beta}$ where $c \in \mathbb{F}_p$ and $(\alpha, \beta) \neq (0,0)$ w.r.t. a monomial order $\hat{R}$.

Algorithm 1 (Uchiyama-Tokunaga's attack).

Input: Akiyama-Goto's public key $X(x,y,t) \in \mathbb{F}_p[x,y,t]$ satisfying Assumption 1, cipher polynomial $F(x,y,t) \in \mathbb{F}_p[x,y,t]$.

Output: Plaintext m which corresponds to the cipher polynomial $F(x,y,t)$.

1. Calculate normal form $R_1(x,y,t)$ of the reduction of $F(x,y,t)$ by $X(x,y,t)$.
2. Among the temrs of R_1, randomly choose the term satisfying $x^i y^j$ $((i,j) \neq (0,0))$, and its coefficient not being in $\mathbb{F}_p$, then let its coefficient be C.
3. Calculate factors in $\mathbb{F}_p[t]$ of C, and let the set consisting of irreducible fators whose degree is greater than or equal to ℓ be $\hat{G}$. Choose the element $g \in \hat{G}$ and the normal form n of R_1 becomes an element in $\mathbb{F}_p[t]$. ($g(t)$ is $f(t)$)

4. Compute a polynomial $n(t) = n_{k-1}t^{k-1} + \cdots + n_1 t + n_0 \in \mathbb{F}_p[t]$, outputs $m = n_0||n_1||\cdots||n_{k-1}$ and end. ($n(t)$ is $m(t)$)

If $c_{\alpha\beta}(t)$ of $\mathrm{LT}(X) = c_{\alpha\beta}(t)x^\alpha y^\beta$ is not constant then the normal form of $F(x,y,t)$ by $X(x,y,t)$ does not necessarily stop in the form as $F(x,y,t) = m(t) + f(t)R_2(x,y,t) + X(x,y,t)(f(t)G_2(x,y,t) + q(x,y,t)) \xrightarrow[X]{} m(t) + f(t)R_2(x,y,t)$, i.e. some terms might be reduced and disappear, so we might fail to detect $f(t)$. It was suggested in January 2007, see [5] for detail.

Next, the author suggested Algorithm 2 in July 2007 (see [9, 10]), and Algorithm 3 in October 2007 (see [11,10]), which are applicable to all cases as follows.

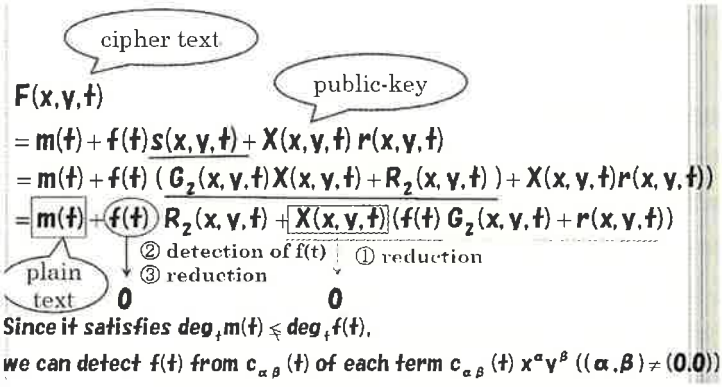

Fig. 3. Cryptanalysis: How to detect a plain-text.

Algorithm 2. (Iwami's attack: straightforward generalization in $\mathbb{F}_p(t)[x,y]$)

Input: Akiyama-Goto's public key $X(x,y,t) \in \mathbb{F}_p[x,y,t]$,
cipher polynomial $F(x,y,t) \in \mathbb{F}_p[x,y,t]$.

Output: Plaintext m which corresponds to the cipher polynomial $F(x,y,t)$.

0. Transform public key X to be monic as $\widetilde{X}$:=$X/\mathrm{LC}(X)$.
1. Calculate the normal form $R_1(x,y,t) \in \mathbb{F}_p(t)[x,y]$ by reduction of F by $\widetilde{X}$.
2. Randomly choose the term satisfying $c_{ij}(t)x^i y^j$ $((i,j) \neq (0,0))$ and $c_{ij}(t)$

not being in $\mathbb{F}_p$, changing $c_{ij}(t)(\in \mathbb{F}_p(t)[x,y])$ to equivalent fractions with a common denominator, and let the numerator be $C(\in \mathbb{F}_p[t])$.

3. Factorize C in $\mathbb{F}_p[t]$, and let the set consisting of irreducible factors whose degree is greater than or equal to ℓ be $\hat{G}$. Choose $g \in \hat{G}$ and calculate the normal form n by reduction of R_1 by g becomes an element in $\mathbb{F}_p[t]$.
4. Compute a polynomial $n(t) = n_{k-1}t^{k-1} + \cdots + n_1 t + n_0 \in \mathbb{F}_p[t]$, outputs $m = n_0||n_1||\cdots||n_{k-1}$ and end.

During the reduction step, to obtain $m(t)$ in $\mathbb{F}_p[x,y,t]$ (not in $\mathbb{F}_p(t)[x,y]$), we must not combine appearing rational functions and the lower polynomial terms.

In the following algorithm, We utilize Gröbner basis techniques introducing a new parameter. It enables us not to work via rational function field but to keep staying in the polynomial ring.

Algorithm 3. (Iwami's attack: Gröbner basis techniques in $\mathbb{F}_p[x,y,t,\mathcal{A}]$)

Input: Akiyama-Goto's public key $X(x,y,t) \in \mathbb{F}_p[x,y,t]$,
cipher polynomial $F(x,y,t) \in \mathbb{F}_p[x,y,t]$.

Output: Plaintext m which corresponds to the cipher polynomial $F(x,y,t)$.

0. Calculate Gröbner basis GB_X for an ideal $I_X := \langle \mathcal{A}\cdot X(x,y,t), \mathcal{A}\cdot \mathrm{LC}(X) - 1\rangle \subset \mathbb{F}_p[x,y,t,\mathcal{A}]$, introducing a new parameter $\mathcal{A}$, using the order $x \succ y \succ \mathcal{A} \succ t$ in $\mathbb{F}_p[x,y,t,\mathcal{A}]$.
1. Calculate the normal form $R(x,y,t,\mathcal{A}) \in \mathbb{F}_p[x,y,t,\mathcal{A}]$ of the reduction of $F(x,y,t)$ by GB_X.
2. Randomly choose the term satisfying $c_{ij}(t,\mathcal{A})x^iy^j$ $((i,j) \neq (0,0))$ where $c_{ij}(t,\mathcal{A})$ not being in $\mathbb{F}_p$, then let $c_{ij}(t,\mathcal{A})$ be C.
3. To perform desired factorization for detecting $f(t)$, we factor out powers of $\mathcal{A}$. Therefore we transform each term of C by using the relation $\mathcal{A}\cdot\mathrm{LC}(X) = 1$ as $\mathcal{A}^0 \mapsto (\mathcal{A}\cdot\mathrm{LC}(X))^2 = \mathcal{A}^2\cdot\mathrm{LC}(X)^2$, $\mathcal{A}^1 \mapsto \mathcal{A}(\mathcal{A}\cdot\mathrm{LC}(X))^1 = \mathcal{A}^2\cdot\mathrm{LC}(X)$, $\cdots$, so as to make the powers of $\mathcal{A}$ of each term equal. Then

perform factorization in $\mathbb{F}_p[t, \mathcal{A}]$, and let the set consisting of irreducible factors whose degree is greater than or equal to ℓ be $\hat{G}$. Choose the element $g(t) \in \hat{G}$. Calculate Gröbner basis GB_g for an ideal $I_g := \langle g(t), \mathcal{A} \cdot \mathrm{LC}(X) - 1 \rangle \subset \mathbb{F}_p[t, \mathcal{A}]$, and calculate the normal form $n \in \mathbb{F}_p[t]$, reducing $R(0, 0, t, \mathcal{A})$ by GB_g.

4. Compute a polynomial $n(t) = n_{k-1}t^{k-1} + \cdots + n_1 t + n_0 \in \mathbb{F}_p[t]$, outputs $m = n_0 || n_1 || \cdots || n_{k-1}$ and end.

Therefore, Algorithm 2, 3 are applicable to all cases, i.e. it shows that the ASC06 is broken. Moreover, Inanov and Voloch suggested another attack by utilizing trace map of algebraic extensions of function fields.

3.3 Improved Algebraic Surface Public-Key Cryptosystem (ASC09)

Akiyama, Goto and Miyake suggested ASC09 [4] as an improved version as follows. Note that the differences between ASC06 and ASC09 are :

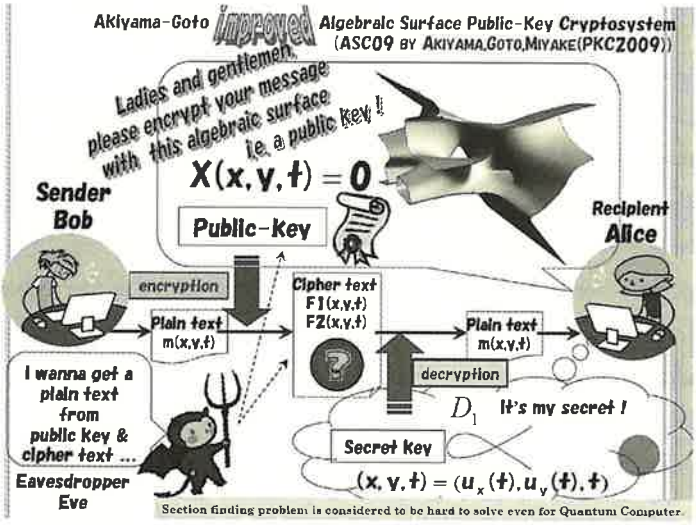

Fig. 4. improved algebraic surface cryptosystem

(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.

[Key generation of ASC09]

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

   (c) $f(x,y,t) = \sum_{(i,j)\in\Lambda_f} f_{ij}(t)x^iy^j$: 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^iy^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 $x^iy^jt^k$ terms in $m(x,y,t)$, so that $m(x,y,t) = \Sigma_{(i,j,k)\in\Gamma_m} c_{ijk}x^iy^jt^k$.

[Encryption of ASC09]

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 ASC09]

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 from $m_{ij}(t)$ and authenticate the MAC of m. We can make certain of the plaintext m, if MAC is authenticated, Otherwise, return step 4.

3.4 Attacks on ASC09

Reduction Attack : Ivanov and Voloch suggested the guideline of substitution attack briefly on ASC09 in section 3 in [7], but the practical algorithm was not given. Then, the author tried another way, i.e. reduction attack on ASC09, but it needs the following assumption. See [12] in detail. Let $\overline{A}^B$ denotes the normal form of A by reduction of B.

Assumption 2. The condition $\overline{f(x,y,t)}^{X(x,y,t)}\overline{s_i(x,y,t)}^{X(x,y,t)} \prec X(x,y,t)$ holds true in the encryption step in ASC09.

Note that if **Assumption 2** is satisfied, then

$$\overline{f(x,y,t)s_i(x,y,t)}^{X(x,y,t)} = \overline{f(x,y,t)}^{X(x,y,t)}\overline{s_i(x,y,t)}^{X(x,y,t)}$$

holds true, and as a result, the attacker can obtain the plaintext by the following algorithm.

Algorithm 4 (Reduction attack on ASC09).

Input: public-key $X(x,y,t)$, cipher polynomials $F_1(x,y,t)$ and $F_2(x,y,t)$, satisfying **Assumption 2.**

Output: plaintext polynomial $m(x,y,t)$.

1. Calculate $\tilde{F}(x,y,t) := F_1(x,y,t) - F_2(x,y,t)$
2. Calculate the normal form $\overline{\tilde{F}(x,y,t)}^{X(x,y,t)}$.
3. Find a factor $\overline{f(x,y,t)}^{X(x,y,t)}$ using their conditions by performing multivariate factorization of $\overline{\tilde{F}(x,y,t)}^{X(x,y,t)}$.

4. Calculate the normal form

$$\overline{\overline{m(x,y,t)}^{X(x,y,t)}\overline{f(x,y,t)}^{X(x,y,t)}} := \overline{\overline{F_1(x,y,t)}^{X(x,y,t)}\overline{f(x,y,t)}^{X(x,y,t)}}.$$

5. $m(x,y,t) := \sum_{(i,j,k)\in\Gamma_m} m_{ijk}x^iy^jt^k$ where $\{m_{ijk}\}$ are unknown. Calculate

$$\overline{\overline{\sum_{(i,j,k)\in\Gamma_m} m_{ijk}x^iy^jt^k}^{X(x,y,t)}\overline{f(x,y,t)}^{X(x,y,t)}}.$$

6. By comparing the coefficients of step4. and step5., we obtain system of equations w.r.t. m_{ijk}.
7. By solving linear equation w.r.t. m_{ijk}, we obtain $\{m_{ijk}\}$ and hence the plaintext polynomial $m(x,y,t)$. If the adequate plaintext polynomial cannot be obtained, go to step3 and let another factor be a factor $\overline{f(x,y,t)}^{X(x,y,t)}$.

Therefore, for security, $f(x,y,t)$, $s_1(x,y,t)$ and $s_2(x,y,t)$ have to be chosen so as not to satisfy $\overline{f(x,y,t)}^{X(x,y,t)}\overline{s_i(x,y,t)}^{X(x,y,t)} \prec X(x,y,t)$ in ASC09.

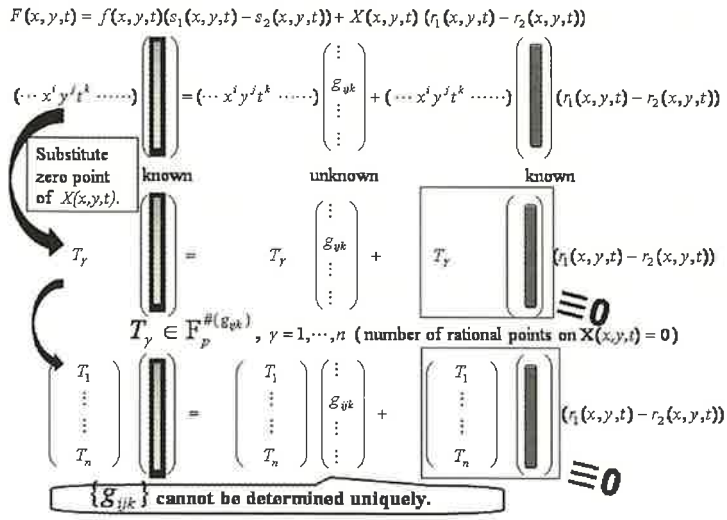

Fig. 5. Ivanov and Voloch's rational point attack

Rational Point Attack : Ivanov and Voloch's rational point attack [7] on ASC09 is as follows.

Algorithm 5 (Ivanov and Voloch's rational point attack).

1. $F(x,y,t) = F_1(x,y,t) - F_2(x,y,t)$ 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
   $g(x,y,t) = \Sigma_{(i,j)\in\Gamma_g} g_{ijk} x^i y^j t^k$ where $\Gamma_g = \{(i,j,k) \in \mathbb{N}^3 | g_{ijk} \neq 0\}$ denotes the set of exponents of nonzero $x^i y^j t^k$ 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 $f(x,y,t)$.
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 in the realistic calculation.

Substitution of Series Solution : The author attacked by substitution of series solution [13] on ASC09 is as follows.

Algorithm 6 (substitution of series solution attack by Iwami).

1. $F(x,y,t) = F_1(x,y,t) - F_2(x,y,t)$ 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
   $$g(x,y,t) = \Sigma_{(i,j)\in\Gamma_g} g_{ijk} x^i y^j t^k$$
   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 $x^i y^j t^k$ 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,

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

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 **Fig. 6.** Note that we can also obtain more equations by raising the field of definition for $X(x,y,t)=0$. But it is no different than one obtained in Voloch's rational point attack in the sense that the polynomial $g(x,y,t)$ (and so $f(x,y,t)$ and $m(x,y,t)$) have too many candidates and cannot be determined uniquely in the realistic calculation. For detail, see [13].

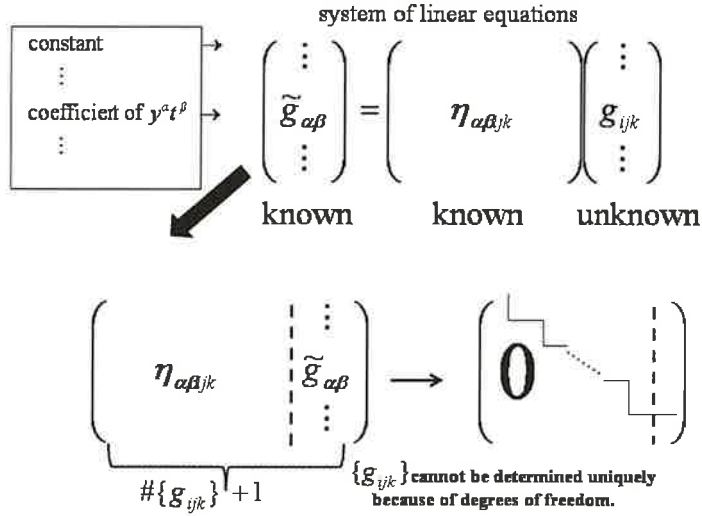

Fig. 6. Iwami's substitution of series solution attack

Parametrization : The author tried to attack by parametrization in [14]. A parameter t introduced in a half-finished state makes it difficult to apply known parametrization algorithms directly. See the following example.

Toy example in [4]:

Let $X(x,y,t)=0$ be a defining equation of a public-key as

$X(x,y,t)=(t+10)x^3y^2+(16t^2+7t+4)xy^2+3t^{16}+8t^{15}+13t^{14}+8t^{13}+3t^{12}+12t^{11}+4t^{10}+8t^7+7t^6+4t^7+13t^6+2t^5+5t^4+4t^3+14t^2+9t+14$

and

$D:(u_x(t),u_y(t),t)=(14t^3+12t^2+5t+1,11t^3+3t^2+5t+4,t)$

be a section of $X(x,y,t)$. Now, our target is a rational parametrization as

$(\frac{\chi_{11}(t)}{\chi_{12}(t)},\frac{\chi_{21}(t)}{\chi_{22}(t)},t)$.

If we apply algorithm "SYMBOLIC-PARAMETRIZATION-BY-DEGREE-d-ADJOINTS" in [20] (pp.142-143), input/output data is as follows.

Input: $X(x,y,t)$ where t is a homogenenizing parameter,

Output: $(\frac{\chi_{11}(t)}{\chi_{12}(t)}, \frac{\chi_{21}(t)}{\chi_{22}(t)}, t)$.

Unfortunately, t is just a homogenenizing parameter of $X(x, y, t)$. This is not what we want.

In other ways, if we apply algorithm "PARAMETRIZE" in [21], input/output data is as follows.

Input: $X(x, y, t)$,

Output: $(\frac{\chi_{11}(a, b)}{\chi_{12}(a, b)}, \frac{\chi_{21}(a, b)}{\chi_{22}(a, b)}, \frac{\chi_{31}(a, b)}{\chi_{32}(a, b)})$.

The form of output is not what we want. Therefore, the attack by parametrization was failed.

Improvement of Voloch' s rational point attack by using monomial reduction : After performing Voloch's rational point attack (or Iwami's substitution of series solutions attack), we try to obtain more equations and decrease the candidates 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 5**) or Iwami's substitution of series solutions attack (step 4. in **Algorithm 6**)). 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 particular 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 7 (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 5** or step 4. in **Algorithm 6**, 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 particular 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 monomials 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 lattice basis where a is a scaling factor.
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
$$\vec{g} = \vec{g_s} + \Sigma c_i \vec{b_i}.$$

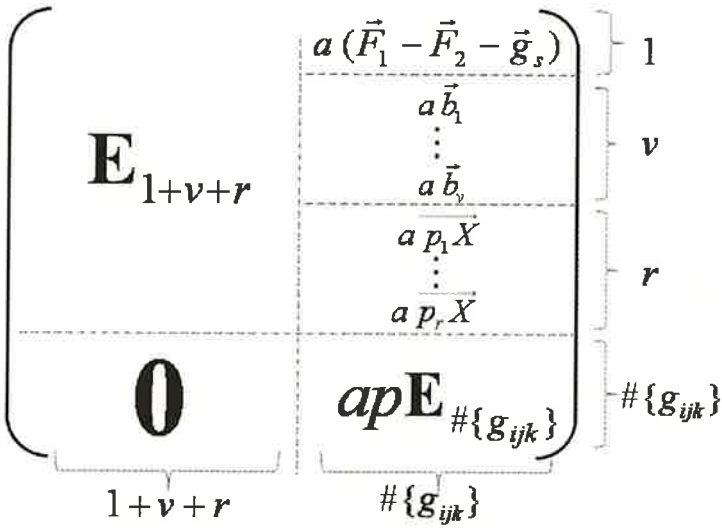

Fig. 7. The matrix for calculating reduced lattice basis.

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

As is shown above, 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.

If the 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 ASC09 were not exist, then it allowed us to success in improvement. However, it has the degree condition, so we cannot improve them. The details are follows.

Theorem 1. *As for* $\vec{F_1} - \vec{F_2} = \vec{g_s} + \Sigma_{i=1}^{v} c_i \vec{b_i} + \Sigma_{i=1}^{r} d_i \vec{p_i X}$ *in* Algorithm 7, *the equation* $v = r$ *holds true.*

Theorem 2. *The rank of the matrix for calculating reduced lattice basis in* Fig. 7 *is* $1+v$, *therefore, the dimension of the solution space of* $g(x, y, t)$ *still remains* v.

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 5 and Algorithm 6 was failed. In other words, these restrictions of the degree conditions keep the supports of $f(s_1 - s_2)$ and $X(r_1 - r_2)$ in the same form, and prevent Algorithm 7 from increasing the number of the system of equations and decreasing the number of candidates of a certain polynomial, therefore the result of the suggested method is the same as Voloch's method, i.e. the improvement was failed. For detail, see [15].

Ideal Decomposition : Faugére and Spaenlehauer suggested algorithms which can break ASC09 using ideal decomposition in polynomial time. The idea of a breakthrough is as follows.

As the cipher-text polynomials are constructed as

$F_i(x,y,t) = m(x,y,t) + f(x,y,t)s_i(x,y,t) + X(x,y,t)r_i(x,y,t)$ $(i = 1,2)$,

then ideal decomposition is performed as follows if and only if $\langle f, X\rangle$ and $\langle s_1 - s_2, X\rangle$ are prime ideals.

$$\begin{aligned}\text{ideal } I &\stackrel{\text{def}}{=} \langle F_1 - F_2, X\rangle \\ &= \langle f(s_1 - s_2) + X(r_1 - r_2), X\rangle \\ &= \langle f(s_1 - s_2) + X\rangle \\ &= \langle f, X\rangle \cap \langle s_1 - s_2, X\rangle\end{aligned}$$

Note that if $\langle f, X\rangle$ and $\langle s_1 - s_2, X\rangle$ are not prime ideals in $\mathbb{F}_p[x,y,t]$ then we cannot perform such decomposition of ideals, that is to say, this strategy is not available. They say in Lemma 1. in [8] that "generically" they are prime ideals in $\mathbb{F}_p[x,y,t]$. However, we can say that there is still room for consideration.

Then we can manupulate implicitly the polynomial f through $\langle f, X\rangle$ as

$$\begin{aligned}\langle F_1, F_2, X\rangle + \langle f, X\rangle &= \langle F_1, F_2, X, f\rangle \\ &= \langle m, f, X\rangle\end{aligned}$$

By using this, we can recover the plain-text polynomial $m(x,y,t)$ by solving linear system.

By introducing a parameter z, the number of candidates of the solutions can be reduced in the field of fractions $\mathbb{F}_p(t)$ as

$$\langle F_1 + z, F_2 + z, X\rangle + \langle f, X\rangle = \langle F_1 + z, F_2 + z, X, f\rangle = \langle m + z, f, X\rangle.$$

Algorithm 8 (Attack using ideal decomposition).

1. Compute the resultant $\mathrm{Res}_x(F_1 - F_2) \in \mathbb{F}_p(t)[y]$.
2. Factor the resultant $\mathrm{Res}_x(F_1 - F_2) = \prod Q_i(y)$. Let $Q_0(y) \in \mathbb{F}_p(t)[y]$ denotes an irreducible factor of highest degree in y.
3. Compute a grevlex-Gröbner basis of the ideal $J = \langle F_1 + z, F_2 + z, X, Q_0\rangle \subset \mathbb{F}_p(t)[x,y,z]$.
4. Consider the following linear system over $\mathbb{F}_p(t)$:

$$NF_J(z) + \sum_{(i,j)\in\Lambda_m} m_{ij}(t) NF_J(x^i y^j) = 0,$$

where NF_J denotes the normal form with respsct to the ideal J. If the system was no solution, then go back to Step 2 and choose another factor of the resultant.

5. Return $m = \sum_{(i,j)\in\Lambda_m} m_{ij}(t) x^i y^j$ where $(m_{ij}(t))$ is the unique solution of the linear system.

They suggested 3 variants of attacks called Level 1 to 3. Algorithm 8 can be seen as "Level 2 Attack: computing in the field of fractions $\mathbb{K} = \mathbb{F}_p(t)$". For detail, see [8].

Althogh there is still room for consideration that $\langle f, X\rangle$ and $\langle s_1 - s_2, X\rangle$ are not always prime ideals in $\mathbb{F}_p[x, y, t]$, ASC09 was broken in polynomial time. But they avoided to solve the section finding problem by using ideal decomposition, so the section finding problem itself is still available and an interesting problem.

4 Conclusion

We give a brief survey of MPKC focusing attention on the interactions between MPKC and various types of computer algebra techniques, especially for algebraic surface cryptosystem. We see various trials to attack using computer algebra techniques such as reduction, application of Gröbner basis, reduced lattice basis, parametrization, substitution of series solutions or rational points, and ideal decomposition. As described in this paper, computer algebra techniques developed cryptosystems, and vice versa. "Multivariate" allows us various ways of approach, therefore, it's attractive.

References

[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] A. Akiyama, Y. Goto : A Security Analysis for a Public-key Cryptosystem using Algebraic Surfaces. CD-ROM 2A3-1, SCIS2006, January 2006.

[3] 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.

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

[5] S. Uchiyama, H. Tokunaga : On the Security of the Algebraic Surface Public-Key Cryptosystems. CD-ROM 2C1-2, SCIS2007, January 2007.

[6] 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.

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

[8] J.Ch. Faugére and P.J. Spaenlehauer : Algebraic Cryptanalysis of the PKC'09 Algebraic Surface Cryptosystem, Public Key Cryptography PKC 2010, LNCS 6056, pp.35-52, Springer, 2010.

[9] M. Iwami : A Reduction Attack on Algebraic Surface Public-Key Cryptosystems. Workshop of Research Institute for Mathematical Sciences (RIMS) Kyoto University, New development of research on Computer Algebra (held on July 4-6 2007) RIMS Kokyuroku 1572, pp.114-123, November 2007.

[10] 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, pp.323-332, Springer, 2008.

[11] 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, pp.93-103, March 2008.

[12] 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.

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

[14] M. Iwami : Surface Parametirizaion and Cryptography (poster presentation), The 11th International Workshop on Computer Algebra in Scientific Computing, September 14 and 19, 2009, Kobe University, Japan.

[15] M. Iwami : An improvement of Voloch's rational point attack on improved algebraic surface cryptosystem, RIMS Kokyuroku, Vol.1759, pp.105-114, 2011.

[16] J. Ding, J.E. Gower, D.S. Schmidt : Multivariate Public Key Cryptosystems, Advances in

Information Security, Vol. 25, Springer.
[17] R. Heindl : New directions in multivariate public key cryptography, Proquest, Umi Dissertation Publishing, 2011.
[18] T. Matsumoto, H.Imai : Public quadratic polynomial-tuples for efficient signature verification and message encryption, Advances in cryptology - EUROCRYPT '88, LNCS 330, pp.419–453, Springer, 1988.
[19] J. Patarin : Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88, Advances in Cryptology - Crypto '95, LNCS 963, pp.248–261, 1995.
[20] J.Rafael Sendra, Franz Winkler, Sonia Perez-Diaz: Rational Algebraic Curves: A Computer Algebra Approach, Springer, 2008.
[21] J. Schicho : Rational parametrization of real algebraic surfaces, ISSAC'98 Proceedings of the 1998 international symposium on Symbolic and algebraic computation, pp.302–308, 1998.

Note

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