An Algebraic Surface Cryptosystem

Koichiro Akiyama[1], Yasuhiro Goto[2], and Hideyuki Miyake[1]

[1] Computer & Network Systems Laboratory, Corporate Research & Development Center, Toshiba Corp., 1 Komukai-Toshiba-cho, Saiwai-ku, Kawasaki, Kanagawa 212-8582, Japan
koichiro.akiyama@toshiba.co.jp, hideyuki.miyake@toshiba.co.jp
[2] Department of Mathematics, Hokkaido University of Education at Hakodate, 1-2 Hachiman-cho, Hakodate, Hokkaido 040-8567, Japan
ygoto@hak.hokkyodai.ac.jp

Abstract. We construct a public-key cryptosystem based on an NP-complete problem in algebraic geometry. It is a problem of finding sections on fibered algebraic surfaces; in other words, we use a solution to a system of multivariate equations of high degrees. Our cryptosystem is a revised version of the algebraic surface cryptosystem (ASC) we constructed earlier (cf. [AG04, AG06]). We revise its encryption algorithm to avoid known attacks. Further, we show that the key size of our cryptosystem is one of the shortest among those of post-quantum public-key cryptosystems known at present.

Keywords: Public-key Cryptosystem, Algebraic Surface, Section.

1 Introduction

In 1994, Shor showed that the factorization problem and the discrete logarithm problem can be solved efficiently by a quantum computer [Shr]. This implies that the RSA cryptosystem and Elliptic Curve cryptosystems will no longer be secure, once a quantum computer is built. We are thus in search for a public-key cryptosystem that does not rely on these problems and possibly can be implemented even on our present machines.

In this paper, we propose a new public-key cryptosystem whose security is based on an NP-complete problem in algebraic geometry. It is a problem of finding sections on algebraic surfaces fibered on an affine line. We shall call it a *section finding problem* (SFP) on algebraic surfaces. The SFP can be viewed as a problem of solving multivariate equation systems (of high degrees) over a finite field $\mathbb{F}_p$ with an arbitrary prime p. As this problem is known to be NP-complete, our cryptosystem is expected to have resistance against quantum computers. In what follows, we call our cryptosystem an *algebraic surface cryptosystem* (ASC).

The first version of the ASC was announced in [AG04]. It was then attacked by Uchiyama-Tokunaga [UT] and Voloch [Vol] in two different methods. The former attack uses a reduction-by-polynomial method that works in some special cases, while the latter employs a trace map of algebraic extensions of function fields that works in any case. (Eventually, Iwami [Iw08] found an unconditional reduction method generalizing the result of Uchiyama-Tokunaga.) The weakness

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-3-642-00468-1_29
S. Jarecki and G. Tsudik (Eds.): PKC 2009, LNCS 5443, pp. 425–442, 2009.

of the original ASC lay in the use of a one-variable polynomial in the encryption algorithm. We have therefore changed it to a three-variable polynomial and revised the entire cryptosystem to avoid the attacks we mentioned above.

The new ASC was announced in [AG07] and soon, Voloch [Vol] came up with an idea of attacking this new system. Fortunately, however, it did not really break our system as we explain in Sect. 5.5 later. In the present paper, we reproduce the cryptosystem described in [AG07], and fill in various details and update the toy example.

One of the advantages of our new ASC is the small key size. To the best of our knowledge, it can offer one of the shortest keys of the known post-quantum public-key cryptosystems. For instance, a multivariate public-key cryptosystem is a candidate for a post-quantum cryptosystem. Its private key size is in the same order as ASC, but the public key size tends to be very large. The following table describes a rough comparison of the key sizes for several post-quantum cryptosystems, where n is a security parameter.

Table 1. Key size of several post-quantum public-key cryptosystems

Cryptosystem	Lattice-based	Multivariate	Knapsack	ASC
Public key	$O(n \log n)$	$O(n^3)$	$O(n^2)$	$O(n)$
Private key	$O(n \log n)$	$O(n)$	$O(n)$	$O(n)$

Both multivariate public-key cryptosystems and our ASC are associated with a system of multivariate algebraic equations $f_1 = \cdots = f_m = 0$ over a finite field $\mathbb{F}_p$. Typically, the public key of a multivariate public-key cryptosystem is constructed directly from polynomials $f_1, \cdots, f_m$. The public key of the ASC, on the other hand, is a single equation $X(x, y) = 0$ over a polynomial ring $\mathbb{F}_p[t]$ whose solution $(u_x(t), u_y(t))$ is a pair of polynomials over $\mathbb{F}_p$ related with $f_1, \cdots, f_m$ (precisely, the coefficients of $u_x(t)$ and $u_y(t)$ are solutions to some equation system $f_1 = \cdots = f_m = 0$). In this way, we can elude the direct use of $f_1, \cdots, f_m$ and save the public-key size drastically.

This paper is organized as follows. Section 2 collects some important facts about algebraic surfaces and recalls our original cryptosystem (ASC04). Section 3 describes the attacks on the ASC04 by Uchiyama-Tokunaga and Iwami, and also by Voloch. We discuss how to avoid their attacks. Section 4 presents our new algebraic surface cryptosystem which has resistance against various types of attacks. That resistance is discussed in Sect. 5. Lastly, the key size of the ASC is evaluated in Sect. 6. In Appendix, we give a toy example to illustrate our algorithm concretely.

2 Preliminaries

2.1 Algebraic Surfaces and the Section Finding Problem

Let $k := \mathbb{F}_p$ be a finite prime field of p elements. An algebraic surface over k is the set of solutions of algebraic equations over k that has two dimensional freedom

over k. In order to construct our cryptosystem, we use an affine algebraic surface, X, in affine 3-space $\mathbb{A}^3_k$ defined by a single equation

$$f(x, y, t) = 0 \tag{1}$$

over k. It does not matter whether X is smooth or singular, but $f(x, y, t)$ should be irreducible.

There are many curves and points on X. For example, if we take another surface Y, then the intersection $X \cap Y$ is often a curve on X. These curves are easy to find, but finding *all* curves on X is a difficult problem; in fact, there is no effective algorithm to do so in general.

There is a special kind of curves on X which are generally very difficult to find explicitly. They are parameterized curves on X written in such a form as

$$(x, y, t) = (u_x(t), u_y(t), t) \ ,$$

where $u_x(t)$ and $u_y(t)$ are polynomials in t over k. If we define a map $\sigma : X \longrightarrow \mathbb{A}^1$ by $\sigma(x, y, t) = t$, then this parameterized curve induces an inverse map $\tau : \mathbb{A}^1 \longrightarrow X$ such that $\sigma \circ \tau = \mathrm{id}_{\mathbb{A}^1}$. The map σ is called a *fibration* of X on $\mathbb{A}^1$ and τ is called a *section* of σ. A section may be explained also as follows: rewriting $f(x, y, t)$ as a polynomial over $k[t]$, we can view X as a curve over the field $k(t)$ (or over the ring $k[t]$). Then a section is a $k(t)$-rational point on this curve. Finding such rational points is a Hilbert's 10th problem over a function field and is a hard mathematical problem. In our case, there is an exponential-time algorithm to solve this problem (cf. [Szp]), but no polynomial-time algorithm exists to find sections in general.

Definition 1. (Section Finding Problem) If $X(x, y, t) = 0$ is a surface over k, then the problem of finding a parameterized curve $(x, y, t) = (u_x(t), u_y(t), t)$ on X is called a *section finding problem* on X.

A general (but computationally inefficient) method of solving this problem, known at present, is as follows: express the defining equation for X as

$$X(x, y, t) = \sum_{(i,j,k)\in\Gamma_X} \eta_{i,j,k} x^i y^j t^k = 0 \ ,$$

where Γ_f denotes the set of indices (i, j, k) that appear in a polynomial $f(x, y, t)$. Choose r_x and r_y that satisfy $\deg u_x(t) < r_x$ and $\deg u_y(t) < r_y$ and write

$$\begin{aligned} u_x(t) &= \alpha_0 + \alpha_1 t + \cdots + \alpha_{r_x-1} t^{r_x-1} \ , \\ u_y(t) &= \beta_0 + \beta_1 t + \cdots + \beta_{r_y-1} t^{r_y-1} \ . \end{aligned}$$

The substitution of these into $X(x, y, t)$ gives

$$X(u_x(t), u_y(t), t) = \sum_{(i,j,k)\in\Gamma_X} \eta_{i,j,k} u_x(t)^i u_y(t)^j t^k =: \sum_i c_i t^i \ ,$$

where c_i are polynomials in α_i and β_j. If we write $r = \max\{i \deg u_x(t) + j \deg u_y(t) + k \mid (i,j,k) \in \Gamma_X\}$, then we find a system of equations

$$\begin{cases} c_0(\alpha_0, \cdots, \alpha_{r_x-1}, \beta_0, \cdots, \beta_{r_y-1}) = 0 \ , \\ \cdots \\ c_r(\alpha_0, \cdots, \alpha_{r_x-1}, \beta_0, \cdots, \beta_{r_y-1}) = 0 \ . \end{cases}$$

A solution to this system is a section of X. In this sense, our section finding problem can be reduced to solving a multivariate equation system of large degrees and such a problem is known to be NP-complete (cf. [GJ]).

2.2 Original Version (ASC04)

We briefly explain the first version of our cryptosystem (ASC04) that was announced in 2004. See [AG04] for the details.

Keys. Following are important system parameters:

1. Size of the ground field: p
2. Maximum degree of sections: d
3. Number of blocks in a plaintext: l (assume $d < l$)

[Public keys and secret keys]

1. The secret key is a pair of two sections

$$D_1 : (x,y,t) = (u_x(t), u_y(t), t), \qquad D_2 : (x,y,t) = (v_x(t), v_y(t), t)$$

with

$$d = \max\{\deg u_x(t), \deg u_y(t), \deg v_x(t), \deg v_y(t)\} \ . \tag{2}$$

2. The public key is a surface X that contains D_i as sections

$$X(x,y,t) = \sum_{(i,j)\in\Lambda_X} c_{ij}(t) x^i y^j = 0 \ ,$$

where $\Lambda_X := \{(i,j) \in \mathbb{N}^2 | c_{ij}(t) \neq 0\} \ni (0,0), (1,0)$.

Key Generation. First we choose polynomials $D_1 = (u_x(t), u_y(t), t)$ and $D_2 = (v_x(t), v_y(t), t)$, and then construct a surface $X(x,y,t)$ that contains D_1 and D_2 as sections. This can be done, for instance, by letting the polynomials satisfy $(u_x(t) - v_x(t)) | (u_y(t) - v_y(t))$.

Encryption Algorithm. Divide a plaintext m into l blocks as $m = m_0 || \cdots ||m_{l-1}$ and embed m into a polynomial in t by

$$m(t) = m_{l-1} t^{l-1} + \cdots + m_1 t + m_0 \quad (0 \leq m_i < p, \ i = 0, \cdots, l-1) \ .$$

1. Choose an irreducible polynomial $f(t)$ of degree l.

2. Choose a random polynomial

$$r(x,y,t) = \sum_{(i,j)\in\Lambda_r} r_{ij}(t)x^i y^j \tag{3}$$

and write

$$X(x,y,t)r(x,y,t) = \sum_{(i,j)\in\Lambda_{Xr}} a_{ij}(t)x^i y^j \tag{4}$$

where $\Lambda_{Xr} := \{(i,j) \in \mathbb{N}^2 | a_{ij}(t) \neq 0\}$.

3. Randomly choose

$$s(x,y,t) = \sum_{(i,j)\in\Lambda_{Xr}} s_{ij}(t)x^i y^j \tag{5}$$

with $\deg s_{ij}(t) = \deg a_{ij}(t) - l$. This makes fs and Xr have the same form as polynomials in x and y over $k[t]$.

4. Set the cipher polynomial $F(x,y,t)$ to be

$$F(x,y,t) = m(t) + f(t)s(x,y,t) + X(x,y,t)r(x,y,t) \ . \tag{6}$$

Decryption Algorithm. First we substitute sections D_i into $F(x,y,t)$ and let

$$\begin{aligned} h_1(t) =& F(u_x(t), u_y(t), t) = m(t) + f(t)s(u_x(t), u_y(t), t) \ , \\ h_2(t) =& F(v_x(t), v_y(t), t) = m(t) + f(t)s(v_x(t), v_y(t), t) \ . \end{aligned}$$

1. Compute $h_1(t) - h_2(t)$ to find $f(t)\{s(u_x(t), u_y(t), t) - s(v_x(t), v_y(t), t)\}$.
2. Factor $h_1(t) - h_2(t)$ and obtain $f(t)$ as an irreducible polynomial of degree l.
3. Find $m(t)$ as the remainder in division of $h_1(t)$ by $f(t)$ and recover the plaintext m from $m(t)$.

3 Attacks on ASC04

There have been announced two attacks on the ASC04. We sketch the ideas of these attacks and analyze how to avoid them.

3.1 Reduction Attack by Uchiyama and Tokunaga

Uchiyama and Tokunaga announced an attack on the ASC04 in 2007 (cf. [UT]). Their algorithm is as follows.

1. Given a cipher text $F(x,y,t)$ as in (6), compute the remainder

$$R(x,y,t) = \sum_{(i,j)\in\Lambda_R} g_{ij}(t)x^i y^j \tag{7}$$

in division of $F(x,y,t)$ by a public key $X(x,y,t)$.

2. Let G be the set of all irreducible factors of $g_{ij}(t)$ of degree $\geq l$.

3. For each $f_i(t) \in G$, find the remainder $m_i(t)$ in division by $g_{00}(t)$. Then one of the $m_i(t)$'s coincides with the plaintext $m(t)$.

To make this algorithm work, it is necessary that G contains $f(t)$ and that g_{00} has the form $g_{00}(t) = m(t) + f(t)s(t)$ for some $s(t)$. In [UT], it is proven that this condition is satisfied if the leading term $LT(X)$ of $X(x, y, t)$ in a monomial order is of the form $LT(X) = cx^{\alpha}y^{\beta}$ with $c \in \mathbb{F}_p$.

The algorithm of Uchiyama and Tokunaga can be generalized if there exists a monomial order for x, y and t with which the remainder of $F(x, y, t)$ in division by $X(x, y, t)$ coincides with some part of

$$m(t) + f(t)s(x, y, t) = m(t) + f(t) \sum_{(i,j)\in\Lambda} s_{ij}(t)x^i y^j \quad . \tag{8}$$

3.2 A Refinement by Iwami

The Uchiyama and Tokunaga attack had an assumption that the leading term $LT(X)$ of $X(x, y, t)$ in a monomial order is of the form $LT(X) = cx^{\alpha}y^{\beta}$ with $c \in \mathbb{F}_p$. In [Iw08], Iwami found a way to get rid of this assumption. The main idea is to consider $X(x, y, t)$ as a polynomial in two variables x and y over the field $\mathbb{F}_p(t)$ rather than as a polynomial in three variables over $\mathbb{F}_p$. Then by dividing through by the coefficient of the leading term, one can always have the situation $LT(X) = x^{\alpha}y^{\beta}$. Now apply the reduction algorithm to $X(x, y, t)$ over $\mathbb{F}_p(t)$ and clear the denominators of the coefficients. The same method of Uchiyama and Tokunaga on the numerators of the coefficients reveals the polynomial $f(t)$.

3.3 Conditions to Avoid the Reduction Attack

One way to avoid the reduction attack is to modify the ASC04 so that no monomial order will be effective to extract sufficient information of $m(t)$ and $f(t)$ when $F(x, y, t)$ is divided by $X(x, y, t)$.

Let $>$ be a monomial order on $k[x_1, \cdots, x_n]$ and write x^{α} for $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. For a non-zero polynomial $f = \sum_{\alpha} a_{\alpha}x^{\alpha} \in k[x_1, \cdots, x_n]$, let $multideg\,(f)$ denote the multidegree of f and $LT(f)$ the leading term of f. It is known that every polynomial $f \in k[x_1, \cdots, x_n]$ can be expressed as

$$f = aX + r$$

for some $a, r \in k[x_1, \cdots, x_n]$ satisfying $r = 0$ or r is a linear combination of monomials that are not divisible by $LT(X)$. Furthermore, if $aX \neq 0$, then $multideg\,(f) \geq multideg\,(aX)$. As r is not divisible by $LT(X)$ when $r \neq 0$, we can avoid the reduction attack if $LT(X)$ divide some monomials in $m(t)$ and $f(t)$ in every monomial order. Since there are an infinite number of monomial orders, almost all monomials in $X(x, y, t)$ can be a leading term. Therefore we are led to change $m(t)$ and $f(t)$ to polynomials $m(x, y, t)$ and $f(x, y, t)$ in 3 variables and pose the following condition:

(Condition). $m(x, y, t)$ and $f(x, y, t)$ contain some monomials that are divisible by all monomials in $X(x, y, t)$.

3.4 An Attack by Voloch

Another attack was suggested by Voloch [Vol]. His idea is to consider an extension of $\mathbb{F}_p(t)$ and use the trace map T. Let $F(x, y, t)$ be a ciphertext.

1. Substitute some polynomial $c(t)$ into y so that $X(x, c(t), t)$ becomes irreducible.
2. Let α be a solution to $X(x, c(t), t) = 0$ over $\mathbb{F}_p(t)$ and find $\beta \in \mathbb{F}_p(t)(\alpha)$ such that $T_{\mathbb{F}_p(t)(\alpha)/\mathbb{F}_p(t)}(\beta) = 0$.
3. Compute $T(\beta F(\alpha, c(t), t))$ and have

$$T(\beta F(\alpha, c(t), t)) = T(\beta m(t) + \beta f(t)s(\alpha, c(t), t)) = f(t)T(\beta s(\alpha, c(t), t)) \ .$$

4. Factor $T(\beta F(\alpha, c(t), t))$ and obtain $f(t)$.
5. Find $\beta_1 \in \mathbb{F}_p(t)(\alpha)$ such that $T_{F_p(t)(\alpha)/F_p(t)}(\beta_1) \in \mathbb{F}_p^{\times}$ and compute:

$$T(\beta_1 F(\alpha, c(t), t)) = m(t)T(\beta_1) + f(t)T(\beta_1 s(\alpha, c(t), t)) \ .$$

6. Divide $T(\beta_1 F(\alpha, c(t), t))$ by $f(t)$ to find $m(t)T(\beta_1)$ and then $m(t)$.

3.5 Ideas to Avoid Voloch's Attack

There may be two ways to avoid Voloch's attack: make the trace computation extremely time-consuming or change the form of $m(t)$ and $f(t)$. Both ideas can be realized simultaneously by letting $m(t)$ and $f(t)$ multi-variable.

For instance, replace $m(t)$ by $m(x, t)$ and $f(t)$ by $f(y, t)$. Choose $x = c(t)$. Let $y = \alpha$ be a solution to $X(c(t), y, t) = 0$. Compute $T(\beta_0 F(c(t), \alpha, t))$ with an element β_0 satisfying $T(\beta_0) = 0$. We can find $T(\beta_0 f(\alpha, t)s(c(t), \alpha, t))$. But, this does not yield $f(\alpha, t)$. Neither in the attempt by $y = c(t)$ can we obtain enough information for $f(y, t)$ or $m(x, t)$. Therefore the Voloch attack does not work in this case.

(On the other hand, if we replace $m(t)$ by $m(x, t)$ and keep $f(t)$ as is, then $f(t)$ can be obtained in the same way as in Sect. 3.4 and $m(x, t)$ can be found by taking various $y = c(t)$. Hence the case $(m(x, t), f(t))$ is insecure.)

Considering all cases, we conclude in particular the following:

(Safe case). The case where $m(t)$ and $f(t)$ are replaced by three-variable polynomials $m(x, y, t)$ and $f(x, y, t)$, respectively, is safe.

4 New Algorithm (Algebraic Surface Cryptosystem)

This section presents an improved algebraic surface public-key cryptosystem (ASC) which has resistance against the attacks described in Sect. 3. The discussions in Sect. 3.5 and 3.3 suggest that $m(t)$ and $f(t)$ should be 3-variable polynomials $m(x, y, t)$ and $f(x, y, t)$.

Although this idea is effective to avoid the attacks, a problem arises now in decryption steps 1 and 2 of ASC04 as $m(u_x(t), u_y(t), t) \neq m(v_x(t), v_y(t), t)$ and

$f(u_x(t), u_y(t), t) \neq f(v_x(t), v_y(t), t)$. Our solution to overcome this drawback is to employ an algebraic surface X with one section and use two cipher polynomials instead.

We assume that algebraic surfaces are defined over a prime field $\mathbb{F}_p$. (p is a prime small enough to calculate, such as primes within the word size.)

4.1 Keys

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) $m(x, y, t) = \sum_{(i,j)\in \Lambda_m} m_{ij}(t)x^i y^j$: a plaintext polynomial where Λ_m and $\deg m_{ij}(t)$ are fixed.
   (c) $f(x, y, t) = \sum_{(i,j)\in \Lambda_f} f_{ij}(t)x^i y^j$: a divisor polynomial where Λ_f and $\deg f_{ij}(t)$ are fixed.

   Here Λ_A denotes the set of exponents of nonzero $x^i y^j$ terms in $A(x, y, t)$. We choose $m(x, y, t)$ and $f(x, y, t)$ so that they satisfy

$$\Lambda_m \subset \Lambda_f \Lambda_X \tag{9}$$

   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:

$$\begin{cases} \deg_x X(x, y, t) < \deg_x m(x, y, t) < \deg_x f(x, y, t) \\ \deg_y X(x, y, t) < \deg_y m(x, y, t) < \deg_y f(x, y, t) \\ \deg_t X(x, y, t) < \deg_t m(x, y, t) < \deg_t f(x, y, t) \end{cases} \\ \text{and} \\ (\deg_x m(x, y, t), \deg_y m(x, y, t), \deg_t m(x, y, t)) \in \Gamma_m \ , \\ (\deg_x f(x, y, t), \deg_y f(x, y, t), \deg_t f(x, y, t)) \in \Gamma_f \ , \tag{10}$$

   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 $m(x, y, t) = \sum_{(i,j,k)\in\Gamma_m} c_{ijk} x^i y^j t^k$.

Condition (10) implies the following inequality:

$$\deg(m(u_x(t), u_y(t), t)) < \deg(f(u_x(t), u_y(t), t)) \ . \tag{11}$$

Also, we see that $m(x, y, t)$ and $f(x, y, t)$ have at least one term divisible by any terms of $X(x, y, t)$.

First we define a set of polynomials D (i.e. secret key) and then construct X containing D as a section. (Details are explained in Sect. 4.3.) For security reasons, we assume that the general fiber of X is not a rational curve. This can be realized, for instance, by letting $\deg_x X(x, y, t) > 2$ and $\deg_y X(x, y, t) > 2$.

4.2 Encryption/Decryption

Encryption. Let m be a plaintext, and divide m into small blocks as $m = m_{00}||\cdots||m_{ij}||\cdots||m_{IJ}$ where

$$\forall (i,j) \in \Lambda_m, \quad |m_{ij}| \leq (|p|-1)(\deg m_{ij}(t)+1) \ .$$

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 plaintext 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 random polynomials $r_0(x,y,t)$ and $r_1(x,y,t)$ 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 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 polynomial $F(x,y,t)$ by

$$\begin{aligned} F_0(x,y,t) &= m(x,y,t) + f(x,y,t)s_0(x,y,t) + X(x,y,t)r_0(x,y,t) \ , \\ F_1(x,y,t) &= m(x,y,t) + f(x,y,t)s_1(x,y,t) + X(x,y,t)r_1(x,y,t) \ . \end{aligned} \tag{12}$$

Decryption. Note that the section D satisfies $X(u_x(t), u_y(t), t) = 0$ as they are on the surface X.

1. Substitute D into $F_i(x,y,t)$:

$$\begin{aligned} h_0(t) &= F_0(u_x(t), u_y(t), t) \\ &= m(u_x(t), u_y(t), t) + f(u_x(t), u_y(t), t)s_0(u_x(t), u_y(t), t) \ , \\ h_1(t) &= F_1(u_x(t), u_y(t), t) \\ &= m(u_x(t), u_y(t), t) + f(u_x(t), u_y(t), t)s_1(u_x(t), u_y(t), t) \ . \end{aligned}$$

2. Compute $h_0(t) - h_1(t)$:

$$h_0(t) - h_1(t) = f(u_x(t), u_y(t), t)\{s_0(u_x(t), u_y(t), t) - s_1(u_x(t), u_y(t), t)\} \ . \tag{13}$$

3. Factor $h_0(t) - h_1(t)$.

4. Find a factor of $h_0(t) - h_1(t)$ whose degree matches $\deg f(u_x(t), u_y(t), t)$. (This degree can be calculated from the initial setting of $f(x, y, t)$ and $D = (u_x(t), u_y(t), t)$.)
5. Compute $h_0(t) \equiv m(u_x(t), u_y(t), t) \pmod{f(u_x(t), u_y(t), t)}$ (cf. (11))
6. Extract the coefficient $m_{ij}(t)$ from $m(x, y, t)$ by solving linear equations. Let $m(x, y, t) = \sum_{(i,j,k)\in\Gamma_m} m_{ijk} x^i y^j t^k$, where m_{ijk}'s are variables. Construct linear equations by comparing the coefficients of t in

$$m(u_x(t), u_y(t), t) = \sum_{(i,j,k)\in\Gamma_m} m_{ijk} u_x(t)^i u_y(t)^j t^k \ .$$

   The left-hand side is given in 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 to Step 4.

In Step 4, we may not always extract $f(u_x(t), u_y(t), t)$ exactly, since the factor of degree equal to $\deg f(u_x(t), u_y(t), t)$ is not always unique. If this happens, then we repeat Steps 4 to 7 until MAC is authenticated.

We note that $\deg m(u_x(t), u_y(t), t)$ and $\deg f(u_x(t), u_y(t), t)$ are fixed. If the difference $\deg(f(u_x(t), u_y(t), t)) - \deg(m(u_x(t), u_y(t), t))$ in (11) is set large, then we have a good chance to find $f(u_x(t), u_y(t), t)$ immediately.

Remark 1. In the decryption process, some factorizations of polynomials in t can be rather time-consuming and Step 4 involves a knapsack problem. But, as we noted above, it is not an arbitrary knapsack problem, and so we can keep the entire algorithm practical. (The exact complexity of the decryption algorithm is under evaluation now and will be discussed elsewhere.)

4.3 Key Generation

Generation of Algebraic Surfaces. Let $X(x, y, t) = 0$ be a surface given by

$$X(x, y, t) = \sum_{(i,j)\in\Lambda_X} c_{ij}(t) x^i y^j \ .$$

1. Randomly choose a set of polynomials $(u_x(t), u_y(t))$ as a section.
2. Randomly choose polynomials $c_{ij}(t)$ with $(i, j) \neq (0, 0)$ and calculate $c_{00}(t)$ by

$$c_{00}(t) = - \sum_{(i,j)\in\Lambda_X\setminus\{(0,0)\}} c_{ij}(t) u_x(t)^i u_y(t)^j \ .$$

The Form of $m(x, y, t)$ and $f(x, y, t)$. We describe a method of determining $\deg f_{ij}(t)$ and $\deg m_{ij}(t)$. The form of $f(x, y, t)$ which satisfies (10) can be defined easily from the information of $X(x, y, t)$. Λ_m can be determined as a subset of $\Lambda_X \Lambda_f$ in (10). To find a plaintext efficiently, linear equations established in decryption step 6 should have a unique solution. In Step 6, we construct equations as follows

$$A \begin{pmatrix} m_{000} \\ m_{001} \\ m_{002} \\ \vdots \\ m_{ijk} \\ \vdots \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_K \end{pmatrix} , \tag{14}$$

where $c_0, \cdots, c_K$ are coefficients of

$$m(u_x(t), u_y(t), t) = \sum_{\tau=0}^{K} c_\tau t^\tau \ .$$

The equations (14) have a unique solution, if and only if $\mathrm{rank}\,(A) = n$, where n denotes the number of variable m_{ijk}'s. Hence we must return to the determining process of the form of $f(x, y, t)$, if $\mathrm{rank}\,(A) < n$.

5 Security Analysis

In this section, we will discuss about the resistance of our system against various types of attacks.

5.1 Reduction to a Multivariate Equation System

When we solve $F_0(x, y, t) - F_1(x, y, t) = f(x, y, t)s(x, y, t) + X(x, y, t)r(x, y, t)$, an obvious way is to let

$$\begin{aligned} f(x, y, t) &= \textstyle\sum_{(i,j,k)\in\Gamma_f} a_{ijk} x^i y^j t^i \ , \\ s(x, y, t) &= \textstyle\sum_{(i,j,k)\in\Gamma_X} b_{ijk} x^i y^j t^k \ , \\ r(x, y, t) &= \textstyle\sum_{(i,j,k)\in\Gamma_f} c_{ijk} x^i y^j t^k \ , \end{aligned}$$

and consider a multivariate equation system in a_{ijk}, b_{ijk} and c_{ijk}. If there exists a solution to this system, then we can obtain exact $f(x, y, t)$. Then we may have $m(x, y, t)$ by using ideal (f, X). But, as $\#\Gamma_f$ and $\#\Gamma_X$ increase, finding a solution to this system becomes considerably difficult, even if c_{ijk}'s are eliminated by substituting rational points of $X(x, y, t)$. For instance, if $\#\Gamma_f > 50$ and $\#\Gamma_X > 50$, then the system contains more than 100 variables. Hence it becomes computationally intractable when we choose a sufficiently large $\#\Gamma_f$ and $\#\Gamma_X$.

5.2 Reduction by the Defining Equation

One can try to divide $F_0(x, y, t) - F_1(x, y, t)$ by $X(x, y, t)$ to find a common divisor $f(x, y, t)$ in the possible remainders. But $f(x, y, t)$ does not appear in these remainders since $m(x, y, t)$ and $f(x, y, t)$ have at least one term divisible by any terms of $X(x, y, t)$; this is due to (10).

5.3 Reduction by Substituting Various Curves

Among the affine curves in $\mathbb{A}^3$, there are many rational curves parameterized in such a way as

$$(x, y, t) = (u_x(\omega), u_y(\omega), u_t(\omega)) \ .$$

If one can find such curves on X, then he can use them for the sections of X and decode the ciphertext in the same way as we decipher it using sections. We show, however, that finding such curves on X is as difficult as finding sections on X. We explain this according to $\deg u_t(\omega)$.

(i) Case $\deg u_t(\omega) \geq 2$

This is part of the divisor finding problem on X. As we assume the difficulty of it, such parameterized curves cannot be found easily.

(ii) Case $\deg u_t(\omega) = 1$

This is equivalent to finding sections on X, and hence it is difficult to find such curves on X.

(iii) Case $\deg u_t(\omega) = 0$

This means that t is set to be some constant value and we try to find a parameterized curve in ω. As we assume that the general fibers of X are non-rational (cf. Sect. 4.1), only singular fibers may contain rational curves. Hence we look for a singular fiber containing a rational curve.

One can find singular fibers by solving a system of equations $\partial X/\partial x = \partial X/\partial y = 0$ consisting of partial derivatives of $X(x, y, t) = 0$ with respect to x and y. But, as we raise the degree of X, this becomes considerably difficult. Also, no efficient algorithm is known for determining whether or not a singular fiber contains a rational curve. Even if it contains a rational curve, finding a parameterization by ω is a divisor finding problem and is known to be difficult. Therefore the attack by substituting rational curves does not seem to be effective.

5.4 Reduction to a Function Field $\mathbb{F}_p(t)$ by the Trace Map

As we explained in Sect. 3.5, Voloch's attack by the trace map (at least in the original form) does not work on ASC.

5.5 Voloch's New Attack

Previously, our ASC was announced in SCIS 2008 (cf. [AG07]) and soon after, Voloch communicated to us with a new attack that uses rational points on surfaces over finite fields; see [Vol]. The attacking procedure is described as follows:

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

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

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 $g_{ijk} \in \mathbb{F}_p$:
$$g(x_\ell, y_\ell, t_\ell) = F(x_\ell, y_\ell, t_\ell) \quad (\ell = 1, \cdots, n) \ . \tag{15}$$
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 $m(x,y,t)$.

Effectiveness of Voloch's Rational Point Attack. The above new attack requires many rational points on $X(x,y,t) = 0$, which can be obtained by raising the field of definition for $X(x,y,t) = 0$. However, we claim that no matter how many rational points we use, the polynomials $f(x,y,t)$ and $m(x,y,t)$ cannot be determined uniquely. In fact, if $g_0(x,y,t)$ is a solution to (15), then for any polynomial $r(x,y,t)$, $g_0(x,y,t) + X(x,y,t)r(x,y,t)$ also serves as a solution. Hence by raising the number of monomials in $r(x,y,t)$ (which is the same as in $f(x,y,t)$), we have too many candidates for $g(x,y,t)$ in the decryption process. More precisely, if γ denotes the number of monomials in $r(x,y,t)$, then there are p^γ candidates for $g(x,y,t)$. Therefore, for instance, by choosing γ that satisfies (16), we may avoid Voloch's rational point attack:
$$p^\gamma > 2^{100} \tag{16}$$
It is not difficult to create the situation with (16).

6 Key Size Estimation

Finally, we discuss the public and secret key sizes to keep the ASC sufficiently secure. ASC has four parameters d (maximal degree of the polynomials defining a section), $w = \deg_{xy} X(x,y,t)$, k (number of terms in $X(x,y,t)$ respect to x and y) and p (size of finite fields). Now we assume $p = 2$ to compare with the case of HFE.

In the case of $w \leq 4$, surfaces X are very likely to be elliptic or rational surfaces whose sections are known well. So w must be greater than or equal to 5 to avoid this case. Also, d must be greater than or equal to 50 to avoid the attack by Faugère et al. in [FJ03].

These observations suggest that the secret key size must be larger than 100 bits. A public key $X(x,y,t)$ contains coefficients $a_1(t), \cdots, a_k(t)$. The degrees of $c_{00}(t)$ can be set equal to dw by the key generation algorithm, if the coefficient of $x^{\deg_x X} y^{\deg_y X}$ is constant. So the public-key size can be set less than or equal to $(k-1)dw$ in size. The lower bound of k is 3, since the key generation algorithm requires a constant term. So the public-key size is presented in the linear from of d. Hence a lower bound for the public-key size is 500 bits, which is much smaller than HFE.

7 Conclusion

This paper has proposed a new type of public-key cryptosystem whose security is based on a section finding problem on algebraic surfaces. The section finding problem has no known efficient algorithm to solve other than finding roots of a multivariable equation system that is NP-complete in general. We show that our system requires only $O(n)$ bit key size that is much smaller than other post-quantum cryptosystems.

Acknowledgments

We thank Felipe Voloch for communicating us with his attacks on our cryptosystems at earlier stages. We also thank Shinji Miura, Shigenori Uchiyama and Hiroo Tokunaga for useful comments and discussions. We are grateful to Jintai Ding and Tatsuaki Okamoto for their constant encouragement. Many thanks are due to the referees for helpful comments and suggestions.

References

[AG04] Akiyama, K., Goto, Y.: An Algebraic Surface Public-key Cryptosystem. IEICE Tech. Report, vol. 104(421), pp. 13–20 (2004)

[AG06] Akiyama, K., Goto, Y.: A Public-key Cryptosystem using Algebraic Surfaces. In: Proc. of PQCrypto 2006, pp. 119–138 (2006)

[AG07] Akiyama, K., Goto, Y.: An improvement of the algebraic surface public-key cryptosystem. In: Proc. of SCIS 2008, CD-ROM 1F1-2 (2008)

[FJ03] Faugère, J.-C., Joux, A.: Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using gröbner bases. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer, Heidelberg (2003)

[Iw08] Iwami, M.: A Reduction Attack on Algebraic Surface Public-Key Cryptosystems. In: Kapur, D. (ed.) ASCM 2007. LNCS, vol. 5081, pp. 323–332. Springer, Heidelberg (2008)

[Kob98] Koblitz, N.: Algebraic Aspects of Cryptography. Springer, Heidelberg (1998)

[Shr] Shor, P.W.: Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In: Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, pp. 124–134 (1994)

[UT] Uchiyama, S., Tokunaga, H.: On the Security of the Algebraic Surface Public-key Cryptosystems (in Japanese). In: Proc. of SCIS 2007, CD-ROM 2C1-2 (2007)

[Vol] Voloch, F.: Breaking the Akiyama-Goto algebraic surface cryptosystem. Arithmetic, Geometry, Cryptography and Coding Theory, CIRM meeting (2007)

[GJ] Garey, M.R., Johnson, D.S.: Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman, New York (1979)

[Szp] Szpiro, L.: Seminaire sur les pinceaux de courbes de genre au moins deux. Asterisque 86(3), 44–78 (1981)

A Toy Example

We give an example of the algebraic surface cryptosystem described in this paper. This example is intended mainly to demonstrate our algorithm explicitly. The security of the system is not fully guaranteed; in practice, we should use more complicated polynomials.

Set $k = \mathbb{F}_{17}$ (i.e. $p = 17$).

A.1 Key Generation

Choose $u_x(t) = 14\,t^3 + 12\,t^2 + 5\,t + 1$ and $u_y(t) = 11\,t^3 + 3\,t^2 + 5\,t + 4$. Let D be a parameterized curve

$$D : (u_x(t), u_y(t), t) = (14\,t^3 + 12\,t^2 + 5\,t + 1, 11\,t^3 + 3\,t^2 + 5\,t + 4, t)\ . \qquad (17)$$

An algebraic surface X having D as a section is constructed as follows:

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

We fix the form of a plain-text polynomial $m(x, y, t)$ and a divisor polynomial $f(x, y, t)$ as follows, where $\mathfrak{F}_m = \{(0, 0) = 17, (4, 4) = 17\}$ for instance means that the index set of $m(x, y, t)$ is $\Lambda_m = \{(0, 0), (4, 4)\}$ and $\deg m_{00}(t) = 17$ and $\deg m_{44}(t) = 17$:

$$\begin{aligned}\mathfrak{F}_X &= \{(0,0) = 16, (1,2) = 2, (3,2) = 1\},\\ \mathfrak{F}_f &= \{(0,0) = 13, (1,2) = 11, (5,5) = 18\},\\ \mathfrak{F}_m &= \{(0,0) = 17, (4,4) = 17\}.\end{aligned}$$

The polynomials $X(x, y, t)$, $f(x, y, t)$ and $m(x, y, t)$ thus constructed satisfy (10) and (16).

A.2 Encryption

For example, a plain text $m = 0xb3f25a22d683a10b362bc3e17a6b832794f5$ can be embedded into a polynomial $m(x, y, t)$ as

$$\begin{aligned}m(x,y,t) = {} & (5\,t^{17} + 15\,t^{16} + 4\,t^{15} + 9\,t^{14} + 7\,t^{13} + 2\,t^{12} + 3\,t^{11} + 8\,t^{10} + 11\,t^9 +\\ & 6\,t^8 + 10\,t^7 + 7\,t^6 + t^5 + 14\,t^4 + 3\,t^3 + 12\,t^2 + 11\,t + 2)x^4y^4 + 6\,t^{17} +\\ & 3\,t^{16} + 11\,t^{15} + t^{13} + 10\,t^{12} + 3\,t^{11} + 8\,t^{10} + 6\,t^9 + 13\,t^8 + 2\,t^7 +\\ & 2\,t^6 + 10\,t^5 + 5\,t^4 + 2\,t^3 + 15\,t^2 + 3\,t + 11.\end{aligned}$$

Then choose randomly an irreducible polynomial $f(x, y, t)$ as

$$\begin{aligned}f(x,y,t) = {} & (t^{18} + 8\,t^{17} + 8\,t^{16} + 6\,t^{15} + 3\,t^{14} + 11\,t^{13} + 12\,t^{12} + 9\,t^{11} + 14\,t^{10} +\\ & 8\,t^9 + 11\,t^8 + 10\,t^7 + 7\,t^6 + 8\,t^5 + 16\,t^4 + 10\,t^3 + 12\,t^2 + 7\,t + 16)x^5y^5 +\\ & (7\,t^{11} + 2\,t^{10} + 16\,t^9 + 16\,t^8 + 2\,t^7 + 4\,t^6 + 4\,t^5 + 9\,t^4 + 9\,t^3 + t^2 +\\ & 7\,t + 14)xy^2 + 8\,t^{13} + 12\,t^{12} + 15\,t^{11} + 5\,t^9 + 12\,t^8 + 13\,t^7 + 6\,t^6 +\\ & 6\,t^5 + 2\,t^4 + 13\,t^3 + 14\,t^2 + 14\,t + 11.\end{aligned}$$

Also, we may choose $s_i(x,y,t)$ and $r_i(x,y,t)$ as

$$\begin{aligned}
s_1(x,y,t) = {} & (4\,t+2)x^3y^2+(16\,t^2+9\,t+4)xy^2+8\,t^{16}+4\,t^{15}+11\,t^{14}+7\,t^{13}+t^{12}+\\
& 11\,t^{10}+8\,t^9+13\,t^8+12\,t^7+14\,t^6+16\,t^5+8\,t^4+13\,t^3+16\,t^2+14\,t+4,
\end{aligned}$$

$$\begin{aligned}
s_2(x,y,t) = {} & (7\,t+11)x^3y^2+(11\,t^2+3\,t+3)xy^2+t^{16}+3\,t^{15}+13\,t^{14}+t^{13}+\\
& 3\,t^{12}+16\,t^{11}+9\,t^{10}+4\,t^9+12\,t^7+t^6+7\,t^5+t^4+4\,t^3+2\,t+1,
\end{aligned}$$

$$\begin{aligned}
r_1(x,y,t) = {} & (10\,t^{18}+3\,t^{17}+7\,t^{16}+t^{15}+10\,t^{14}+10\,t^{13}+5\,t^{12}+7\,t^{11}+15\,t^{10}+\\
& 10\,t^9+8\,t^8+2\,t^7+16\,t^6+4\,t^4+t^3+3\,t^2+16\,t+2)x^5y^5+(t^{11}+\\
& 10\,t^{10}+14\,t^9+10\,t^8+2\,t^7+4\,t^6+13\,t^5+6\,t^4+10\,t^3+10\,t^2+\\
& 4\,t+15)xy^2+5\,t^{13}+16\,t^{12}+t^{11}+8\,t^{10}+8\,t^9+3\,t^8+3\,t^7+5\,t^6+\\
& 3\,t^5+3\,t^4+9\,t^3+7\,t^2+t+15,
\end{aligned}$$

$$\begin{aligned}
r_2(x,y,t) = {} & (12\,t^{18}+2\,t^{17}+7\,t^{16}+6\,t^{15}+8\,t^{14}+9\,t^{13}+16\,t^{12}+4\,t^{11}+8\,t^8+\\
& 8\,t^7+10\,t^6+13\,t^5+12\,t^4+11\,t^3+8\,t^2+4\,t+16)x^5y^5+(t^{11}+\\
& 8\,t^{10}+2\,t^9+t^8+4\,t^7+2\,t^6+8\,t^5+4\,t^4+13\,t^3+15\,t^2+2\,t+\\
& 8)xy^2+16\,t^{13}+6\,t^{12}+t^{11}+11\,t^{10}+16\,t^9+4\,t^8+2\,t^7+14\,t^6+\\
& 3\,t^5+7\,t^4+13\,t^3+13\,t^2+8\,t+16,
\end{aligned}$$

where $r_i(x,y,t)$ satisfies the condition of a divisor polynomial, $s_i(x,y,t)$ is in the same form as $X(x,y,t)$. Expanding $F_i(x,y,t)$, we obtain the following polynomial:

$$\begin{aligned}
F_0(x,y,t) = {} & (14\,t^{19}+t^{18}+9\,t^{16}+10\,t^{15}+7\,t^{14}+5\,t^{13}+15\,t^{12}+6\,t^{11}+16\,t^{10}+\\
& 15\,t^9+8\,t^8+16\,t^7+2\,t^6+16\,t^5+11\,t^4+13\,t^3+13\,t^2+2\,t+1)x^8y^7+\\
& (6\,t^{20}+3\,t^{18}+5\,t^{17}+6\,t^{16}+2\,t^{15}+7\,t^{13}+16\,t^{12}+5\,t^{11}+t^{10}+11\,t^9+\\
& 4\,t^8+11\,t^7+8\,t^6+6\,t^5+9\,t^4+14\,t^3+13\,t^2+12\,t+4)x^6y^7+(4\,t^{34}+\\
& 4\,t^{33}+10\,t^{32}+13\,t^{31}+2\,t^{30}+11\,t^{29}+3\,t^{28}+15\,t^{27}+7\,t^{25}+13\,t^{24}+\\
& 4\,t^{23}+6\,t^{21}+4\,t^{20}+t^{18}+15\,t^{17}+6\,t^{16}+16\,t^{15}+15\,t^{14}+7\,t^{13}+\\
& 14\,t^{11}+12\,t^{10}+8\,t^9+9\,t^8+6\,t^7+6\,t^6+10\,t^5+14\,t^4+2\,t^3+4\,t^2+t+\\
& 7)x^5y^5+(5\,t^{17}+15\,t^{16}+4\,t^{15}+9\,t^{14}+7\,t^{13}+14\,t^{12}+11\,t^{11}+3\,t^{10}+\\
& 2\,t^9+12\,t^8+3\,t^7+16\,t^6+11\,t^5+2\,t^4+16\,t^3+10\,t^2+10)x^4y^4+\\
& (3\,t^{14}+11\,t^{13}+7\,t^{12}+14\,t^{11}+6\,t^{10}+5\,t^9+7\,t^8+4\,t^6+2\,t^5+10\,t^4+\\
& 9\,t^3+2\,t^2+12\,t+2)x^3y^2+(9\,t^{13}+7\,t^{12}+5\,t^{11}+9\,t^{10}+7\,t^9+9\,t^8+\\
& 12\,t^7+8\,t^6+2\,t^5+13\,t^4+8\,t^3+4\,t^2+3\,t+14)x^2y^4+(8\,t^{27}+14\,t^{26}+\\
& 8\,t^{25}+16\,t^{24}+16\,t^{23}+13\,t^{22}+6\,t^{21}+13\,t^{20}+10\,t^{19}+4\,t^{18}+10\,t^{17}+\\
& 10\,t^{16}+13\,t^{15}+11\,t^{14}+14\,t^{13}+14\,t^{12}+15\,t^{11}+4\,t^{10}+11\,t^9+\\
& 13\,t^8+5\,t^7+4\,t^6+10\,t^5+13\,t^4+3\,t^3+2\,t^2+16\,t+13)xy^2+11\,t^{29}+\\
& 12\,t^{28}+10\,t^{27}+t^{26}+14\,t^{25}+16\,t^{24}+12\,t^{23}+14\,t^{22}+14\,t^{21}+11\,t^{20}+\\
& 7\,t^{19}+15\,t^{18}+6\,t^{17}+16\,t^{16}+15\,t^{15}+10\,t^{14}+4\,t^{13}+7\,t^{12}+16\,t^{11}+\\
& 11\,t^{10}+8\,t^9+2\,t^8+16\,t^7+t^6+12\,t^5+3\,t^4+13\,t^3+12\,t^2+5\,t+10,
\end{aligned}$$

$$\begin{aligned}
F_1(x,y,t) = {} & (2\,t^{19}+2\,t^{18}+t^{17}+2\,t^{16}+2\,t^{15}+12\,t^{14}+5\,t^{13}+2\,t^{12}+16\,t^{11}+\\
& 6\,t^{10}+3\,t^9+7\,t^8+11\,t^7+8\,t^6+2\,t^5+3\,t^4+6\,t^3+10\,t^2+7\,t+\\
& 13)x^8y^7+(16\,t^{20}+3\,t^{19}+12\,t^{17}+t^{16}+15\,t^{15}+15\,t^{14}+6\,t^{13}+\\
& 3\,t^{12}+3\,t^{11}+9\,t^{10}+11\,t^9+14\,t^8+7\,t^7+t^5+4\,t^4+t^3+5\,t^2+10\,t+\\
& 10)x^6y^7+(3\,t^{34}+11\,t^{33}+8\,t^{31}+11\,t^{30}+11\,t^{29}+4\,t^{28}+5\,t^{27}+t^{26}+
\end{aligned}$$

$$4\,t^{25}+3\,t^{24}+9\,t^{23}+5\,t^{22}+7\,t^{21}+16\,t^{20}+4\,t^{19}+10\,t^{18}+7\,t^{17}+9\,t^{16}+15\,t^{15}+13\,t^{14}+8\,t^{13}+9\,t^{12}+10\,t^{11}+10\,t^{10}+3\,t^{9}+14\,t^{7}+15\,t^{6}+4\,t^{5}+11\,t^{4}+2\,t^{3}+7\,t^{2}+t+2)x^5y^5+(5\,t^{17}+15\,t^{16}+4\,t^{15}+9\,t^{14}+7\,t^{13}+t^{12}+10\,t^{11}+3\,t^{10}+14\,t^{9}+6\,t^{8}+5\,t^{6}+5\,t^{5}+8\,t^{4}+16\,t^{3}+3\,t^{2}+10\,t+15)x^4y^4+(4\,t^{14}+15\,t^{13}+9\,t^{12}+16\,t^{11}+8\,t^{10}+14\,t^{9}+10\,t^{8}+15\,t^{7}+13\,t^{6}+15\,t^{5}+9\,t^{4}+10\,t^{3}+16\,t^{2}+4\,t+9)x^3y^2+(8\,t^{13}+8\,t^{12}+6\,t^{11}+3\,t^{10}+10\,t^{9}+9\,t^{8}+16\,t^{7}+13\,t^{6}+15\,t^{5}+4\,t^{4}+7\,t^{3}+6\,t^{2}+8\,t+6)x^2y^4+(10\,t^{27}+4\,t^{26}+9\,t^{25}+7\,t^{24}+3\,t^{23}+13\,t^{22}+16\,t^{21}+14\,t^{20}+t^{19}+t^{17}+6\,t^{16}+11\,t^{15}+9\,t^{14}+2\,t^{13}+16\,t^{12}+9\,t^{11}+16\,t^{10}+13\,t^{9}+2\,t^{7}+2\,t^{6}+14\,t^{5}+6\,t^{4}+15\,t^{3}+6\,t^{2}+14\,t+2)xy^2+5\,t^{29}+12\,t^{28}+6\,t^{27}+14\,t^{26}+5\,t^{25}+10\,t^{24}+12\,t^{23}+t^{22}+8\,t^{21}+2\,t^{20}+15\,t^{19}+3\,t^{18}+5\,t^{17}+14\,t^{15}+7\,t^{14}+5\,t^{13}+2\,t^{12}+9\,t^{11}+7\,t^{10}+11\,t^{9}+3\,t^{8}+10\,t^{7}+7\,t^{6}+14\,t^{4}+t^{3}+8\,t^{2}+6\,t+8.$$

A.3 Decryption

Substituting the section defined in (17) into $F_i(x,y,t)$ $(i=0,1)$, we obtain

$$\begin{aligned} h_0(t) &= F_0(u_x(t),u_y(t),t)\\ &= 13\,t^{64}+8\,t^{63}+8\,t^{62}+13\,t^{61}+7\,t^{60}+16\,t^{58}+10\,t^{57}+13\,t^{56}+6\,t^{55}+3\,t^{54}+15\,t^{53}+3\,t^{52}+t^{51}+4\,t^{50}+2\,t^{49}+5\,t^{48}+12\,t^{47}+3\,t^{46}+8\,t^{44}+14\,t^{43}+9\,t^{42}+13\,t^{41}+14\,t^{40}+10\,t^{39}+8\,t^{38}+11\,t^{37}+12\,t^{36}+9\,t^{35}+7\,t^{33}+14\,t^{32}+12\,t^{31}+8\,t^{30}+4\,t^{28}+9\,t^{27}+15\,t^{26}+t^{25}+4\,t^{24}+8\,t^{23}+5\,t^{22}+14\,t^{21}+3\,t^{20}+7\,t^{19}+6\,t^{18}+7\,t^{17}+16\,t^{16}+9\,t^{15}+6\,t^{13}+3\,t^{12}+8\,t^{11}+11\,t^{10}+11\,t^{9}+14\,t^{8}+11\,t^{7}+15\,t^{6}+14\,t^{5}+2\,t^{4}+10\,t^{3}+10\,t^{2}+t+10, \end{aligned}$$

$$\begin{aligned} h_1(t) &= F_1(u_x(t),u_y(t),t)\\ &= 14\,t^{64}+6\,t^{63}+6\,t^{62}+8\,t^{61}+7\,t^{60}+t^{59}+4\,t^{58}+t^{57}+7\,t^{56}+11\,t^{55}+10\,t^{54}+2\,t^{53}+13\,t^{52}+16\,t^{51}+14\,t^{50}+15\,t^{49}+3\,t^{48}+3\,t^{46}+t^{45}+11\,t^{44}+10\,t^{43}+13\,t^{42}+8\,t^{41}+6\,t^{40}+9\,t^{39}+4\,t^{38}+13\,t^{37}+16\,t^{36}+13\,t^{35}+12\,t^{34}+t^{33}+t^{32}+6\,t^{31}+15\,t^{30}+15\,t^{29}+16\,t^{28}+14\,t^{27}+2\,t^{26}+13\,t^{25}+16\,t^{24}+16\,t^{23}+3\,t^{22}+13\,t^{21}+4\,t^{20}+5\,t^{19}+15\,t^{18}+5\,t^{17}+4\,t^{16}+t^{15}+10\,t^{14}+15\,t^{13}+t^{11}+8\,t^{10}+6\,t^{9}+13\,t^{8}+15\,t^{6}+10\,t^{5}+4\,t^{4}+8\,t^{3}+11\,t^{2}+12\,t+2. \end{aligned}$$

Factor $h_1(t)-h_2(t)$. We have

$$\begin{aligned} h_1(t)-h_2(t) = {} & 16\,(t^3+3\,t^2+13\,t+3)(t^4+11\,t^3+15\,t^2+14\,t+13)(t^9+8\,t^8+11\,t^7+3\,t^5+4\,t^4+6\,t^3+14\,t^2+12\,t+13)(t^{17}+2\,t^{16}+14\,t^{15}+5\,t^{14}+5\,t^{13}+8\,t^{12}+9\,t^{11}+11\,t^{10}+3\,t^{9}+13\,t^{8}+10\,t^{7}+8\,t^{6}+15\,t^{5}+7\,t^{4}+12\,t^{3}+10\,t^{2}+3\,t+2)(t^5+13\,t^4+4\,t^3+2\,t^2+4\,t+13)(t^{16}+4\,t^{15}+11\,t^{14}+t^{13}+4\,t^{12}+13\,t^{11}+t^{10}+2\,t^{9}+t^{8}+2\,t^{7}+t^{6}+2\,t^{4}+15\,t^{3}+5\,t^{2}+11\,t+6)(t^6+4\,t^5+3\,t^4+10\,t^3+14\,t^2+2\,t+5)(t^4+4\,t^3+5\,t^2+16\,t+10). \end{aligned}$$

Then we find 4 candidates for $f(u_x(t),u_y(t),t)$ as it should have degree 48. Furthermore, by comparison of the degrees of $m(u_x(t),u_y(t),t)$ and $h_1(t) \pmod{f(t)}$, we can single out the correct $f(u_x(t),u_y(t),t)$ as

$$\begin{aligned} f(u_x(t), u_y(t), t) = {} & (t^3+3\,t^2+13\,t+3)(t^4+11\,t^3+15\,t^2+14\,t+13)(t^5+13\,t^4+ \\ & 4\,t^3+2\,t^2+4\,t+13)(t^6+4\,t^5+3\,t^4+10\,t^3+14\,t^2+2\,t+ \\ & 5)(t^9+8\,t^8+11\,t^7+3\,t^5+4\,t^4+6\,t^3+14\,t^2+12\,t+13)(t^{17}+ \\ & 2\,t^{16}+14\,t^{15}+5\,t^{14}+5\,t^{13}+8\,t^{12}+9\,t^{11}+11\,t^{10}+3\,t^9+ \\ & 13\,t^8+10\,t^7+8\,t^6+15\,t^5+7\,t^4+12\,t^3+10\,t^2+3\,t+2)(t^4+ \\ & 4\,t^3+5\,t^2+16\,t+10) \end{aligned}$$

and we obtain

$$\begin{aligned} m(u_x(t), u_y(t), t) = {} & 5\,t^{41}+10\,t^{40}+9\,t^{38}+9\,t^{36}+5\,t^{35}+12\,t^{34}+14\,t^{33}+9\,t^{31}+ \\ & 6\,t^{30}+t^{29}+t^{27}+7\,t^{26}+10\,t^{25}+3\,t^{24}+10\,t^{23}+13\,t^{22}+ \\ & 4\,t^{21}+10\,t^{20}+11\,t^{19}+6\,t^{18}+4\,t^{17}+5\,t^{16}+7\,t^{15}+14\,t^{14}+ \\ & t^{13}+7\,t^{12}+11\,t^{11}+5\,t^{10}+2\,t^9+8\,t^8+14\,t^7+13\,t^6+12\,t^5+ \\ & 16\,t^4+13\,t^3+9\,t^2+13\,t+13. \end{aligned}$$

Now recall that $m(u_x(t), u_y(t), t)$ has the form

$$\begin{aligned} m(u_x(t), u_y(t), t) = {} & (m_{4,4,17}t^{17} + m_{4,4,16}t^{16} + \cdots + m_{4,4,1}t + \\ & m_{4,4,0})u_x(t)^4u_y(t)^4 + m_{0,0,17}t^{17} + m_{0,0,16}t^{16} + \cdots + \\ & m_{0,0,1}t + m_{0,0,0}. \end{aligned} \tag{18}$$

By comparing two expressions of $m(u_x(t), u_y(t), t)$ above, we create a system of linear equations with variables $m_{i,j,t}$ as follows:

$$\begin{cases} m_{4,4,17} & = 5 \\ m_{4,4,0} + m_{0,0,0} & = 13 \\ 16\,m_{4,4,17} + m_{4,4,16} & = 10 \\ m_{0,0,1} + m_{4,4,1} + 8\,m_{4,4,0} & = 13 \\ \quad\vdots & \\ m_{4,4,15} + 13\,m_{4,4,2} + 14\,m_{4,4,12} + 2\,m_{4,4,8} + 12\,m_{4,4,6} + & \\ 16\,m_{4,4,3}+10\,m_{4,4,13}+13\,m_{4,4,5}+5\,m_{4,4,0}+3\,m_{4,4,1}+m_{4,4,17}+ & \\ m_{4,4,14} + 8\,m_{4,4,16} + m_{0,0,17} & = 4. \end{cases}$$

Solving this, we recover the plaintext polynomial

$$\begin{aligned} m(x, y, t) = {} & (5\,t^{17}+15\,t^{16}+4\,t^{15}+9\,t^{14}+7\,t^{13}+2\,t^{12}+3\,t^{11}+8\,t^{10}+11\,t^9+ \\ & 6\,t^8+10\,t^7+7\,t^6+t^5+14\,t^4+3\,t^3+12\,t^2+11\,t+2)x^4y^4+6\,t^{17}+ \\ & 3\,t^{16}+11\,t^{15}+t^{13}+10\,t^{12}+3\,t^{11}+8\,t^{10}+6\,t^9+13\,t^8+2\,t^7+ \\ & 2\,t^6+10\,t^5+5\,t^4+2\,t^3+15\,t^2+3\,t+11. \end{aligned}$$