TOSHIBA

Leading Innovation

A Survey on the Algebraic Surface Cryptosystems

Koichiro Akiyama (TOSHIBA Corporation)
Joint work with Prof. Yasuhiro Goto

2013/03/02

Contents

1. **Introduction**

   Public key cryptosystem, Motivation

2. **Section Finding Problem**

   A Computational Hard Problem on Algebraic Surface

3. **Algebraic Surface Public-key Cryptosystem**

   Encryption/Decryption/Key Generation Algorithms

4. **Known Attacks**

   －Rational Point Attack

   －Ideal Factorization Attack

5. **Conclusion and Future Research**

Contents

1. **Introduction**

   Public key cryptosystem, Motivation

2. **Section Finding Problem**

   A Computational Hard Problem on Algebraic Surface

3. **Algebraic Surface Public-key Cryptosystem**

   Encryption/Decryption/Key Generation Algorithms

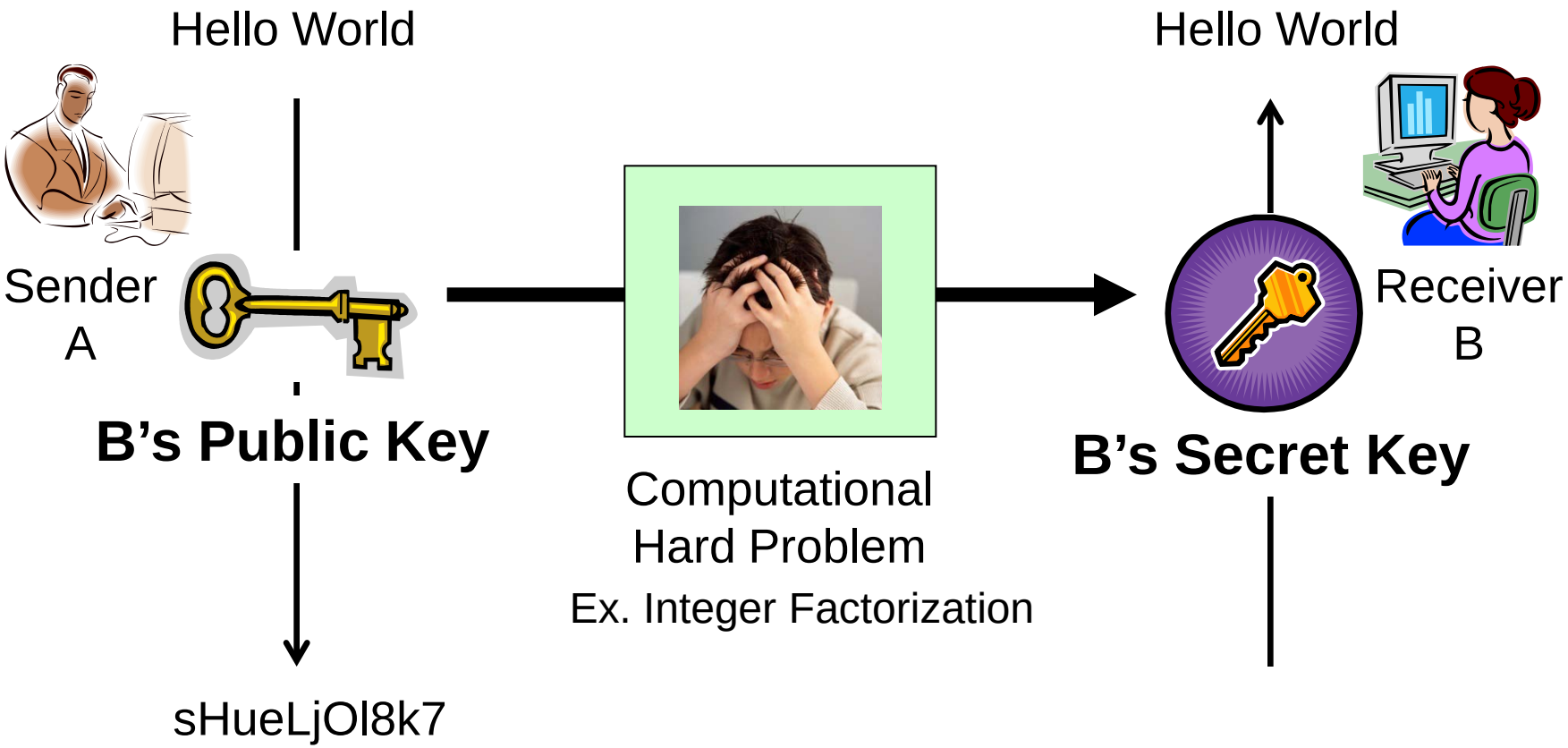
4. **Known Attacks**

   – Rational Point Attack

   – Ideal Factorization Attack

5. **Conclusion and Future Research**

Public key Cryptosystem (Concept)



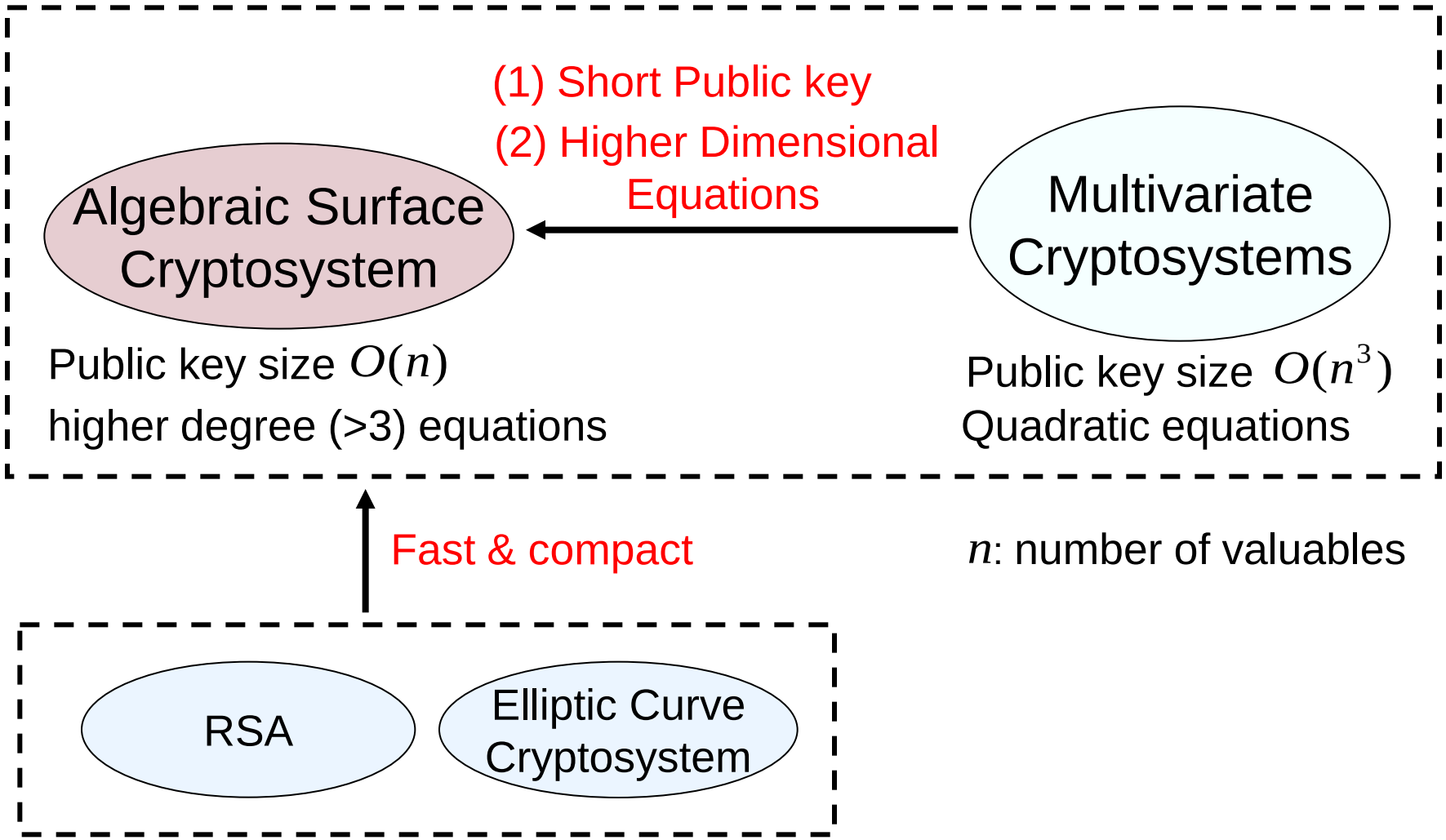
Security of public key cryptosystem relies on the the problem which is hard to compute.

Motivation

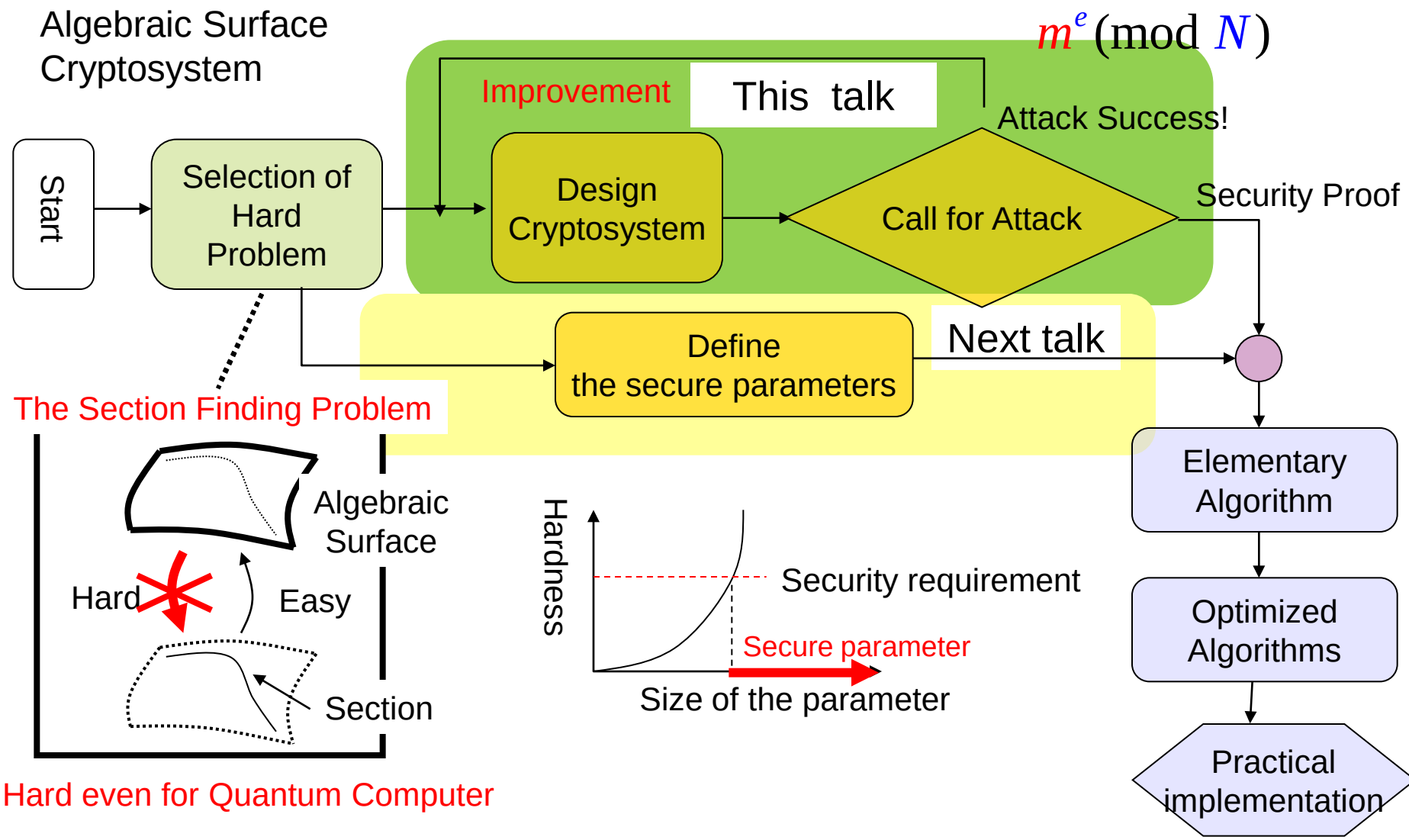
- **Want to construct public-key cryptosystems having following features**
  - Resistant against known attacks by quantum computer.
    (Not based on the factorization or discrete logarithm problems.)
  - Fast in process time & compact in size.
  - Based on a hard problem in algebraic geometry.

⇨ Our target is an algebraic surface

Comparison with other cryptosystems



Construction for Public Key Cryptosystem



Contents

1. **Introduction**

   Public key cryptosystem, Motivation

2. **Section Finding Problem**

   A Computational Hard Problem on Algebraic Surface

3. **Algebraic Surface Public-key Cryptosystem**

   Encryption/Decryption/Key Generation Algorithms

4. **Known Attacks**

   – Rational Point Attack

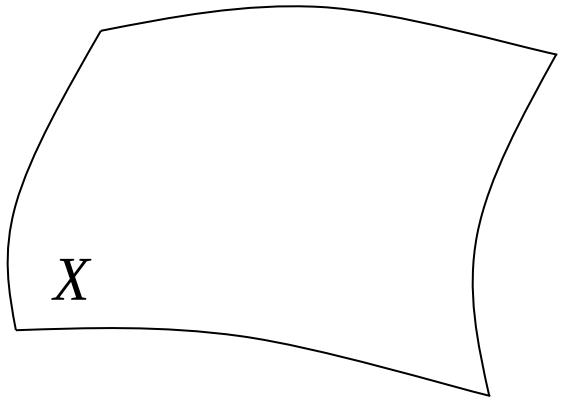
   – Ideal Factorization Attack

5. **Conclusion and Future Research**

Algebraic Surface

An algebraic surface (we use) is
a 2-dimensional affine algebraic variety with fibration.

$$X(x, y, t) = y^5 + 2xy^3 + tx^4 + 5txy + t^3y + t + 5 = 0$$



We consider algebraic surfaces defined over a finite field F_q .

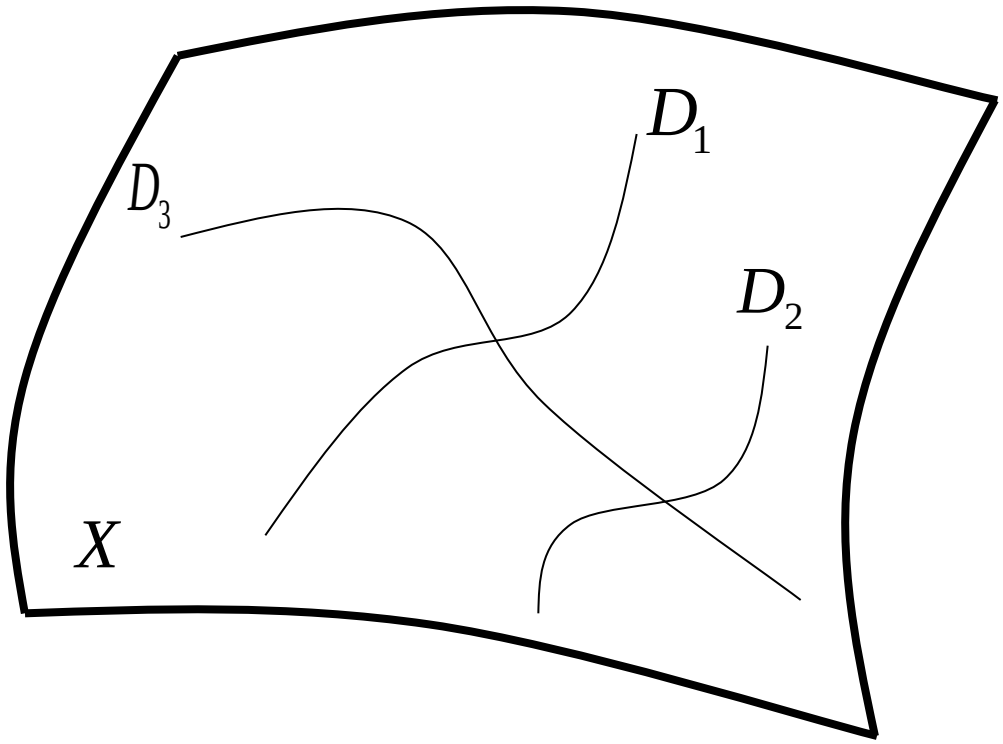
where F_q is small enough to calculate,

but $char(F_q)$ need not be 2.

Section Finding Problem (SFP)

Algebraic Surface

$$X(x,y,t) = 3tx^3y^2 + (t+1)2xy^3 + 4t^3x^2y + 3tx + 1 = 0$$



Algebraic Surface

$$X(x,y,t) = 0$$

hard ↓ ↑ easy

section

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

$$X(u_x(t), u_y(t), t) = 0$$

General Solution of SFP

To solve the SFP, we put the section as follows:

$$u_x(t) = \alpha_d t^d + \cdots + \alpha_1 t + \alpha_0 \quad u_y(t) = \beta_d t^d + \cdots + \beta_1 t + \beta_0$$

($\alpha_0, \alpha_1 \cdots, \alpha_d, \beta_0, \beta_1 \cdots, \beta_d$ are variables)

Substitute $u_x(t), u_y(t)$ into $X(x, y, t) = 0$, we obtain

$$X(u_x(t), u_y(t), t) = \sum_{(i,j,k) \in I} \eta_{ijk} u_x(t)^i u_y(t)^j t^k$$

$$= \sum_{h=0}^{r} c_h(\alpha_0, \cdots, \alpha_d, \beta_0, \cdots, \beta_d) t^h = 0$$

The SFP is reduced to multivariable equations

$$\begin{cases} c_0(\alpha_0, \cdots, \alpha_d, \beta_0, \cdots, \beta_d) = 0 \\ \cdots\cdots\cdots \\ c_r(\alpha_0, \cdots, \alpha_d, \beta_0, \cdots, \beta_d) = 0 \end{cases}$$

$$r = \max\{(i+j)d + k \mid \sum_{u_{ijk} \neq 0} \eta_{ijk} x^i y^j t^k = 0\}$$

Contents

1. **Introduction**

   Public key cryptosystem, Motivation

2. **Section Finding Problem**

   A Computational Hard Problem on Algebraic Surface

3. **Algebraic Surface Public-key Cryptosystem**

   Encryption/Decryption/Key Generation Algorithms

4. **Known Attacks**

   – Rational Point Attack

   – Ideal Factorization Attack

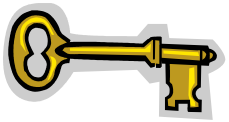
5. **Conclusion and Future Research**

Keys

1. System parameters

- Size of finite field F_p : prime p (example) $p = 5$
- Degree of section : $d = \deg u_x(t) = \deg u_y(t)$

2. Public key



- Algebraic surface

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

- Form of the plaintext polynomial

$$m(x,y,t) = \sum_{(i,j)\in\Lambda_m} m_{ij}(t)x^i y^j \pmod p$$

- Form of the divisor polynomial ($\Lambda_m, \deg m_{ij}(t)$ are given)

$$f(x,y,t) = \sum_{(i,j)\in\Lambda_f} f_{ij}(t)x^i y^j \pmod p$$

($\Lambda_f, \deg f_{ij}(t)$ are given)

3. Secret key

$$\deg_* X(x,y,t) < \deg_* m(x,y,t) < \deg_* f(x,y,t)$$

$$* \in \{x, y, t\}$$

- Section

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

Form of the plaintext polynomial

$$m(x,y,t)=\sum_{(i,j)\in\Lambda_m} m_{ij}(t)x^i y^j \pmod p$$

Λ_m and $\deg m_{ij}(t)$ ($\forall(i,j)\in\Lambda_m$) are designated.

For example,

$$\Lambda_m=\{(3,0),(1,2),(0,0)\}$$

$$\deg m_{30}(t)=2,\deg m_{12}(t)=1,\deg m_{00}(t)=0$$

Form described the formula as fllows:

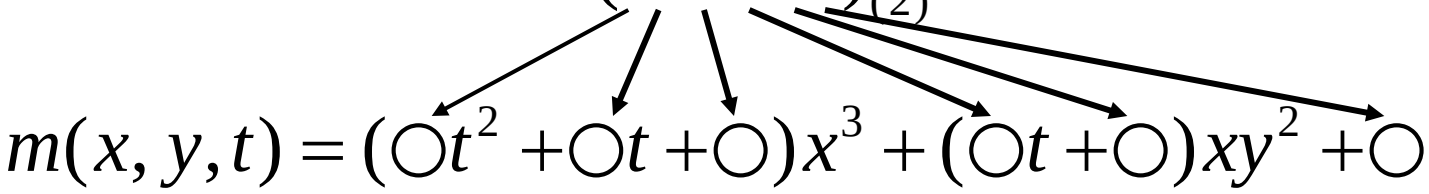
$$m(x,y,t)=(\bigcirc t^2+\bigcirc t+\bigcirc)x^3+(\bigcirc t+\bigcirc)xy^2+\bigcirc$$

○ indicates an element of F_p

How to embed plaintext m into m(x,y,t)

In the case of F_2

$$m = (101101)_{(2)}$$



So the plaintext described as

$$m(x,y,t) = (t^2+1)x^3 + txy^2 + 1$$

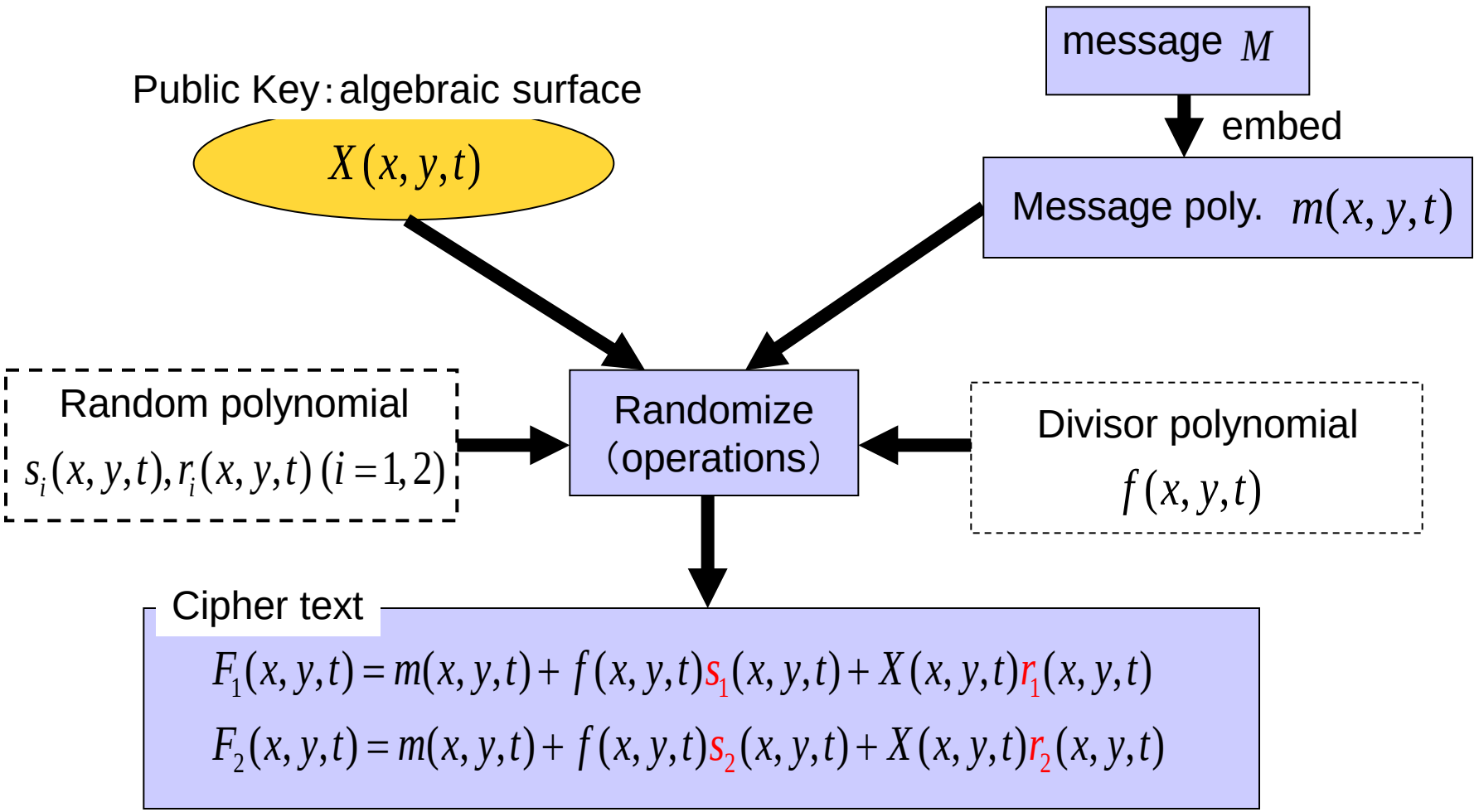
In the case of F_5 plaintext must be divided into 2bits block

$$m = (10|11|01|10|00|10)_{(2)}$$

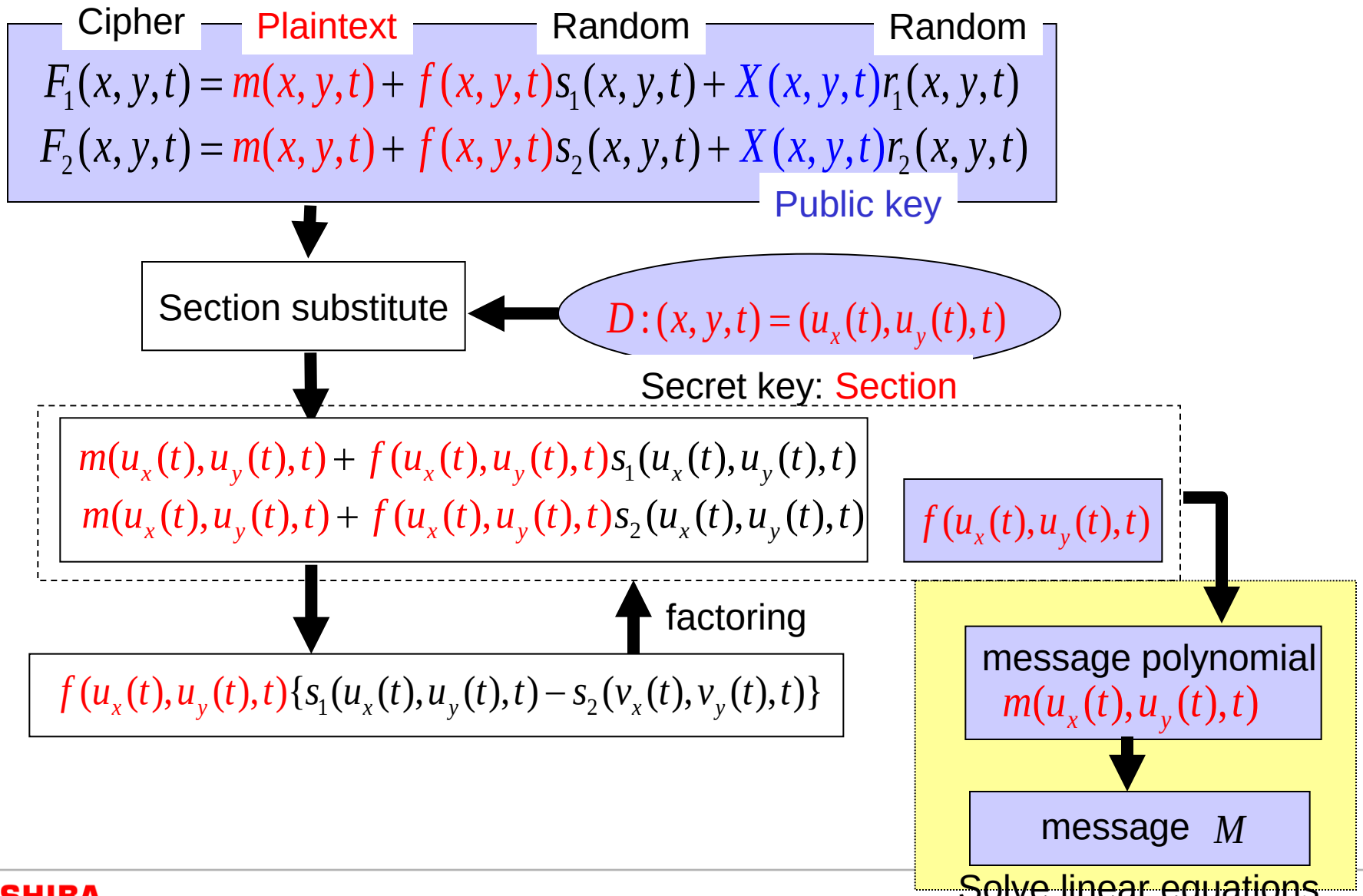
$$m(x,y,t) = (2t^2+3t+1)x^3 + 2txy^2 + 2$$

Therefore m embedded to m(x,y,t) as coefficients

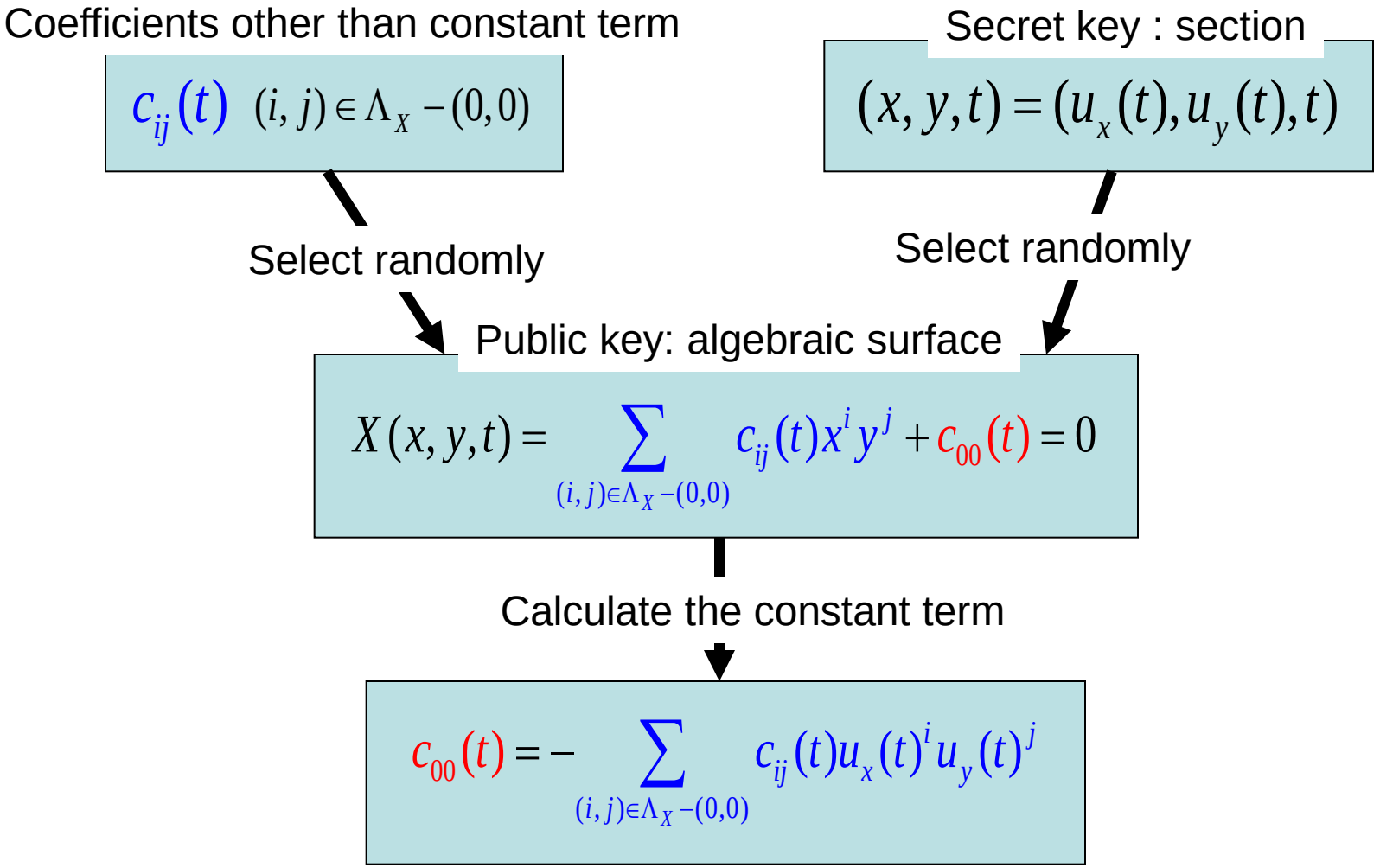
Encryption


Public Key : algebraic surface
$X(x,y,t)$
message M
embed
Message poly. $m(x,y,t)$
Random polynomial
$s_i(x,y,t), r_i(x,y,t)\ (i=1,2)$
Randomize
(operations)
Divisor polynomial
$f(x,y,t)$
Cipher text
$F_1(x,y,t) = m(x,y,t) + f(x,y,t)s_1(x,y,t) + X(x,y,t)r_1(x,y,t)$
$F_2(x,y,t) = m(x,y,t) + f(x,y,t)s_2(x,y,t) + X(x,y,t)r_2(x,y,t)$

Decryption


Cipher
Plaintext
Random
Random
$F_1(x,y,t) = m(x,y,t) + f(x,y,t)s_1(x,y,t) + X(x,y,t)r_1(x,y,t)$
$F_2(x,y,t) = m(x,y,t) + f(x,y,t)s_2(x,y,t) + X(x,y,t)r_2(x,y,t)$
Public key
Section substitute
$D:(x,y,t) = (u_x(t), u_y(t), t)$
Secret key: Section
$m(u_x(t),u_y(t),t) + f(u_x(t),u_y(t),t)s_1(u_x(t),u_y(t),t)$
$m(u_x(t),u_y(t),t) + f(u_x(t),u_y(t),t)s_2(u_x(t),u_y(t),t)$
$f(u_x(t),u_y(t),t)$
factoring
$f(u_x(t),u_y(t),t)\{s_1(u_x(t),u_y(t),t) - s_2(v_x(t),v_y(t),t)\}$
message polynomial
$m(u_x(t),u_y(t),t)$
message M
Solve linear equations

Key generation



Contents

1. **Introduction**

   Public key cryptosystem, Motivation

2. **Section Finding Problem**

   A Computational Hard Problem on Algebraic Surface

3. **Algebraic Surface Public-key Cryptosystem**

   Encryption/Decryption/Key Generation Algorithms

4. **Known Attacks**

   – Rational Point Attack

   – Ideal Factorization Attack

5. **Conclusion and Future Research**

Rational point attack (1)

$$F_1(x,y,t) = m(x,y,t) + f(x,y,t)s_1(x,y,t) + X(x,y,t)r_1(x,y,t)$$
$$F_2(x,y,t) = m(x,y,t) + f(x,y,t)s_2(x,y,t) + X(x,y,t)r_2(x,y,t)$$

Remove the plaintext polynomial

subtract

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

$$F(x,y,t) = F_1(x,y,t) - F_2(x,y,t)$$
where $s(x,y,t) = s_1(x,y,t) - s_2(x,y,t)$
$$r(x,y,t) = r_1(x,y,t) - r_2(x,y,t)$$

Rational point attack (2)

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

rational points (x_n, y_n, t_n) $(X(x_n, y_n, t_n) = 0)$

substitution

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

$$g(x_n, y_n, t_n) = \sum_{(i,j,k)\in\Gamma_g} g_{ijk} x_n{}^i y_n{}^j t_n{}^k = F(x_n, y_n, t_n)$$

Solve Linear Equation

construct

$g(x,y,t)$

factoring

$f(x,y,t)s(x,y,t)$

extract

$f(x,y,t)$

Success!

Rational point attack (3)

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

$$m(x,y,t) = \sum_{(i,j,k)\in\Gamma_m} m_{ijk}x^i y^j t^k \quad (f_{ijk} \in F_p)$$

$$s_1(x,y,t) = \sum_{(i,j,k)\in\Gamma_s} s_{ijk}x^i y^j t^k \quad (s_{ijk} \in F_p)$$

rational points (x_n, y_n, t_n)

$(X(x_n, y_n, t_n) = 0)$

substitution

$$\sum_{(i,j,k)\in\Gamma_m} m_{ijk}x_n{}^i y_n{}^j t_n{}^k + f(x_n,y_n,t_n) \sum_{(i,j,k)\in\Gamma_s} s_{ijk}x_n{}^i y_n{}^j t_n{}^k = F(x_n,y_n,t_n)$$

Solve linear equations

reconstruct

$m(x,y,t)$

Counter measure against RPA

$$F(x,y,t) = \underbrace{f(x,y,t)s(x,y,t)}_{\| \; g(x,y,t)} + X(x,y,t)r(x,y,t)$$

$g(x,y,t)$ and $X(x,y,t)r(x,y,t)$ are in the same form

If $g_0 (= g_0(x,y,t))$ is a solution, there exists polynomial r_0 which is in the same form of f and satisfy $F = g_0 + Xr_0$.

For arbitrary r which is in the same form of f,

$$F = g_0 + Xr_0 = \underbrace{(g_0 + Xr)}_{\text{This is also another solution}} + X(r_0 - r)$$

We can avoid the attack, when we select the form of f which has enough polynomials not to be able to identify the correct one.

Ideal factorization attack

Cipher text

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

Ideal Factoring

$$(F_1 - F_2, X) = I_1 \cap I_2$$

where $I_1 = (f, X),\ I_2 = (s_1 - s_2, X)$

$$J = (F_1, F_2, X) + I_1 = (m, f, X)$$

$m(x,y,t)$

Solve Linear Eq.

$$NF_J(m) = \sum_{(i,j)\in\Lambda_m} \sum_{k=0}^{d_{ij}^{(m)}} m_{ijk} NF_J(x^i y^j t^k) = 0$$

Sequence of events on ASC

Jan 2004 1st version was proposed in domestic conference

May 2006 1st version was presented
in international conference PQC2006
Jintai Ding pointed out a flaw in our system

Oct 2006 2nd version was presented in AMS conference.

Jan 2007 Shigenori Uchiyama proposed an attack against 2nd version

Apr 2007 Felipe Voloch proposed another attack against 2nd version

Jan 2008 3rd version was proposed in domestic conference.

Mar 2009 3rd was presented
in international conference PKC2009

May 2010 Jean-Charles Faugere(INRIA)
proposed an attack against 3rd version.

Now We are preparing 4th version
whose security is equivalent to SFP.

Contents

1. **Introduction**

   Public key cryptosystem, Motivation

2. **Section Finding Problem**

   A Computational Hard Problem on Algebraic Surface

3. **Algebraic Surface Public-key Cryptosystem**

   Encryption/Decryption/Key Generation Algorithms

4. **Known Attacks**

   – Rational Point Attack

   – Ideal Factorization Attack

5. **Conclusion and Future Research**

Conclusions

- We showed a new type of public-key cryptosystem using an algebraic surface.
  - We showed the algorithm for encryption, decryption and key generation.

- Our contributions are
  - The public key size is O(n).
  - Our cryptosystem is associated higher general equations than multivariate cryptosystems. (contains equation which degree is more than 3)

Open Problems

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

- Construct a secure algorithm
  - We try to construct a provable secure cryptosystem

- Determine the recommendable parameter size
  - We developed an efficient algorithm to solve the SFP.
  - Now we estimate computational complexity by computational experimentation.

Next Talk


TOSHIBA
Leading Innovation