TOSHIBA
Leading Innovation

4th ASIA PQC Forum

Indeterminate Equation Public-key Cryptosystem "*Giophantus*™"

Koichiro AKIYAMA
TOSHIBA Corporation

Joint work with
Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida, Goichiro Hanaoka, Hideo Shimizu, Yasuhiko Ikematsu

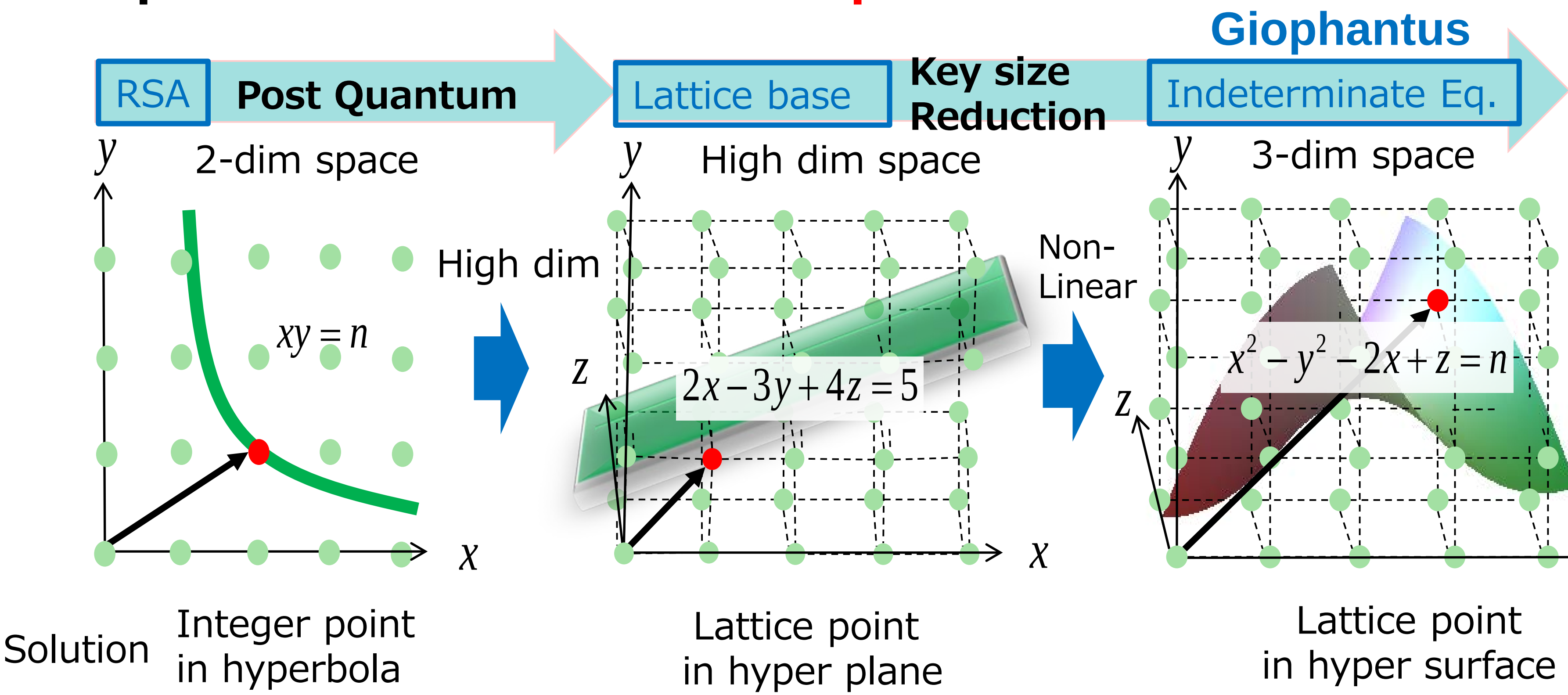
2018.06.29

Agenda

1. **Design concept**
2. **Algorithm**
3. **Computational assumption**
4. **Cryptanalysis**
5. **Evaluating at one attack**
6. **Conclusion**

Concept for Design

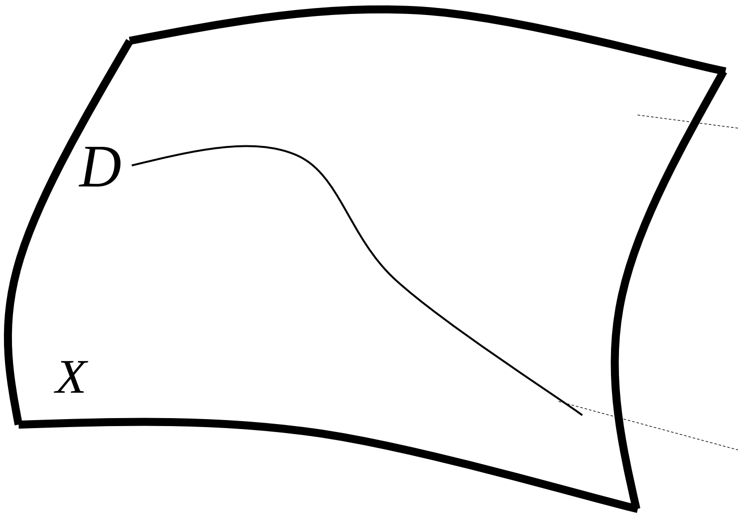
To construct a public-key cryptosystem whose security depends on some non-linear problem.



Giophantus provides new variation of PQC which is located between **multivariate & lattice based** cryptosystem

Section Finding Problem

Algebraic Surface



Section Finding Problem

Algebraic Surface public key

$$X(x, y) = 0 \text{ on } F_p[t]$$

Hard ↓ ↑ **Easy**

Section secret key

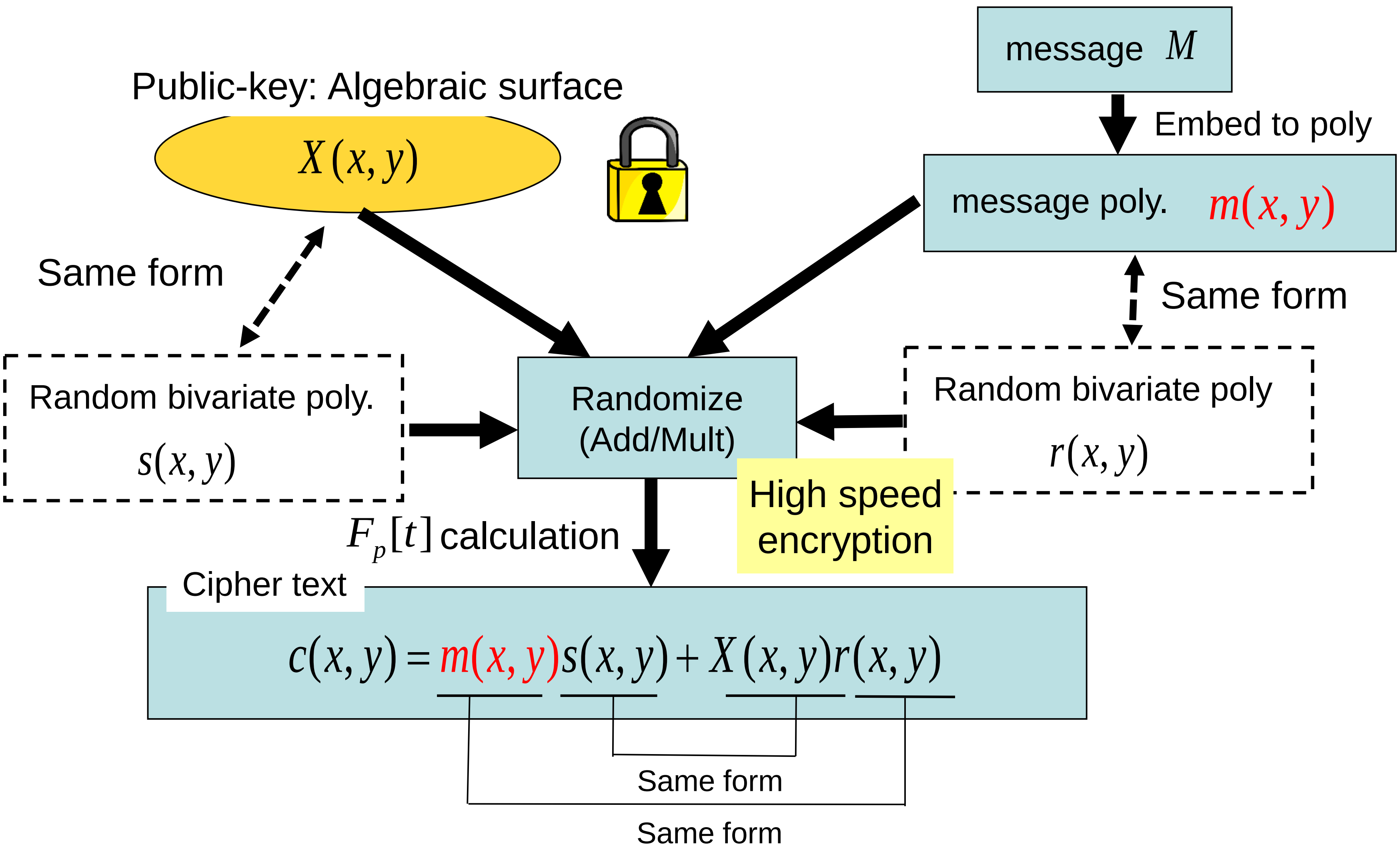
$$(x, y) = (u_x(t), u_y(t))$$

$$u_x(t), u_y(t) \in F_p[t]$$

This problem is considered as a Diophantine problems on $F_p[t]$

Algebraic Surface Cryptosystem (ASC)

Algebraic Surface Cryptosystem（Encryption）



Algebraic Surface Cryptosystem（Decryption）

Cipher text

$$c(x,y) = m(x,y)s(x,y) + X(x,y)r(x,y)$$

↓

Section substitution ← Secret key : section $D:(x,y,t)=(u_x(t),u_y(t))$

↓

$$m(u_x(t),u_y(t))s(u_x(t),u_y(t))$$

↓ Factoring (univariate poly.)

Message poly.
$m(u_x(t),u_y(t))$

↓ Solving linear equations

message M

History & Progression of ASC

$$c = m + Xr$$

multiple structure ⇩ Linear Algebra Attack

Reduction Attack

$$c = m(t)s + Xr(t)$$

3 variables ⇩ Trace Attack by Voloch

$$c = ms + Xr$$ PKC2009

noise addition ⇩ Ideal Decomposition Attack

by Faugere

$$\boxed{c = m(t) + Xr + \ell \cdot e}$$ Eliminate mult. structure (noise added structure)

Giophantus™

Small Solution Problem

The "small" solution $u_x(t), u_y(t)$ has coefficients are in the range of 0 to $\ell - 1$,where ℓ is small enough to q .

Small Solution Problem

Indeterminate Equation

$$X(x,y)=0 \ \ on\ F_q[t]/(t^n-1)$$

Hard ↓ ↑ **Easy**

Small Solution

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

$$u_x(t),u_y(t) \in F_q[t]/(t^n-1)$$

Section Finding Problem

Algebraic Surface

$$X(x,y)=0\ on\ F_p[t]$$

↓ ↑

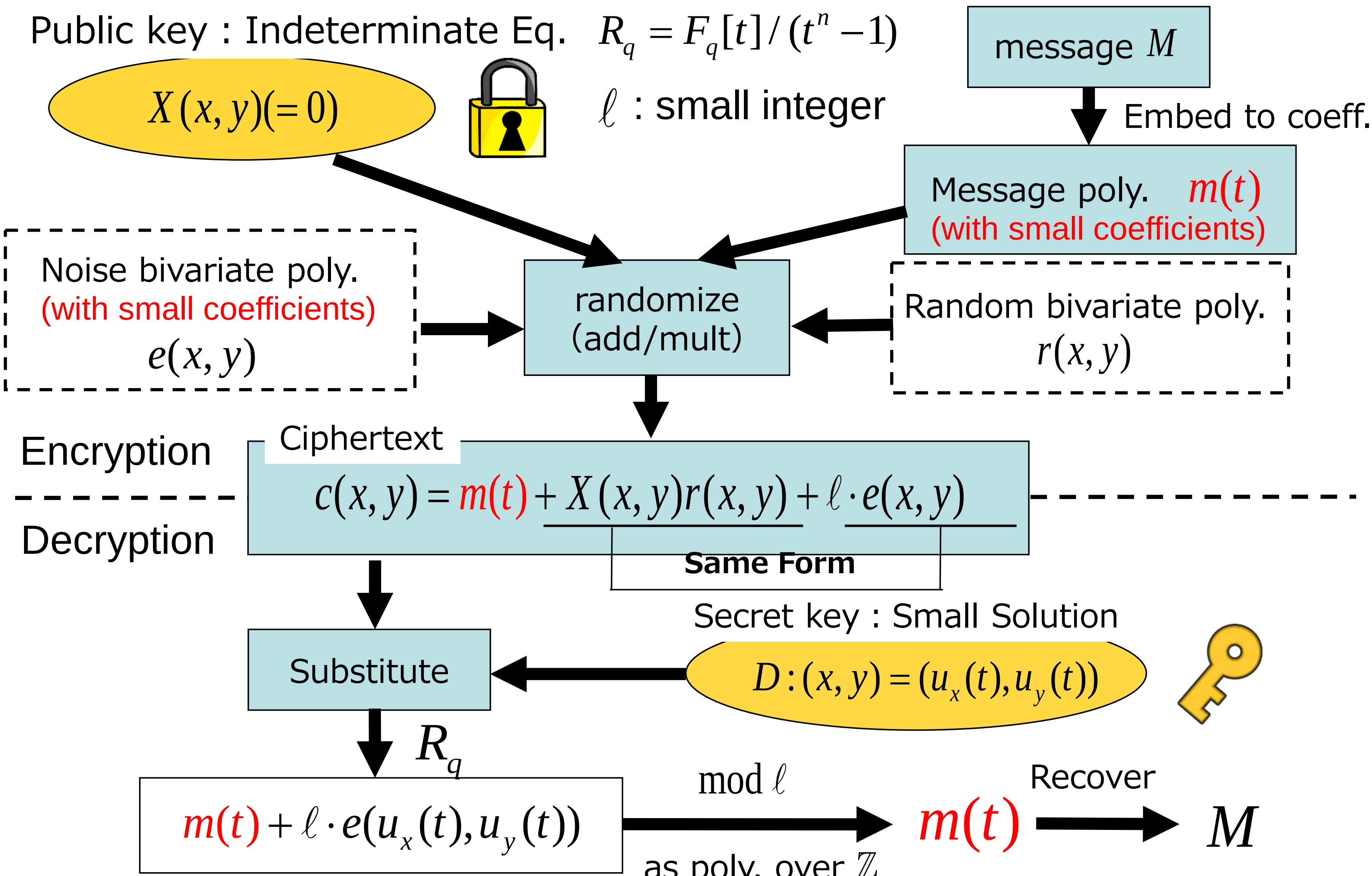
Section

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

$$u_x(t),u_y(t) \in F_p[t]$$

Encryption/Decryption

Giophantus™



$F_q[t]/(t^n-1)$ calculation

$F_q[t]/(t^3-1)$ calculation $\underbrace{(2t^2+3t+4)}_{\text{Matrix}}\underbrace{(at^2+bt+c)}_{\text{Vector}}=\underbrace{dt^2+et+f}_{\text{Vector}}$

$$t^3 \equiv 1$$

$$\begin{aligned}(2t^2+3t+4)at^2 &= 2at^4+3at^3+4at^2\\ &= 4at^2+2at+3a\\ (2t^2+3t+4)bt &= 2bt^3+3bt^2+4bt\\ &= 3bt^2+4bt+2b\\ (2t^2+3t+4)c &= 2ct^2+3ct+4c\end{aligned}$$

Matrix expression

$$\begin{pmatrix}4 & 3 & 2\\ 2 & 4 & 3\\ 3 & 2 & 4\end{pmatrix}\begin{pmatrix}a\\ b\\ c\end{pmatrix}=\begin{pmatrix}4a+3b+2c\\ 2a+4b+3c\\ 3a+2b+4c\end{pmatrix}\begin{matrix}t^2\\ t\\ 1\end{matrix}$$

IE-LWE Problem/Assumption

X :Irreducible polynomial with small zero point
Y :random bivariate polynomial
$\Big\}$ on $F_q[t]/(t^n - 1)$

Decision problem between the distribution $(X, Xr + e)$ and the distribution (X, Y) called IE-LWE problem & assumption.

Attack	Method sample (X, Z)	Infulluence	
		deg X=1	deg X=2
Linear Algebra Attack（LAA）	$Z = Xr + e \xrightarrow[\text{of coefficients}]{\text{Comparison}} r, e$	○ ∧	◎ ∨
Key Recovery Attack（KRA）	$X(x, y) = 0 \xrightarrow[\text{Ind. Eq.}]{\text{Soving}} (u_x, u_y)$	○	×

The lattice reduction technique can be applied to these attacks since these goals are common in finding small solutions.

Linear Algebra Attack (LAA)

$$\sum_{(i,j)\in\Gamma_e} d_{ij}x^i y^j = \Big(\sum_{(i,j)\in\Gamma_X} a_{ij}x^i y^j\Big)\Big(\sum_{(i,j)\in\Gamma_r} r_{ij}x^i y^j\Big) + \sum_{(i,j)\in\Gamma_e} e_{ij}x^i y^j \quad \text{on } F_q[t]/(t^n-1)$$

$\deg_{xy} X = \deg_{xy} r = 1$

$$X(x,y) = a_{10}x + a_{01}y + a_{00}$$
$$r(x,y) = r_{10}x + r_{01}y + r_{00}$$
$$e(x,y) = e_{20}x^2 + e_{11}xy + e_{02}y^2 + e_{10}x + e_{01}y + e_{00}$$
$$Z(x,y) = d_{20}x^2 + d_{11}xy + d_{02}y^2 + d_{10}x + d_{01}y + d_{00}$$

Substitute & Compare as $F_q[t]/(t^n-1)$

$$\begin{cases} \boxed{a_{10}r_{10} + e_{20} = d_{20}} \\ a_{10}r_{01} + a_{01}r_{10} + e_{11} = d_{11} \\ a_{01}r_{01} + e_{02} = d_{02} \\ a_{10}r_{00} + a_{00}r_{10} + e_{10} = d_{10} \\ a_{01}r_{00} + a_{00}r_{01} + e_{01} = d_{01} \\ a_{00}r_{00} + e_{00} = d_{00} \end{cases}$$

LAA against IE-LWE （ single term ）

$$a_{10}r_{10} + e_{20} = d_{20} \quad \text{on } F_q[t]/(t^n - 1)$$

Integerization

$$a_{10}r_{10} + e_{20} + qu_{20} = d_{20} \quad \text{on } \mathbb{Z}[t]/(t^n - 1)$$

Linear Equation

$$\begin{pmatrix} A_{10} & I_n & qI_n \end{pmatrix} \begin{pmatrix} \overrightarrow{r_{10}} \\ \overrightarrow{e_{20}} \\ \overrightarrow{u_{20}} \end{pmatrix} = \begin{pmatrix} \overrightarrow{d_{20}} \end{pmatrix} \quad \text{on } \mathbb{Z}$$

element of the $\overrightarrow{e_{20}}$ is small

LAA against IE-LWE　(all terms)

If we consider the all equations

$$\underbrace{\begin{pmatrix} A_{10} & & & I_n & & & & & & qI_n & & & & & \\ A_{01} & A_{10} & & & I_n & & & & & & qI_n & & & & \\ & A_{01} & & & & I_n & & & & & & qI_n & & & \\ A_{00} & & A_{10} & & & & I_n & & & & & & qI_n & & \\ & A_{00} & A_{01} & & & & & I_n & & & & & & qI_n & \\ & & A_{00} & & & & & & I_n & & & & & & qI_n \end{pmatrix}}_{\mathcal{L}_{LAA}} \begin{pmatrix} \overrightarrow{r_{10}} \\ \overrightarrow{r_{01}} \\ \overrightarrow{r_{00}} \\ \overrightarrow{e_{20}} \\ \overrightarrow{e_{11}} \\ \overrightarrow{e_{02}} \\ \overrightarrow{e_{10}} \\ \overrightarrow{e_{01}} \\ \overrightarrow{e_{00}} \\ \overrightarrow{u_{20}} \\ \overrightarrow{u_{11}} \\ \overrightarrow{u_{02}} \\ \overrightarrow{u_{10}} \\ \overrightarrow{u_{01}} \\ \overrightarrow{u_{00}} \end{pmatrix} = \begin{pmatrix} \overrightarrow{d_{20}} \\ \overrightarrow{d_{11}} \\ \overrightarrow{d_{02}} \\ \overrightarrow{d_{10}} \\ \overrightarrow{d_{01}} \\ \overrightarrow{d_{00}} \end{pmatrix} \quad \text{on } \mathbb{Z}$$

where element of the $\overrightarrow{e_{ij}}$ is small

$$\boxed{rank(\mathcal{L}_{LAA}) = 6n}$$

Attack Improvement (by Xagawa)

$$X(x,y) = a_{10}x + a_{01}y + a_{00}$$
$$r(x,y) = r_{10}x + r_{01}y + r_{00}$$
$$e(x,y) = e_{20}x^2 + e_{11}xy + e_{02}y^2 + e_{10}x + e_{01}y + e_{00}$$
$$Z(x,y) = d_{20}x^2 + d_{11}xy + d_{02}y^2 + d_{10}x + d_{01}y + d_{00}$$

Substitute $y = 0$

$$X(x,0) = a_{10}x + a_{00}$$
$$r(x,0) = r_{10}x + r_{00}$$
$$e(x,0) = e_{20}x^2 + e_{10}x + e_{00}$$
$$Z(x,0) = d_{20}x^2 + d_{10}x + d_{00}$$

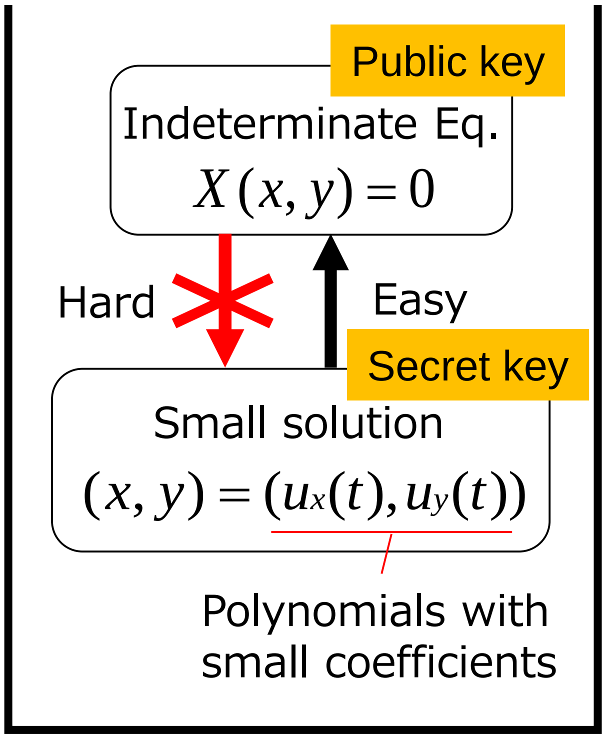
$$\begin{cases} a_{10}r_{10} + e_{20} = d_{20} \\ a_{10}r_{00} + a_{00}r_{10} + e_{10} = d_{10} \\ a_{00}r_{00} + e_{00} = d_{00} \end{cases}$$

$$\boxed{rank(\mathcal{L}'_{LAA}) = 3n}$$

$$\mathcal{L}'_{LAA} = \begin{pmatrix} A_{10} & & I_n & & & qI_n & & \\ A_{00} & A_{10} & & I_n & & & qI_n & \\ & A_{00} & & & I_n & & & qI_n \end{pmatrix}$$

Key Recovery Attack　　Linear case

Small solution problem of Indeterminate. Eq.



Linear Ind. Eq.

$$X(x, y) = c_{10}x + c_{01}y + c_{00} = 0$$

$$R_q (= F_q[t]/(t^n - 1))$$

Convert to $\mathbb{Z}[t]/(t^n - 1)$

$$c_{01}u_x + c_{10}u_y + qu = -c_{00} \qquad \begin{pmatrix} \overrightarrow{u_x} \\ \overrightarrow{u_y} \\ \vec{u} \end{pmatrix}$$

Coefficient comparison

$$\underbrace{\begin{pmatrix} C_{01} & C_{10} & qI \end{pmatrix}}_{\mathcal{L}_{KRA}} \begin{pmatrix} \overrightarrow{u_x} \\ \overrightarrow{u_y} \\ \vec{u} \end{pmatrix} = -\left(\overrightarrow{c_{00}}\right)$$

Find a small solution $(\vec{u}_x, \vec{u}_y, \vec{u})^T$

How to find a small solution

$$\mathcal{L}_{KRA}\begin{pmatrix}\overrightarrow{u_x}\\ \overrightarrow{u_y}\\ \vec{u}\end{pmatrix} = -\left(\overrightarrow{c_{00}}\right) \xrightarrow{\text{Find}} \vec{v} \xrightarrow{\text{Generalize}} \vec{v} \pm \vec{w} \quad \text{General solution}$$

$$\mathcal{L}_{KRA}(\vec{v} \pm \vec{w}) = -(\vec{c}_{00})$$

$$\mathcal{L}_{KRA}\begin{pmatrix}\overrightarrow{u_x}\\ \overrightarrow{u_y}\\ \vec{u}\end{pmatrix} = \left(\vec{0}\right) \longrightarrow \vec{w}$$

General solution

Shortest Vector problem : To find a small $\vec{v} \pm \vec{w}$

Closest Vector Problem : To find the closest $\vec{w}$ **to** $\vec{v}$

Embedding Technique

Hermite normal form

$$\mathcal{L}_{KRA} = \begin{pmatrix} I_n & B & \boxed{C} \\ O & qI_n & \boxed{D} \end{pmatrix} \leftarrow \vec{w}_c$$

correspond to

$$\mathcal{L}_{KRA} \begin{pmatrix} \overrightarrow{w_x} \\ \overrightarrow{w_y} \\ \overrightarrow{w_c} \end{pmatrix} = \left(\vec{0}\right)$$

B, C, D Cyclic matrix

$$\mathcal{L}'_{KRA} = \begin{pmatrix} I_n & B \\ O & qI_n \end{pmatrix} \Rightarrow \mathcal{L}^{+}_{KRA} = \begin{pmatrix} I & B & \vec{0}^T \\ O & qI & \vec{0}^T \\ \vec{v}_x & \vec{v}_y & \mu \end{pmatrix}$$

small integer

CVP

Embedding Technique

SVP

A solution of

$$\boxed{rank(\mathcal{L}'_{KRA}) = 2n}$$

$$\boxed{rank(\mathcal{L}^{+}{}_{KRA}) = 2n+1}$$

$$\mathcal{L}_{KRA} \begin{pmatrix} \overrightarrow{v_x} \\ \overrightarrow{v_y} \\ \overrightarrow{v_c} \end{pmatrix} = -\left(\overrightarrow{c_{00}}\right)$$

Experimental results (LLL)

			$\mathcal{L}^{+}_{KRA}$			$\mathcal{L}'_{KRA}$		
n	q	rank	Norm1	Norm2	Gap	Norm1	result	time
10	33149	21	8	186	22	204	Success	0.02
20	131059	41	12	619	50	633	Success	0.09
30	293791	61	15	1416	97	1619	Success	0.26
40	521299	81	17	3236	191	3325	Success	0.76
50	813623	101	19	6013	315	6581	Success	1.77
60	1170751	121	21	11444	552	11738	Success	3.52
70	1592659	141	22	20796	943	20589	Success	6.45
80	2079401	161	24	37181	1563	37601	Success	10.74
90	2630917	181	25	66292	2641	65551	Success	57.79
100	3247243	201	27	106864	4026	110512	Success	318.16
110	3928361	221	28	186219	6724	201748	Success	788.46
120	4674289	241	29	307382	10474	313401	Success	1361.19
130	5484979	261	373397	574752	2	542968	Failure	2315.24

The norm of 1st basis vector

The norm of 2nd basis vector

Gap=Norm2/Norm1

By Bai-Galbraith $\begin{pmatrix} I_n & A \\ O & qI_n \end{pmatrix}$

This problem is a Unique-SVP

$$\| \lambda_2(\mathcal{L}^{+}_{KRA}) \| \approx \underline{GH(\mathcal{L}'_{KRA})}$$

shortest vector

Experimental result (BKZ)

- We carried out a BKZ experiment by changing block size β

$(b_1, b_2, \cdots, b_{2n+1})$

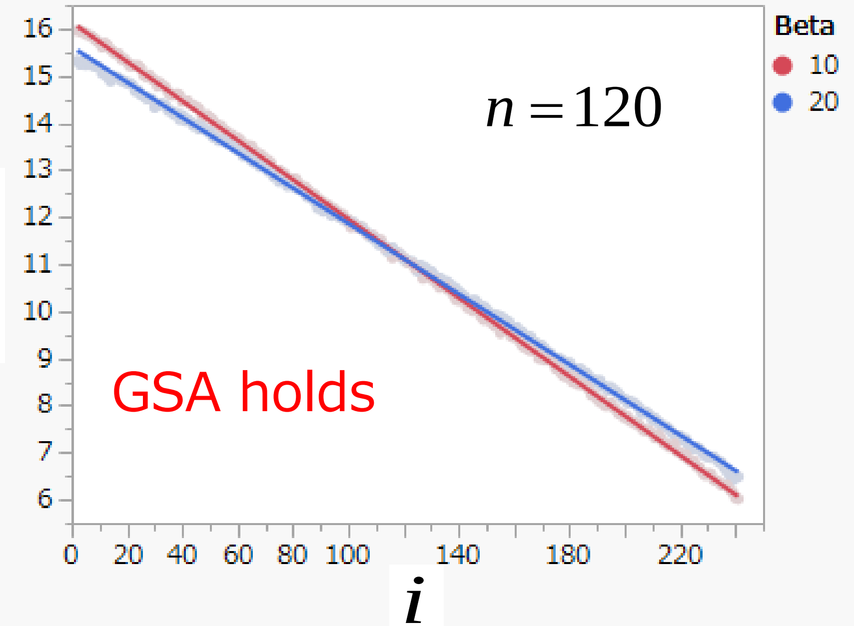
Sufficiently reduced basis of $\mathcal{L}_{KRA}^{+}$

Gram-Schmidt orthonormalization

$(b_1^*, b_2^*, \cdots, b_{2n+1}^*)$

$\log_2 \| b_i^* \|$

$i = 2, \cdots, 2n-1$



line fitting Beta=10
line fitting Beta=20

(*)Geometric series Assumption)

β	slope	y-int.	$\| b_2^* \| / \| b_1^* \|$	$\| b_2 \| / \| b_1 \|$
10	-0.0835	32.274	4320402	4320505
20	-0.0749	31.228	1783504	1783497

$\| b_2^* \| / \| b_1^* \| \approx \| b_2 \| / \| b_1 \|$

The complexity of BKZ　　2016 Estimate

We assume that the complexity for BKZ is as same as the LWE problem with

parameters	meaning	Key recovery attack
n	dimension	n
m	Number of samples	$2n$
q	modulus	$\sim 324n^2 + 72n + 15$
σ	standard deviation	1.12

■ Estimation for the root of Hermite factor for SVP

$$\delta_0 = (((\pi\beta)^{1/\beta}\beta / (2\pi e))^{1/)2(\beta-1))}$$

■ 2016 Estimate

$$\sqrt{\beta/(2n)}\lambda_1(\mathcal{L}_{KRA}^{+}) \geq \delta_0^{2\beta-2n}(\det \mathcal{L}_{KRA}^{+})^{1/2n}$$

(where $\lambda_1(\mathcal{L}_{KRA}^{+}) = \sqrt{5n/2}$ holds)

Find a pair (n, β) satisfied both conditions

Time complexity
$8 \cdot 2n \cdot 2^{0.292\beta+12.31}$

Parameter & Performance

In linear case, namely deg X(x,y)=1, we choose the parameter n by cryptanalysis based on the "**2016 estimate**".

$\ell = 4$

reference implementation

k	n	q	Public Key(KB)	Secret Key(KB)	Cipher Text(KB)	Key Gen (Mcycle)	Encrypt (Mcycle)	Decrypt (Mcycle)
135	1201	**467424413**	15	0.6	29	93	179	336
196	1733	**973190461**	21	0.9	42	161	379	717
259	2267	**1665292879**	28	1.2	55	240	627	1187

prime prime

Small

High speed

q is a prime next to

$$\ell - 1 + \ell(\ell - 1) + 2\ell(\ell - 1)^2 n + 3\ell(\ell - 1)^3 n^2$$

CPU : Xeon E5-1620 3.6GHz
OS : Windows 7, 64bit
Memory : 32GB

Evaluating at one attack

Decryption

$$c(x,y,t) = m(t) + X(x,y,t)r(x,y,t) + \ell \cdot e(x,y,t)$$

small solution $X(x,y,t)=0$ $\quad R_q = (F_q[t]/(t^n-1))$

$$(u_x(t),u_y(t)) = (\sum_{i=0}^{n-1} a_i t^i, \sum_{i=0}^{n-1} b_i t^i)$$

$$0 \le a_i, b_i < \ell - 1$$

$$c(u_x(t),u_y(t),t) = m(t) + \ell \cdot e(u_x(t),u_y(t),t)$$

$\mathbb{Z}[t]$

$$c(u_x(t),u_y(t),t) \bmod \ell = m(t)$$

$t=1$

$t=1$

Attack

$$c(x,y,1) = m(1) + X(x,y,1)r(x,y,1) + \ell \cdot e(x,y,1)$$

small solution $X(x,y,1)=0$ $\quad F_q$ exhaustive search

$$(s_x, s_y) = (u_x(1),u_y(1)) = (\sum_{i=0}^{n-1} a_i, \sum_{i=0}^{n-1} b_i)$$

$$0 \le s_x, s_y < n(\ell - 1)$$

$$c(s_x,s_y,1) = m(1) + \ell \cdot e(s_x,s_y,1)$$

$\mathbb{Z}[t]$

$$c(s_x,s_y,1) \bmod \ell = m(1) \bmod \ell$$

Ward Beullens, Wouter Castryck and Frederik Vercauteren consider this relation leads to breaking IND-CPA.

But the attack does not always work. Because,

$$c(s_x, s_y, 1) = m(1) + \ell \cdot e(s_x, s_y, 1) \quad F_q$$

$$\downarrow$$

$$c(s_x, s_y, 1) \bmod \ell = m(1) \bmod \ell \quad \mathbb{Z}$$

q must be larger than

$$(\ell - 1)n + 2(\ell - 1)^2 n^2 + 3(\ell - 1)^3 n^3$$

$$\Downarrow$$

$$c(u_x(t), u_y(t), t) = m(t) + \ell \cdot e(u_x(t), u_y(t), t) \quad R_q$$

$$\downarrow$$

$$c(u_x(t), u_y(t), t) \bmod \ell = m(t) \quad \mathbb{Z}[t]$$

q is a prime next to

$$\ell - 1 + \ell(\ell - 1) + 2\ell(\ell - 1)^2 n + 3\ell(\ell - 1)^3 n^2$$

in appropriate parameters

n	The minimum required q		attack/ decode
	scheme	attack	
1201	467424413	140344178502	300.25
1733	973190461	421634751198	433.25
2267	1665292879	943804735206	566;75

$$c(s_x, s_y, 1) \bmod \ell = m(1) \bmod \ell$$

is not always satisfied !

Experimental Result (parameter using fixed q)

However, we fix the parameter $q = 2^{31} - 1$ for optimal implementation

n	$c(s_x, s_y, 1) \bmod \ell$				Distinguishing Advantage(*)
	0	1	2	3	
1201	703	1167	52688	45442	0.9626
1733	36852	28222	13412	21514	0.3015
2267	24747	25522	25218	24513	0.0148

Here we set
$m(1) \bmod \ell = 1$

Distinguish Advantage=Pr(2 most likely value)-Pr(2 least likely value)

Random

$c(s_x, s_y, 1) \bmod \ell$				Distinguishing Advantage
0	1	2	3	
24844	24900	25255	25001	0.00512
25038	24946	24983	25033	0.00142
25094	25056	25120	24730	0.00428

distinguishable

Evaluating at one attack almost works the scheme with parameter used in optimal implementation.

Experimental Result (appropriate parameter)

For appropriate parameter, we employ minimum q which leads non-error decryption.

n	q	$c(s_x, s_y, 1) \bmod \ell$				Distinguishing Advantage(*)
		0	1	2	3	
1201	467424413	24769	25113	25559	24559	0.01344
1733	973190461	25136	25035	25008	24821	0.00342
2267	1665292879	25117	24791	25021	25071	0.00376

indistinguishable

Random

$c(s_x, s_y, 1) \bmod \ell$				Distinguishing Advantage
0	1	2	3	
24873	24922	25144	25061	0.0041
24883	24945	25032	25140	0.00344
25121	25114	24970	24795	0.0047

The distinguishability strongly depends on the public key. We need to consider about how to detect weak keys.

Conclusion

- We proposed a new variant of PQC called "Giophantus" which is located between Multivariate and Lattice based.
- We found the secure parameters by 2016 estimate.
- Giophantus requires short secret key in size and short process time.
- Evaluate at one Attack does not always work on Giophantus.
  - parameter used for optimization : almost works
  - appropriate parameter : depends on the public-key

TOSHIBA

Leading Innovation >>>