TOSHIBA
Leading Innovation

First PQC Standardization Conference

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

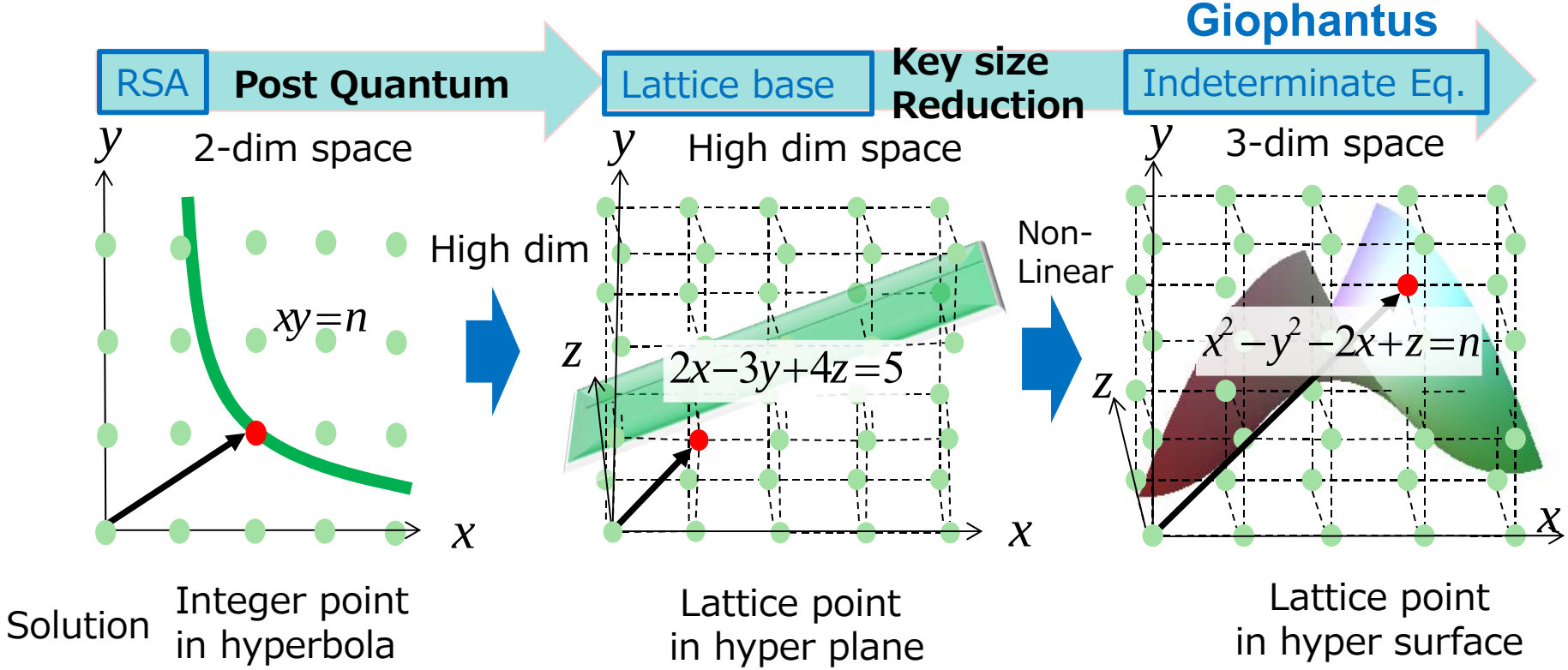
Koichiro AKIYAMA
TOSHIBA Corporation

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

2018.04.12

Concept for Design

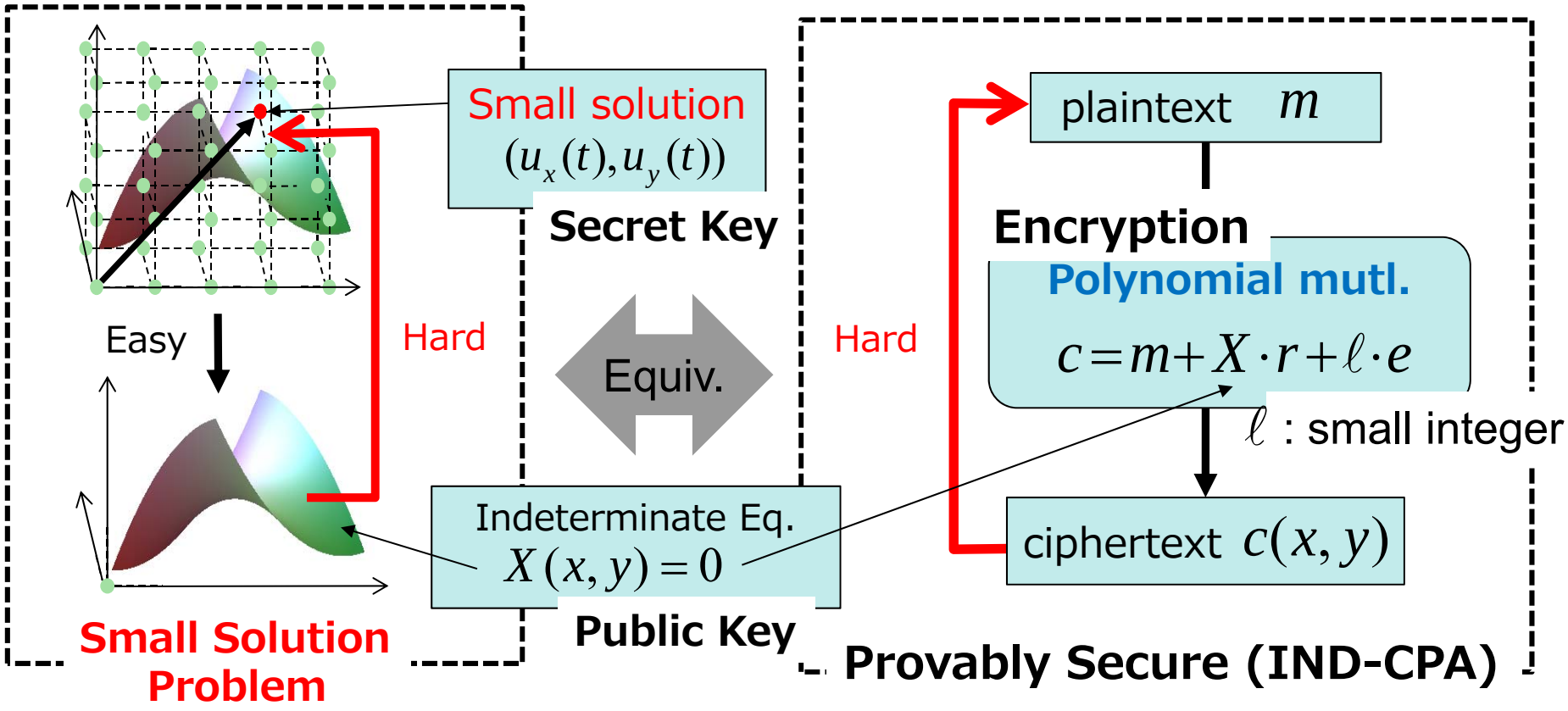
To construct a public-key cryptosystem whose security depends on some non-linear problem.



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

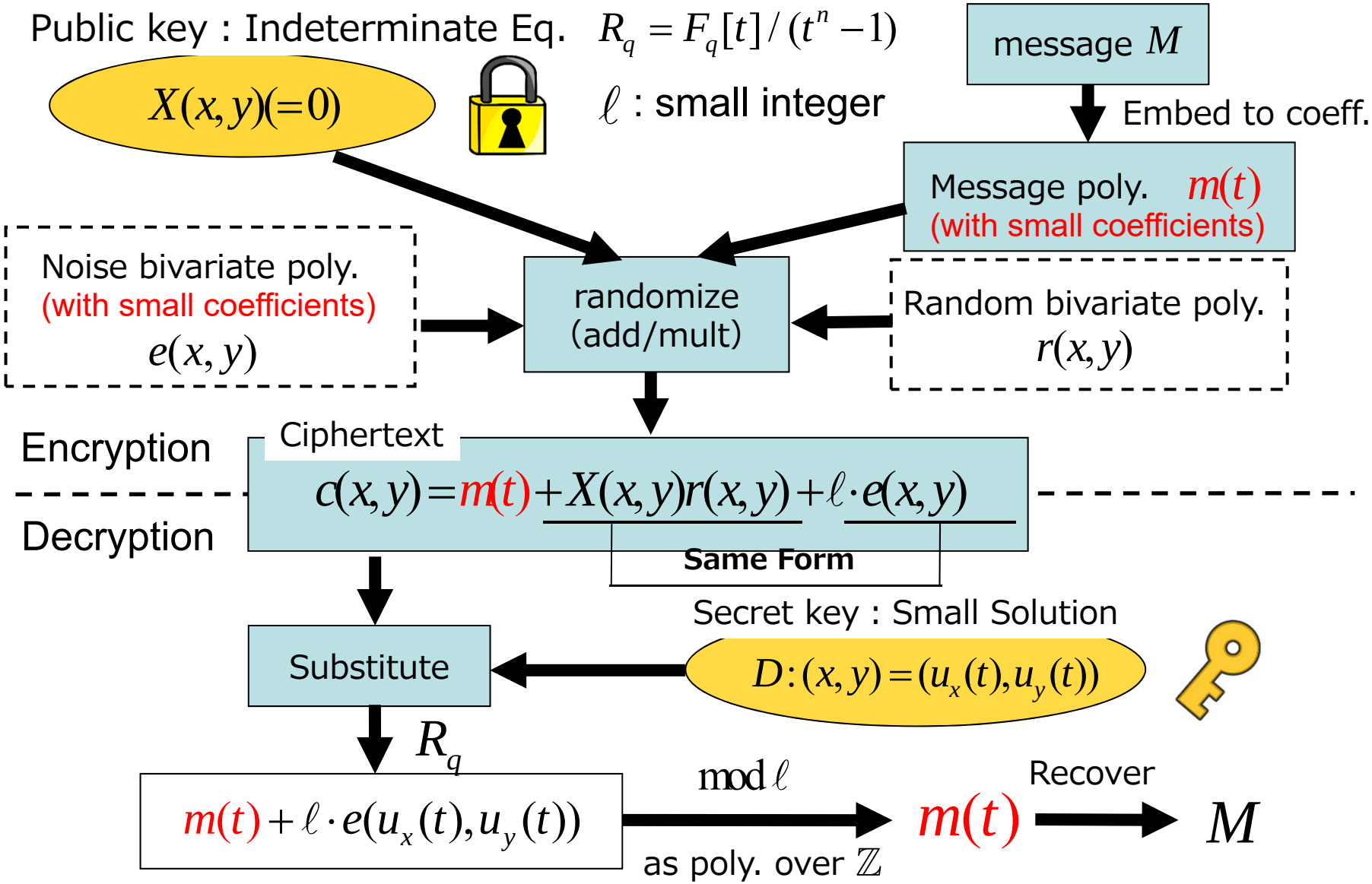
Indeterminate Equation Cryptosystem (Giophantus)

We take $R_q (= F_q[t]/(t^n - 1))$ as underlying algebra.



The security of Giophantus depends on the small solution problem on $F_q[t]/(t^n - 1)$

Encryption/Decryption



Parameter & Benchmark

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)
128	1201	**467424413**	15	0.6	29	93	179	336
192	1733	**973190461**	21	0.9	42	161	379	717
256	2267	**1665292879**	28	1.2	55	240	627	1187

prime prime

Small

High speed

q is a prime next to

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

Attack by Vercauteren

Decryption

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

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

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

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

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

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

$\mathbb{Z}[t]$

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

Attack

$t = 1$

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

small solution $X(x,y,1) = 0$

F_q exhaustive search

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

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

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

$\mathbb{Z}[t]$

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

Vercauteren et. al consider this relation leads to breaking IND-CPA.

But the attack does not 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

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

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

$$\downarrow$$

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

$$\mathbb{Z}[t]$$

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

$c(s_x, s_y, 1) \bmod \ell = m(1) \bmod \ell$ is not satisfied !

Experimental Result

We set $m(1) \bmod \ell = 1$

n	c(sx,sy,1) mod l				the minimum required q		attack /appropriate
	0	1	2	3	appropriate	attack	
1201	2438	2541	2528	2493	467424413	140344178502	300.25
1733	2558	2427	2509	2506	973190461	421634751198	433.25
2267	2492	2470	2472	2566	1665292879	943804735206	566.75

correct answer

Since the attack requires q which is over 300 times larger than appropriate one, the correct answer never be obtained when q is little bit large prime to .

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

Conclusion

- We proposed a new variant of PQC called "Giophantus" which is located between Multivariate and Lattice based.
- Giophantus requires short secret key in size and short process time.
- Vercauteren's Attack does not work on Giophantus.


TOSHIBA
Leading Innovation