Security Analysis of rSTS Type Multivariate Public Key Cryptosystems against Algebraic Attack Using Gröbner Bases

May 28, 2010
Recent Results Session
The Third International Workshop on
Post-Quantum Cryptography (PQCrypto 2010)

◎Ryo FUJITA
Research and Development Initiative, Chuo University

This work is supported by the “Strategic information and COmmunications R&D Promotion programmE” (SCOPE)
from the Ministry of Internal Affairs and Communications of Japan.

Contents

1. Introduction
2. Multivariate Quadratic
   Public Key Cryptosystems (MQPKCs)
   - rSTS type MPKC, R(S)SE
3. Algebraic Attack against MQPKC
4. Computer Experiments
   - Security of rSTS type MPKC
   - Security of R(S)SE
5. Concluding Remarks

Contents

1. Introduction
2. Multivariate Quadratic
   Public Key Cryptosystems (MQPKCs)
   - rSTS type MPKC, R(S)SE
3. Algebraic Attack against MQPKC
4. Computer Experiments
   - Security of rSTS type MPKC
   - Security of R(S)SE
5. Concluding Remarks

Early Research on Multivariate Public Key Cryptosystems

Cryptographic Schemes

MI (Matsumoto, Imai et al., 1983, 1985, 1988)

Sequential Solution Method (SSM)

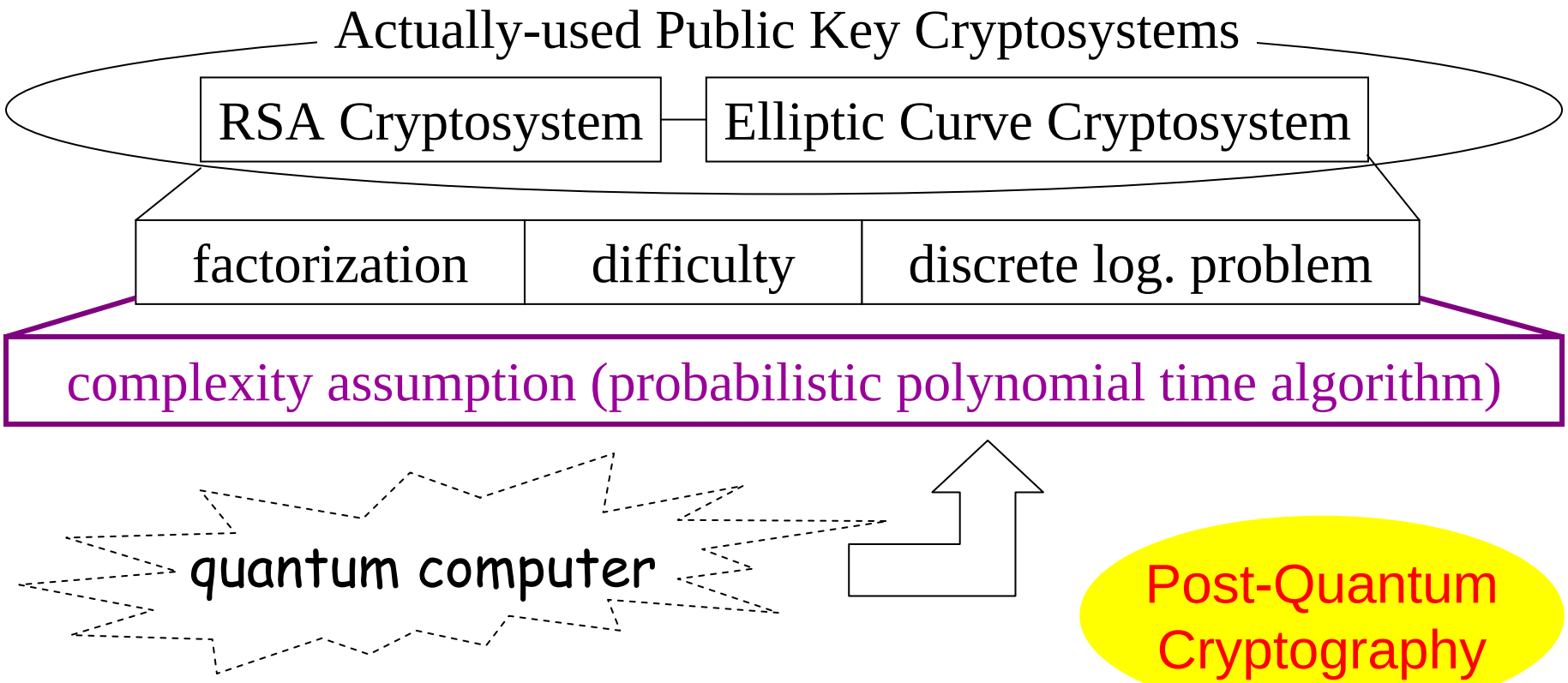
(Tsujii et al., 1985, 1986)

Core Transformation (generalized SSM)

(Tsujii et al., 1989)

Since 80's, Public Key Cryptosystems originated in Japan.

Crisis of PKCs in the future



→PKCs based on other mathematical difficulty
(ex. Multivariate Public Key Cryptosystems: MPKCs)
are needed to be developed.

Characteristics of MPKCs

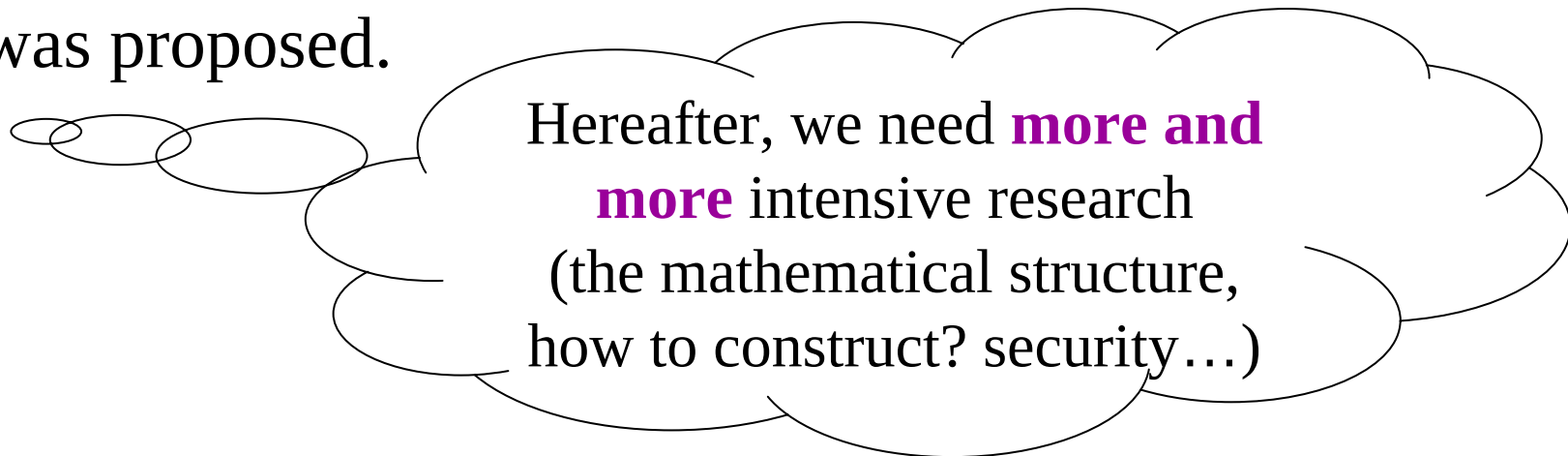
- Problem based on their security:
  (related to) solving nonlinear simultaneous multivariate equations is difficult
  (NP hard problem)
  →strongly considered to be hard to solve it
  even with **quantum computer**

- fast encryption/decryption
  …simple operation: only addition and multiplication

- relatively-long key size (a few Kbit, a few Mbit)

The current state of research on MPKCs

- Almost all of their schemes have been broken, while many various schemes have been proposed.
- In 2003, SFLASH has been selected by NESSIE and recommended for low-cost smart cards.
- In 2007, practical cryptanalysis against SFLASH was proposed.



Security of MPKCs (2/2)

Given E, $\mathbf{c}$,
to compute $\mathbf{p}$ is hard.

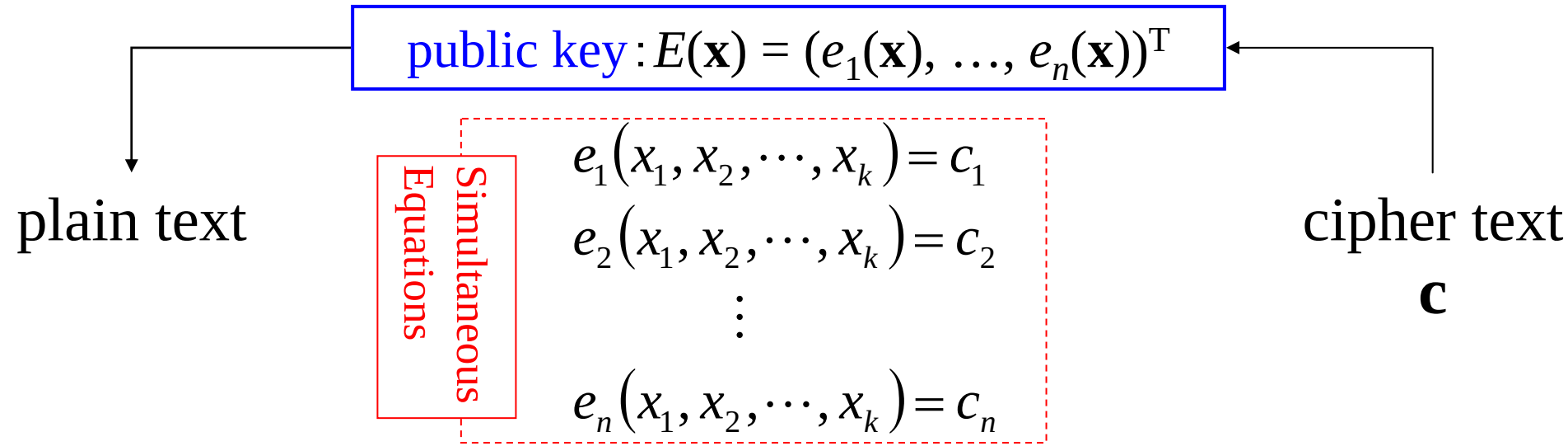
public key: E:
multivariate polynomials
(tuple)

plain text
$\mathbf{p} \in (\mathbf{F}_q)^k$

cipher text
$\mathbf{c} \in (\mathbf{F}_q)^n$

Algebraic Attack

An attack to compute the plain text **p**,
given public key E and cipher text **c**.



The attacker solves system of equations
using XL algorithm, Gröbner Basis computation, etc.

Applications of Algebraic Attacks

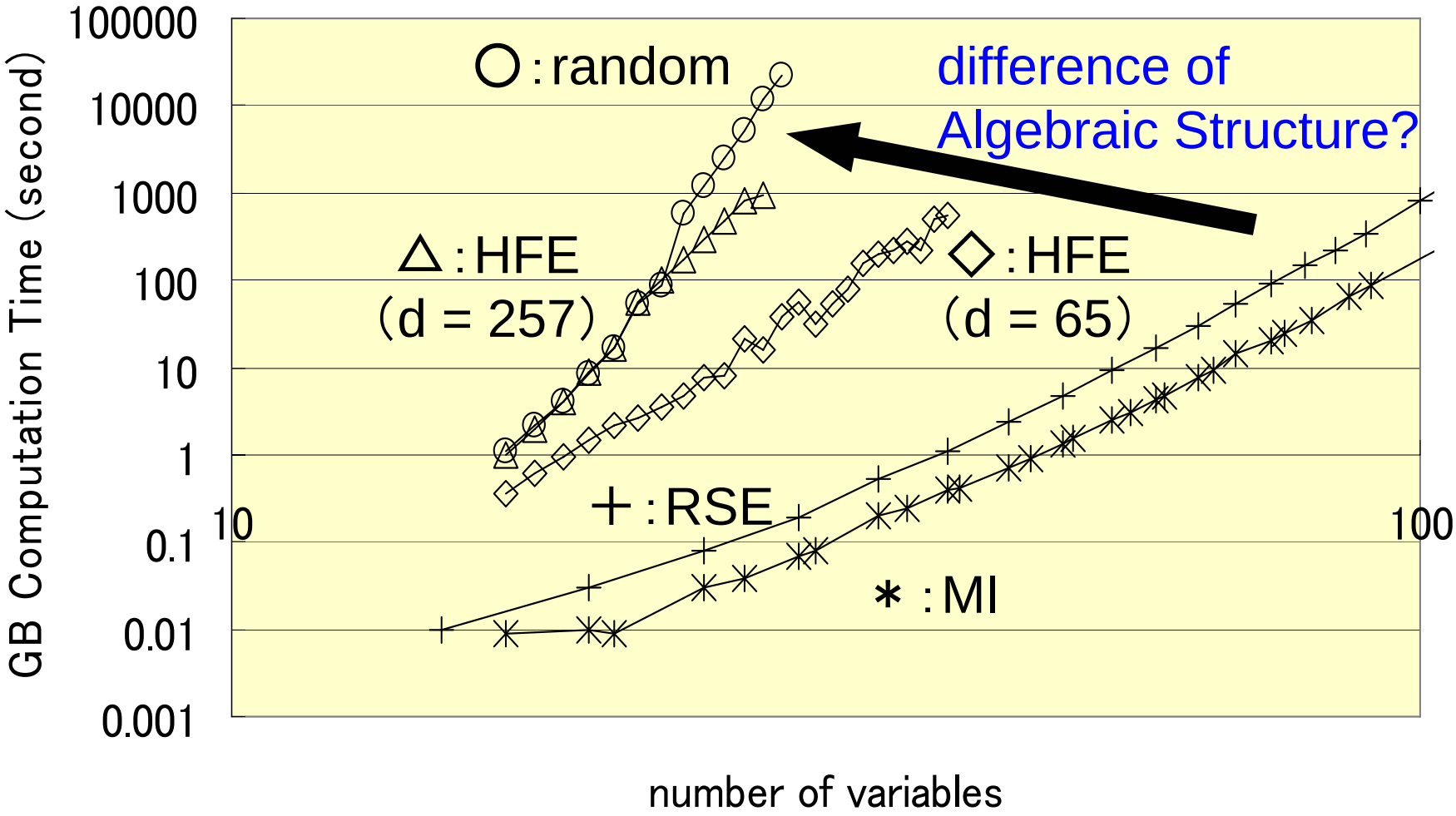
- HFE [Courtois-Daum-Felke, PKC 2003]

  [Faugère-Joux, CRYPTO 2003]

  [Granboulan-Joux-Stern, CRYPTO 2006]
- TRMC [Joux-Kunz-Jacques-Muller-Ricordel, PKC 2005]
- TRMS [Bettale-Faugère-Perret, AFRICACRYPT 2008]

- Study of security of UOV
  [Braeken-Wolf-Preneel, CT-RSA 2005]
- Complexity Estimates on PMI
  [Ding et al., 2005]

Security against GB Attack



Research Target

Showing the security of STS type MPKCs against algebraic attacks

– rSTS type MPKCs :

Special case of STS type MPKCs

ex. : SSM [Tsujii et al., 1985, 1986]

R(S)SE [Kasahara-Sakai, 2004, 2005]

Contents

1. Introduction
2. Multivariate Quadratic Public Key Cryptosystems (MQPKCs)
   - rSTS type MPKC, R(S)SE
3. Algebraic Attack against MQPKC
4. Computer Experiments
   - Security of rSTS type MPKC
   - Security of R(S)SE
5. Concluding Remarks

Multivariate Quadratic Public Key Cryptosystems (1/5)

Parameters: characteristic of the finite field q,
dimension of the plain text (vector) k,
dimension of the cipher text (vector) n

$\mathbf{F}_q = \mathrm{GF}(q)$

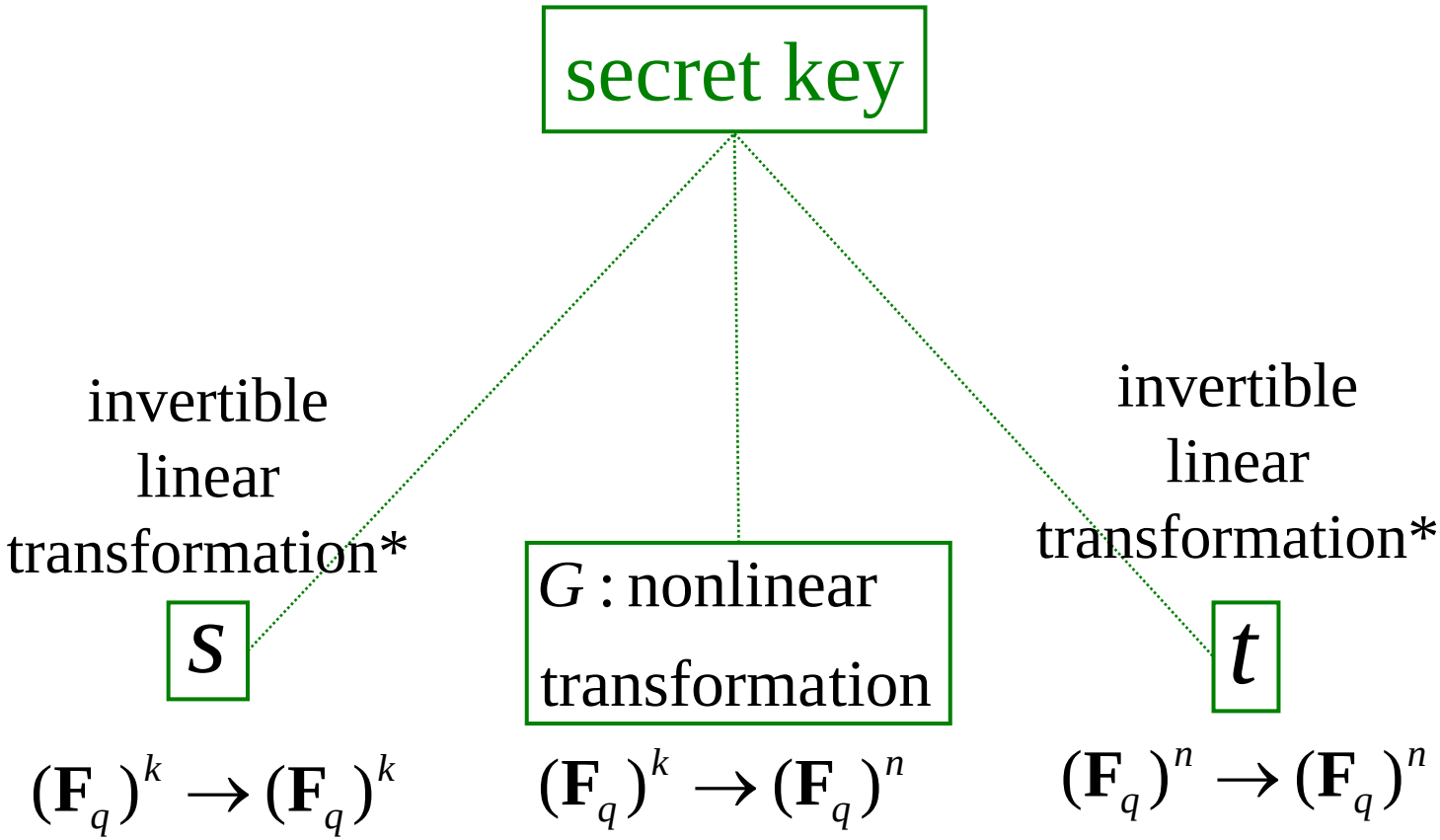
plain text

$\mathbf{p} \in (\mathbf{F}_q)^k$

cipher text

$\mathbf{c} \in (\mathbf{F}_q)^n$

Multivariate Quadratic Public Key Cryptosystems (2/5)



*: generally Affine transformation

Multivariate Quadratic Public Key Cryptosystems (3/5)

$$\mathbf{F}_q[x_1, \ldots, x_k]^n$$

public key : $E = t \circ G \circ s$:
mulrivariate polynomials (tuple)

invertible linear transformation*

s

$$(\mathbf{F}_q)^k \to (\mathbf{F}_q)^k$$

G : nonlinear transformation

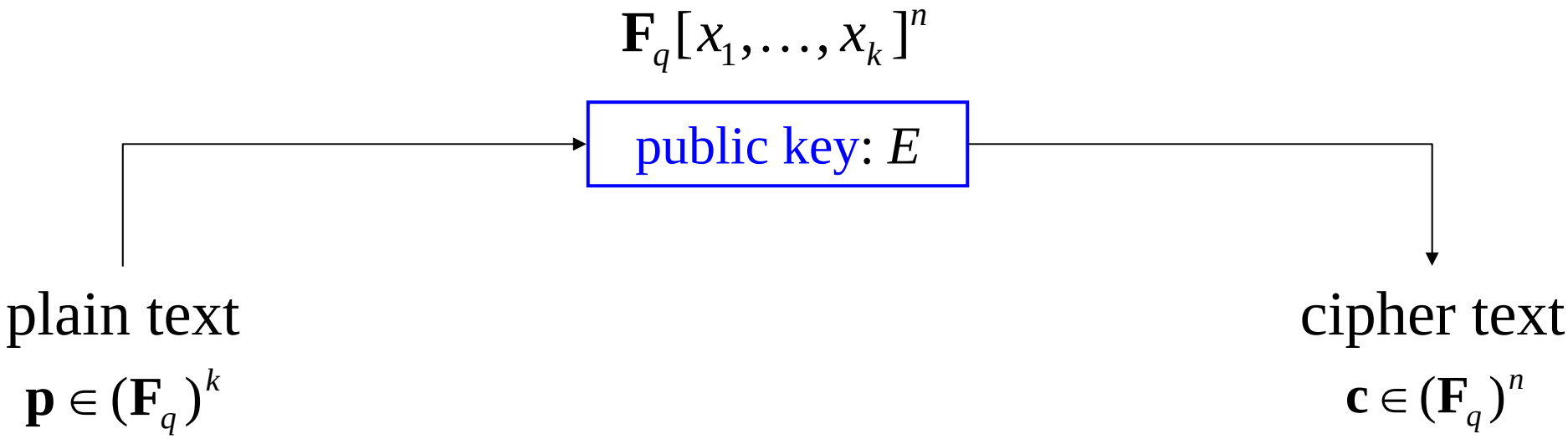
$$(\mathbf{F}_q)^k \to (\mathbf{F}_q)^n$$

invertible linear transformation*

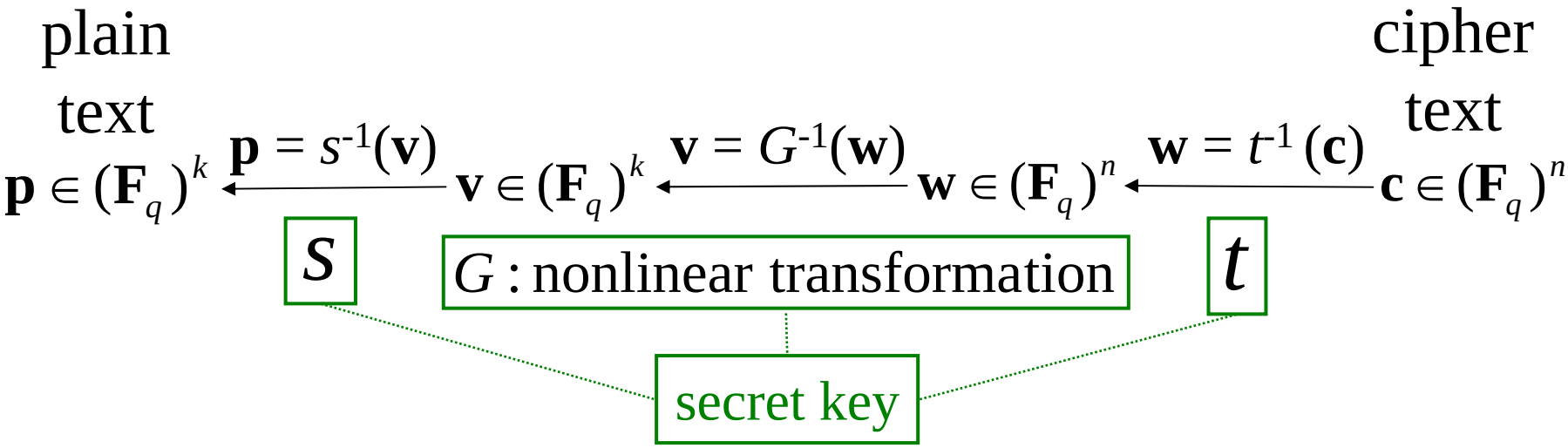
t

$$(\mathbf{F}_q)^n \to (\mathbf{F}_q)^n$$

Multivariate Quadratic Public Key Cryptosystems (4/5)



Multivariate Quadratic Public Key Cryptosystems (5/5)

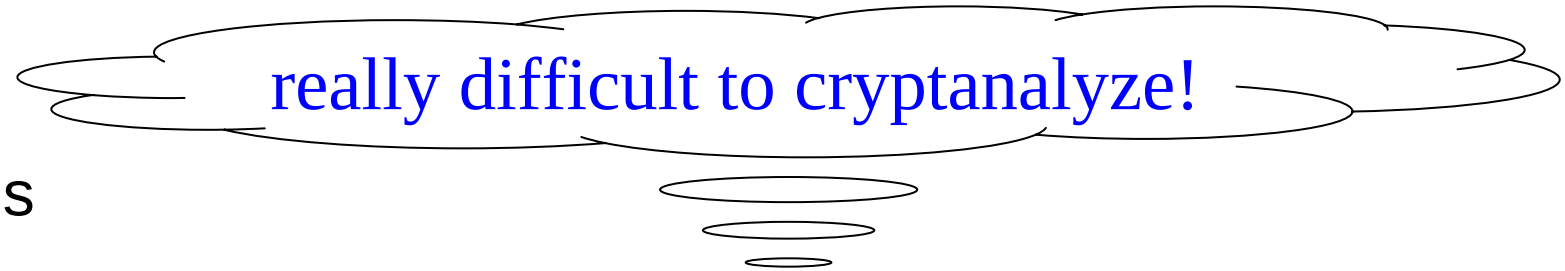


RSSE(2)minus open problem

http://www.osaka-gu.ac.jp/php/kasahara/publickeyn.html

Public-Key Cryptosystem based on Singular Simultaneous Equations and Its Variants

Please solve the following problems by computing the candidates of each message. In these problems, we have given the hashed value of the messages in a random manner for preventing the dependency of the hashed function,



Problems

Simple Problem 1: k = 100, n = 92 (cipher-text size)

Challenge Problem 1: k = 160, n = 152 (cipher-text size)

Step-wise Triangular Structure (STS)

[Wolf-Braeken-Preneel, 2004]

step 1
$$\begin{cases} g_1(x'_1,\ldots,x'_{r_1}) \\ \vdots \\ g_{m_1}(x'_1,\ldots,x'_{r_1}) \end{cases}$$

$\vdots$

step l
$$\begin{cases} g_{m_1+\cdots+m_{l-1}+1}(x'_1,\ldots,x'_{r_1},\ldots,x'_{r_1+\cdots+r_{l-1}+1},\ldots,x'_{r_1+\cdots+r_l}) \\ \vdots \\ g_{m_1+\cdots+m_l}(x'_1,\ldots,x'_{r_1},\ldots,x'_{r_1+\cdots+r_{l-1}+1},\ldots,x'_{r_1+\cdots+r_l}) \end{cases}$$

$\vdots$

step L
$$\begin{cases} g_{m_1+\cdots+m_{L-1}+1}(x'_1,\ldots,x'_k) \\ \vdots \\ g_n(x'_1,\ldots,x'_k) \end{cases}$$

m_i: number of equations in step i

r_i: number of variables added in step i

L: number of steps

$k = r_1 + r_2 + \ldots + r_L$

$n = m_1 + m_2 + \ldots + m_L$

regular Step-wise Triangular Structure (rSTS)

[Wolf-Braeken-Preneel, 2004]

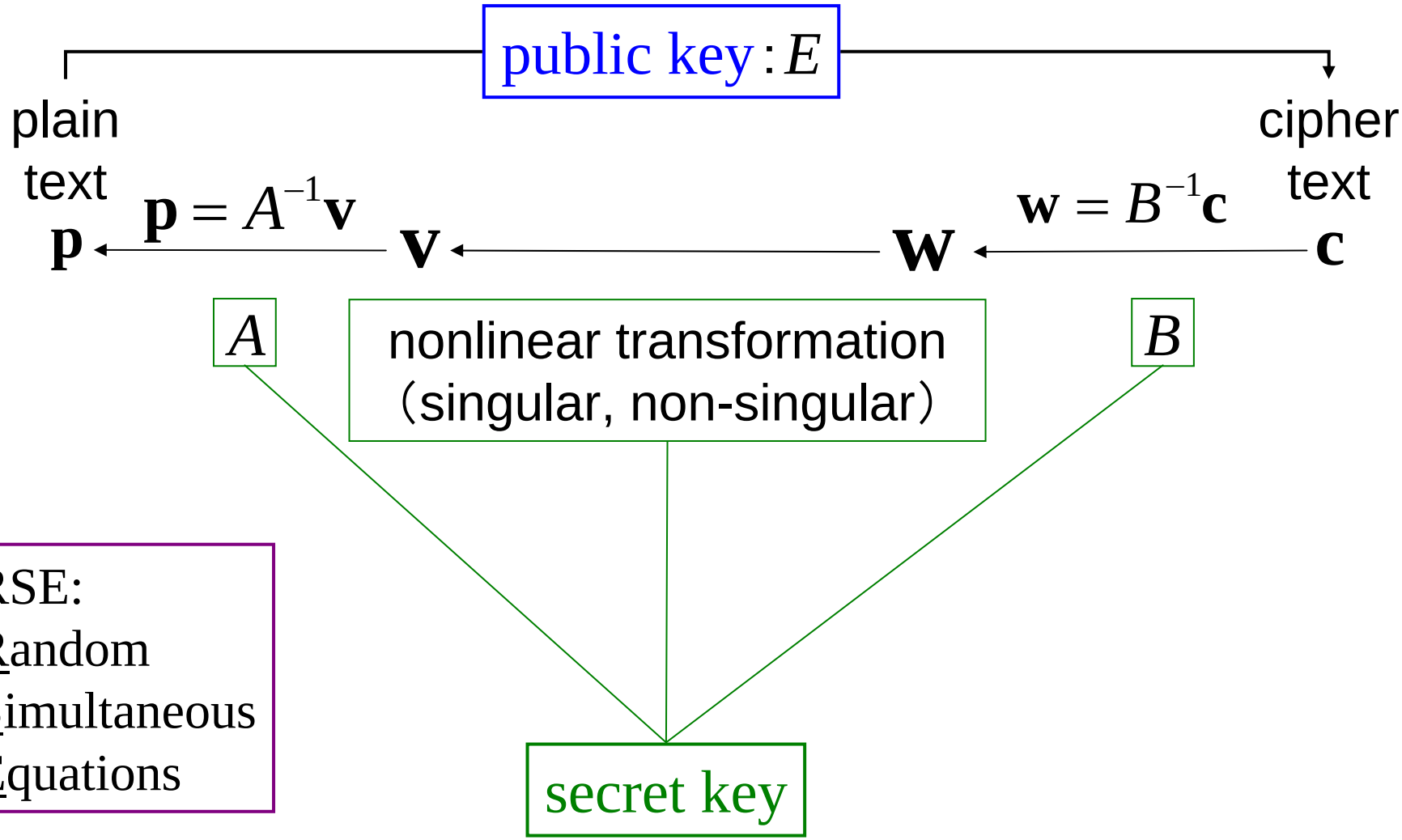
$$
\begin{array}{ll}
\text{step } 1 & \left\{ \begin{array}{c} g_1(x'_1,\ldots,x'_r) \\ \vdots \\ g_r(x'_1,\ldots,x'_r) \end{array} \right. \\
\vdots & \\
\text{step } l & \left\{ \begin{array}{c} g_{(l-1)r+1}(x'_1,\ldots,x'_r,\ldots,x'_{(l-1)r+1},\ldots,x'_{lr}) \\ \vdots \\ g_{lr}(x'_1,\ldots,x'_r,\ldots,x'_{(l-1)r+1},\ldots,x'_{lr}) \end{array} \right. \\
\vdots & \\
\text{step } L & \left\{ \begin{array}{c} g_{(L-1)r+1}(x'_1,\ldots,x'_k) \\ \vdots \\ g_{Lr}(x'_1,\ldots,x'_k) \end{array} \right.
\end{array}
$$

r: number of equations, number of variables added in each step.

L: number of steps

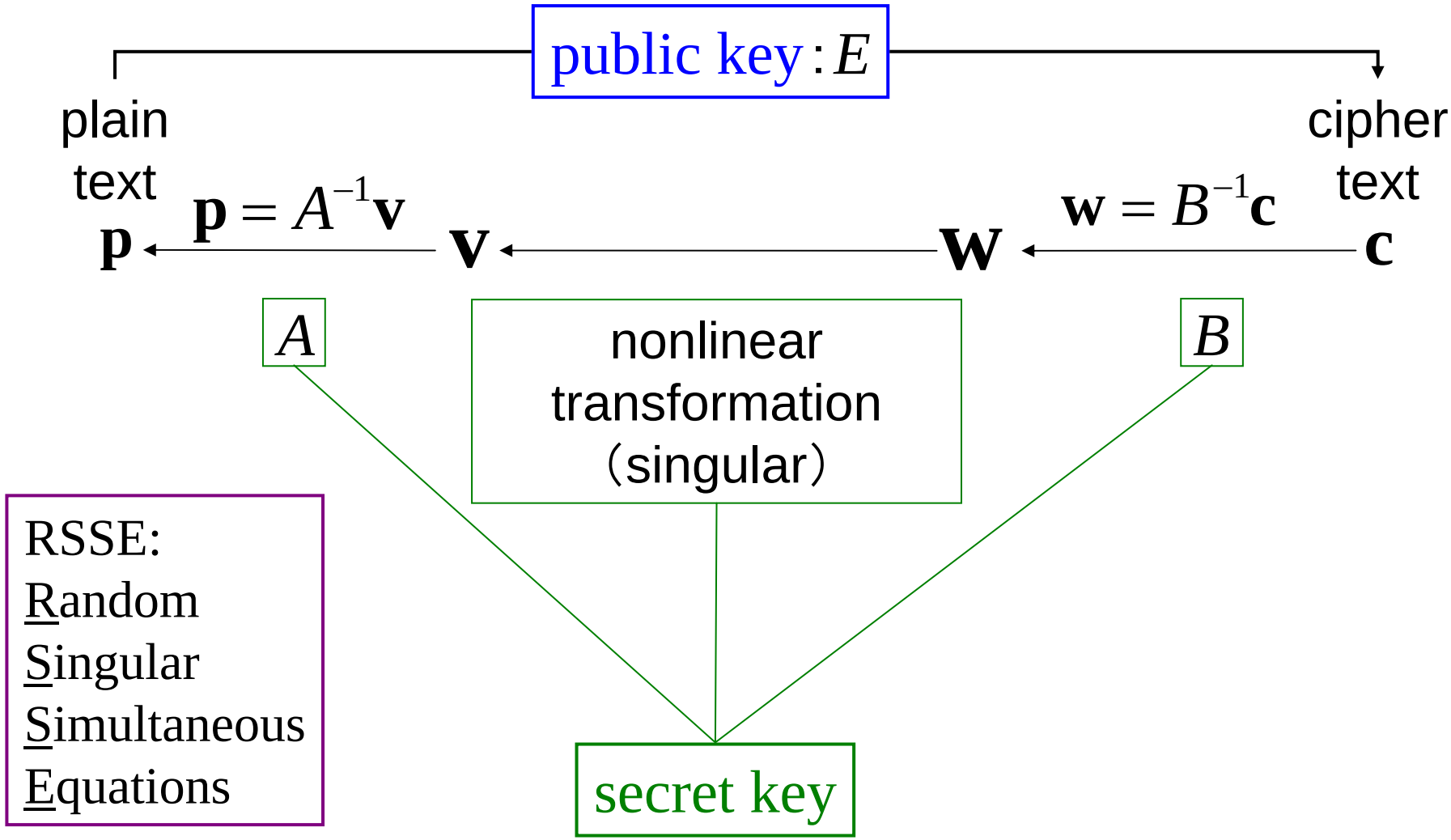
$k = n = Lr$

RSE



RSE:
Random
Simultaneous
Equations

RSSE



RSSE:
Random
Singular
Simultaneous
Equations

R(S)SE:
singular and non-singular

non-singular transformation f is that

input $(v_1, v_2, \cdots, v_r)$ and output $f(v_1, v_2, \cdots, v_r)$ correspond one to one.

$$z_1 = v_1 + v_3 + v_1 v_2 + v_3 v_1$$
$$z_2 = v_2 + v_3 + v_1 v_2$$
$$z_3 = v_2 + v_3 + v_2 v_3 + v_3 v_1$$

$$f : \mathbf{v} = (v_1, v_2, v_3) \mapsto \mathbf{z} = (z_1, z_2, z_3)$$

decimal value	v_1	v_2	v_3		z_1	z_2	z_3	decimal value
0	0	0	0	→	0	0	0	0
1	0	0	1	→	1	1	1	7
2	0	1	0	→	0	1	1	3
3	0	1	1	→	1	0	1	5
4	1	0	0	→	1	0	0	4
5	1	0	1	→	1	1	0	6
6	1	1	0	→	0	0	1	1
7	1	1	1	→	0	1	0	2

R(S)SE:
singular and non-singular

singular transformation g is that

input $(v_1, v_2, \cdots, v_r)$ and output $g(v_1, v_2, \cdots, v_r)$ does not correspond one to one.

$$w_1 = v_2 + v_3 + v_1 v_2$$

$$w_2 = v_1 + v_3 + v_2 v_3$$

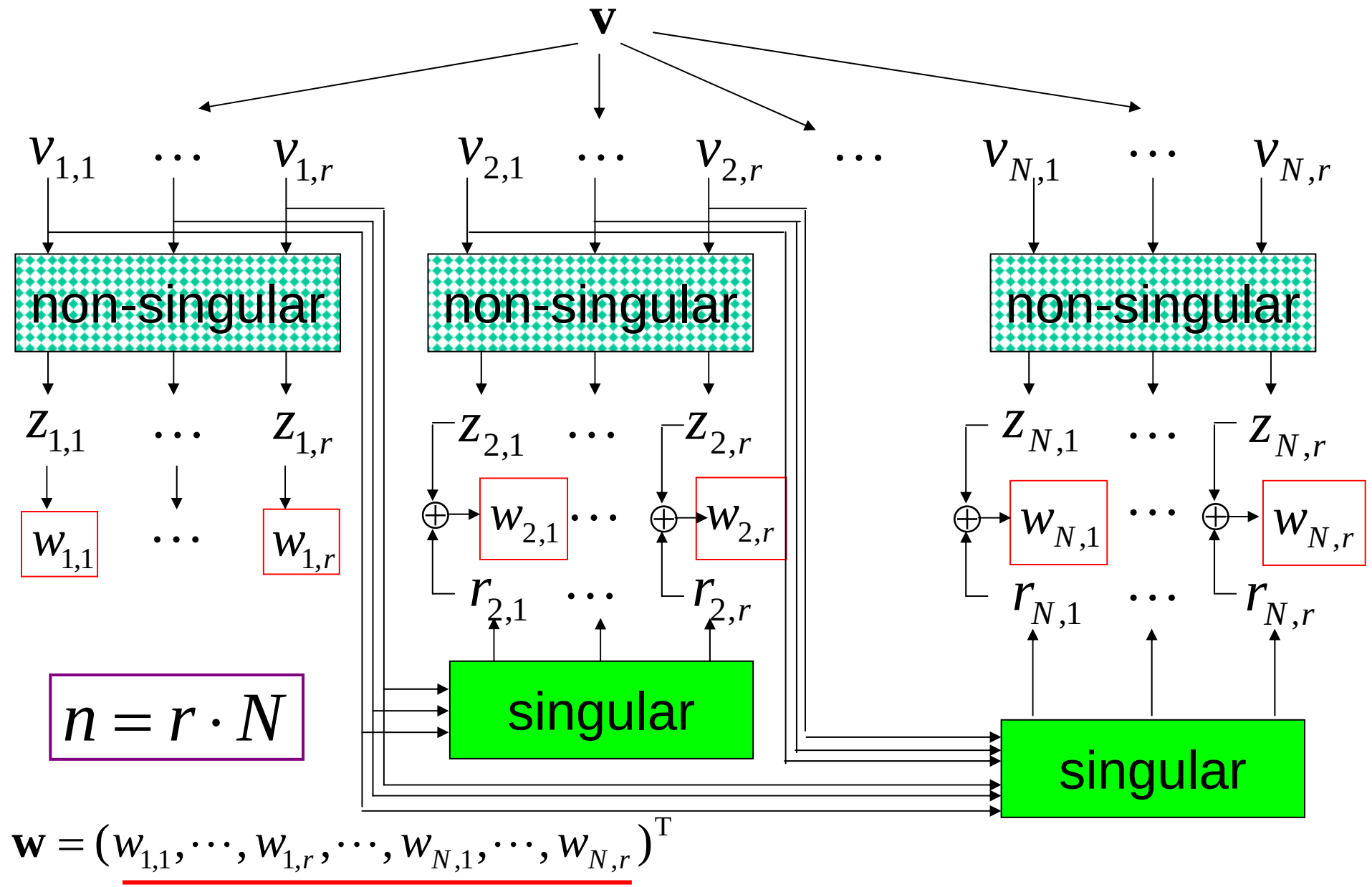
$$w_3 = v_1 + v_2 + v_1 v_2$$

$$g : \mathbf{v} = (v_1, v_2, v_3)$$

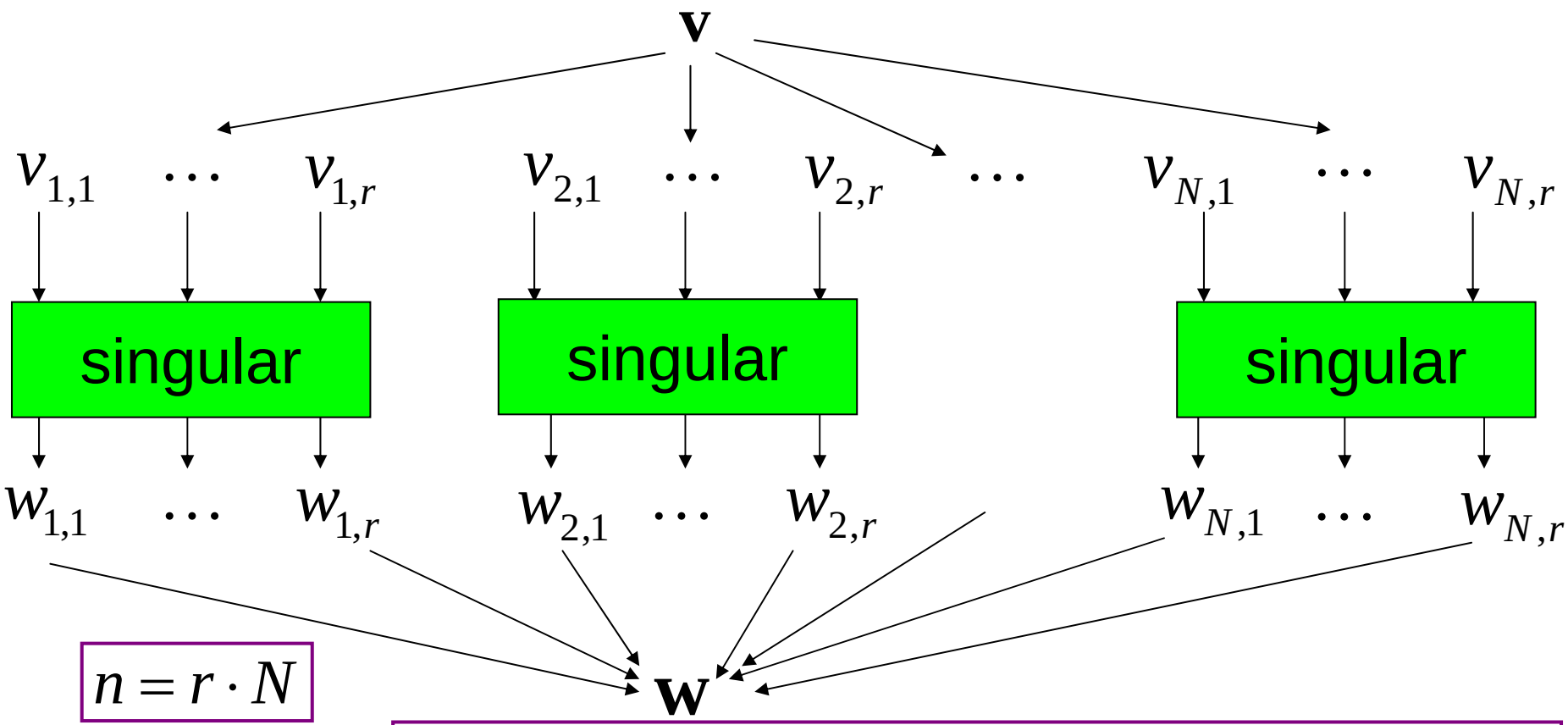
$$\mapsto \mathbf{w} = (w_1, w_2, w_3)$$

decimal value	v_1	v_2	v_3		w_1	w_2	w_3	decimal value
0	0	0	0	→	0	0	0	0
1	0	0	1	→	1	1	0	6
2	0	1	0	→	1	0	1	5
3	0	1	1	→	0	0	1	1
4	1	0	0	→	0	1	1	3
5	1	0	1	→	1	0	1	5
6	1	1	0	→	0	1	1	3
7	1	1	1	→	1	1	1	7

Nonlinear Transformation in RSE



Nonlinear Transformation in RSSE



$n = r \cdot N$

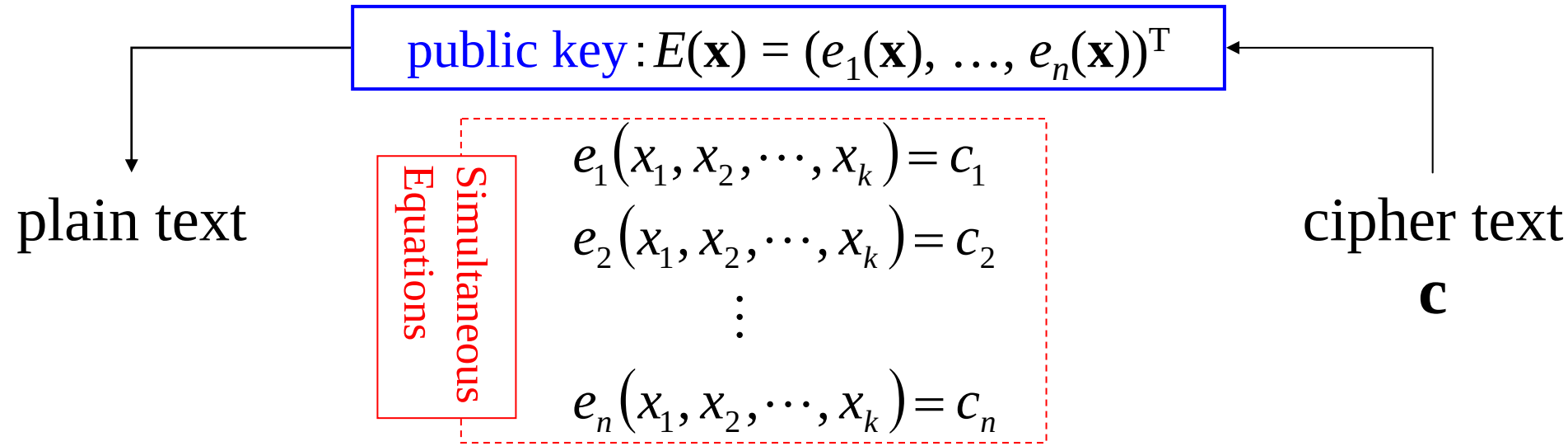
Decryption is not unique.
Redundant bits are needed to correct the error.

Contents

1. Introduction
2. Multivariate Quadratic
   Public Key Cryptosystems (MQPKCs)
   - rSTS type MPKC, R(S)SE
3. Algebraic Attack against MQPKC
4. Computer Experiments
   - Security of rSTS type MPKC
   - Security of R(S)SE
5. Concluding Remarks

Algebraic Attack

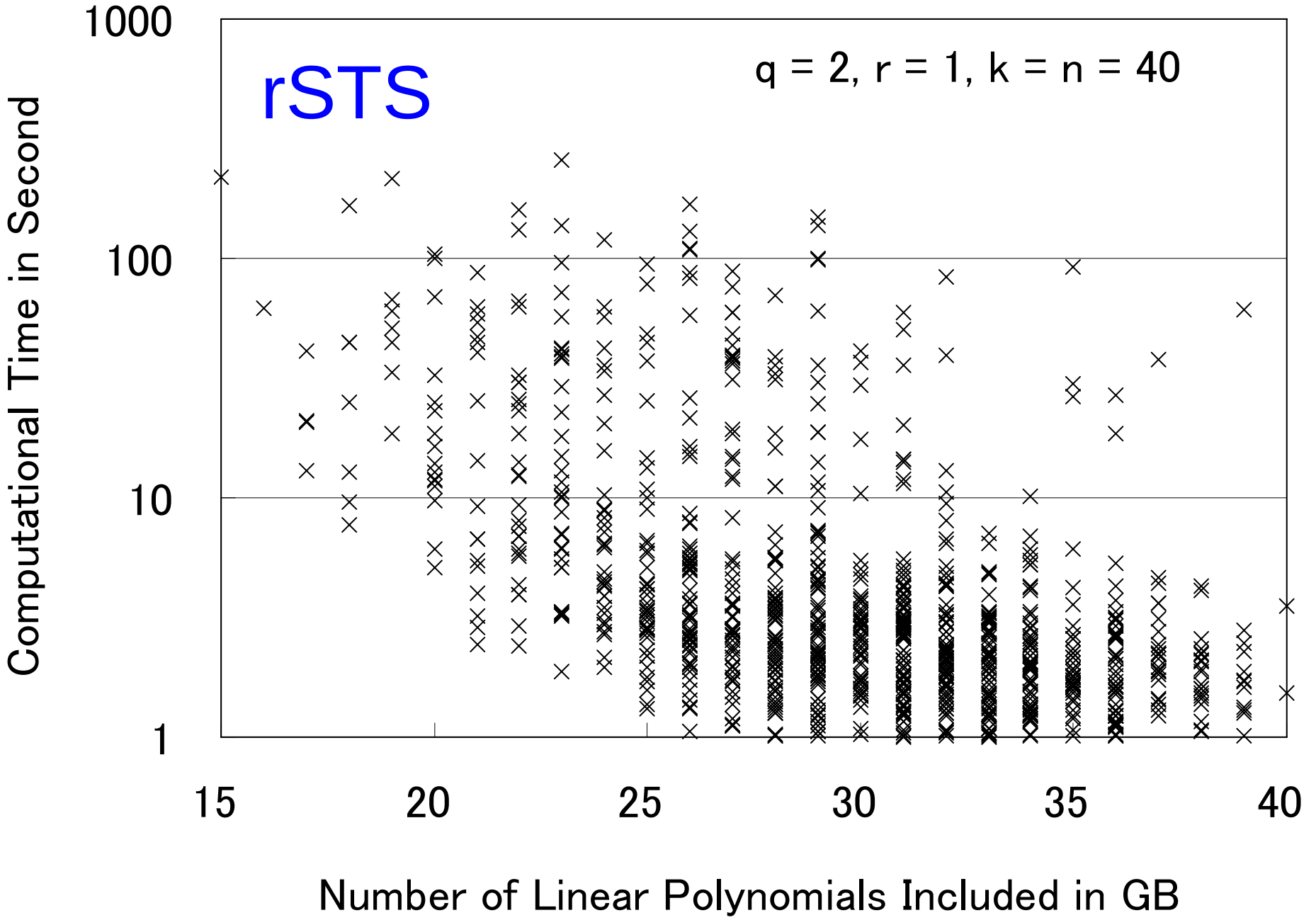
An attack to compute the plain text **p**,
given public key E and cipher text **c**.

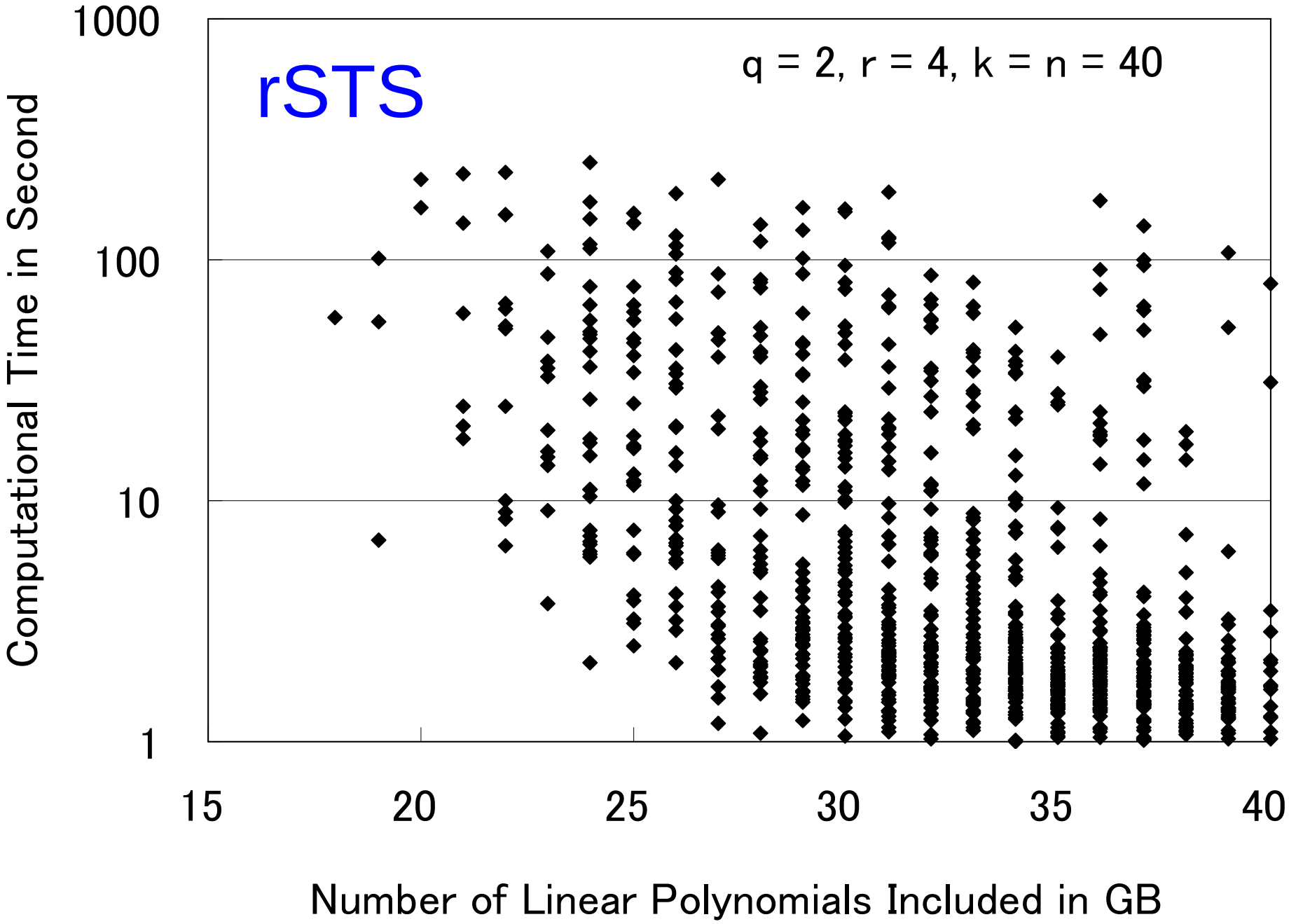


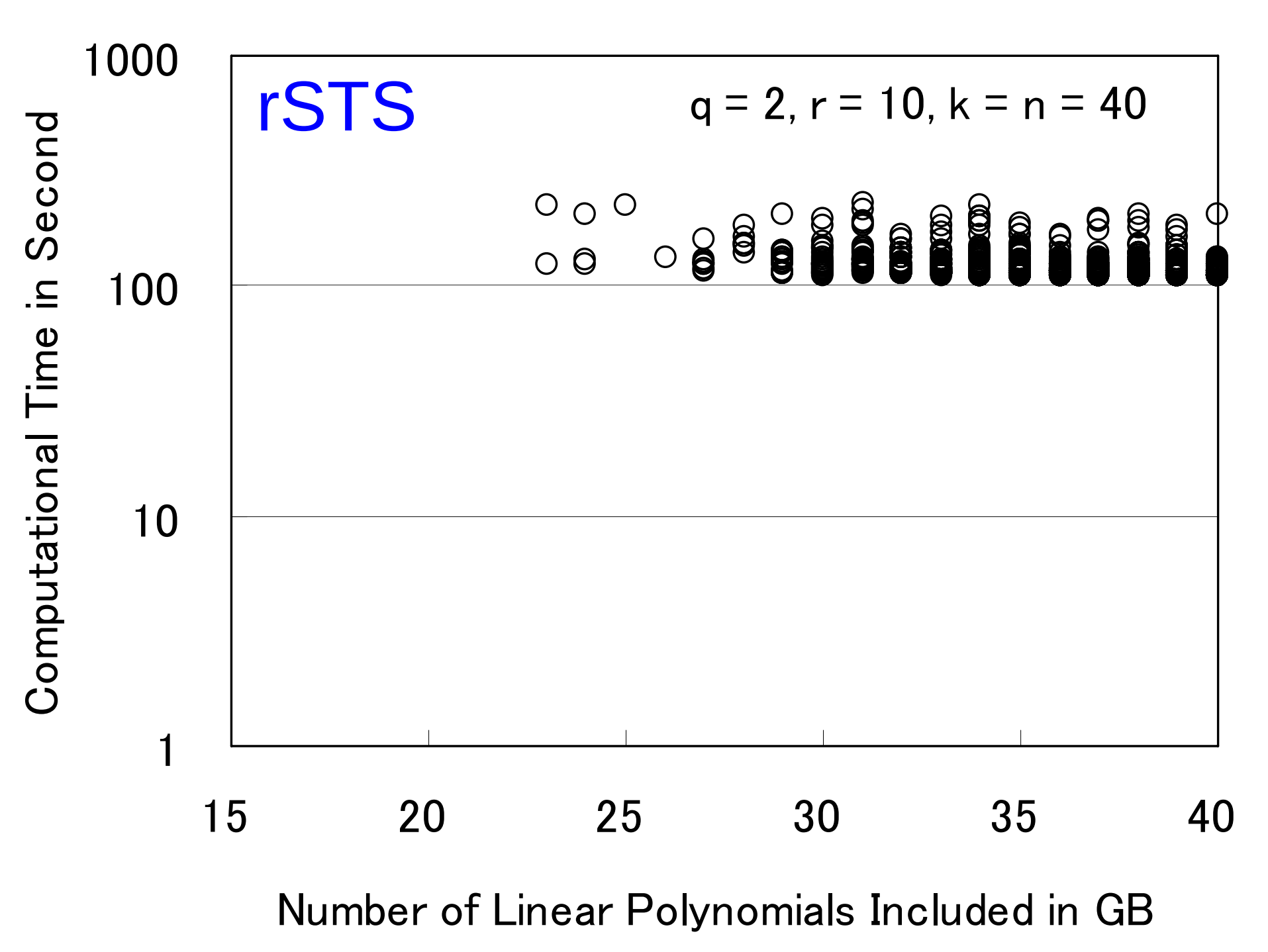
The attacker solves system of equations
using XL algorithm, Gröbner Basis computation, etc.

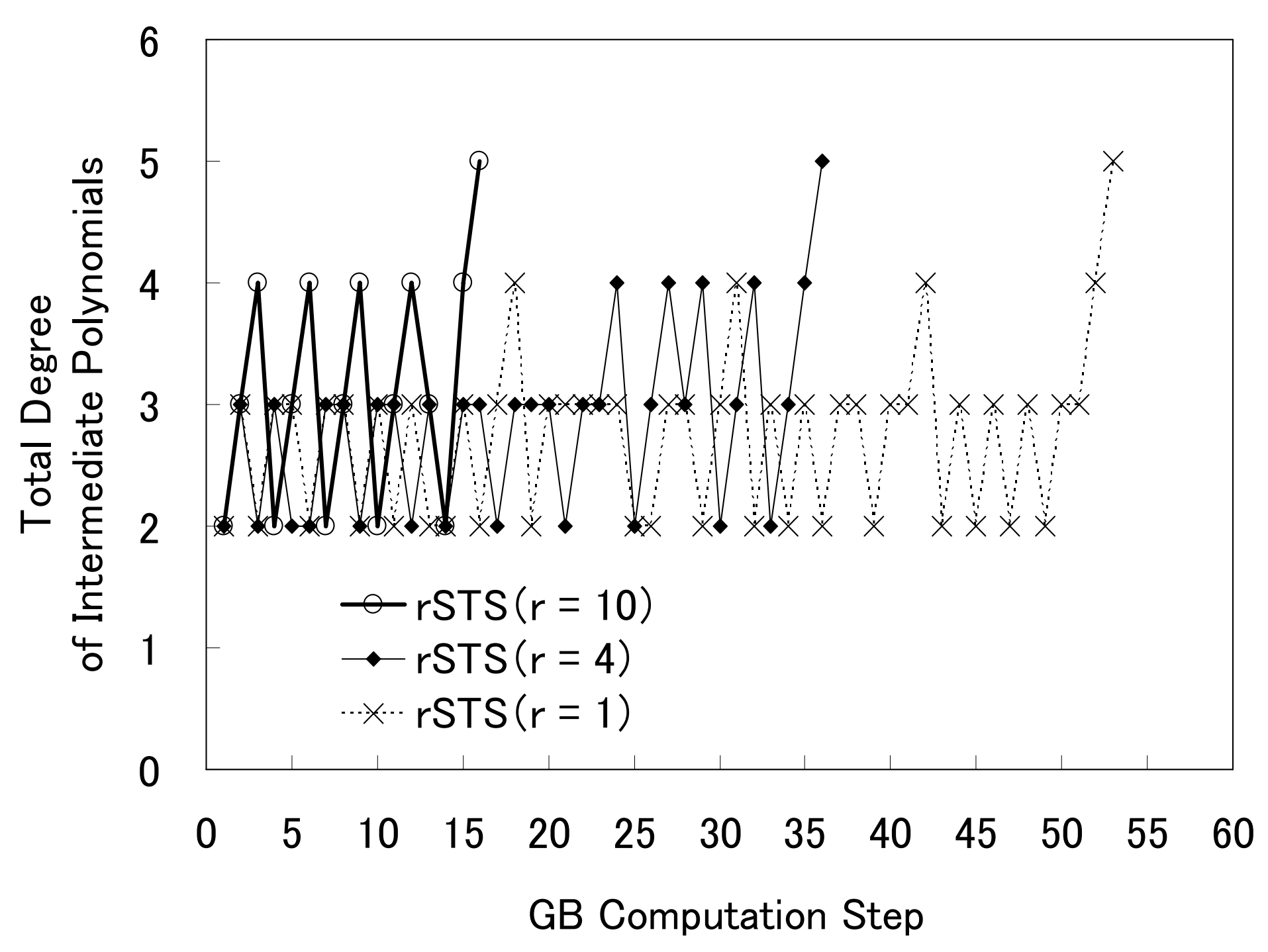
Contents

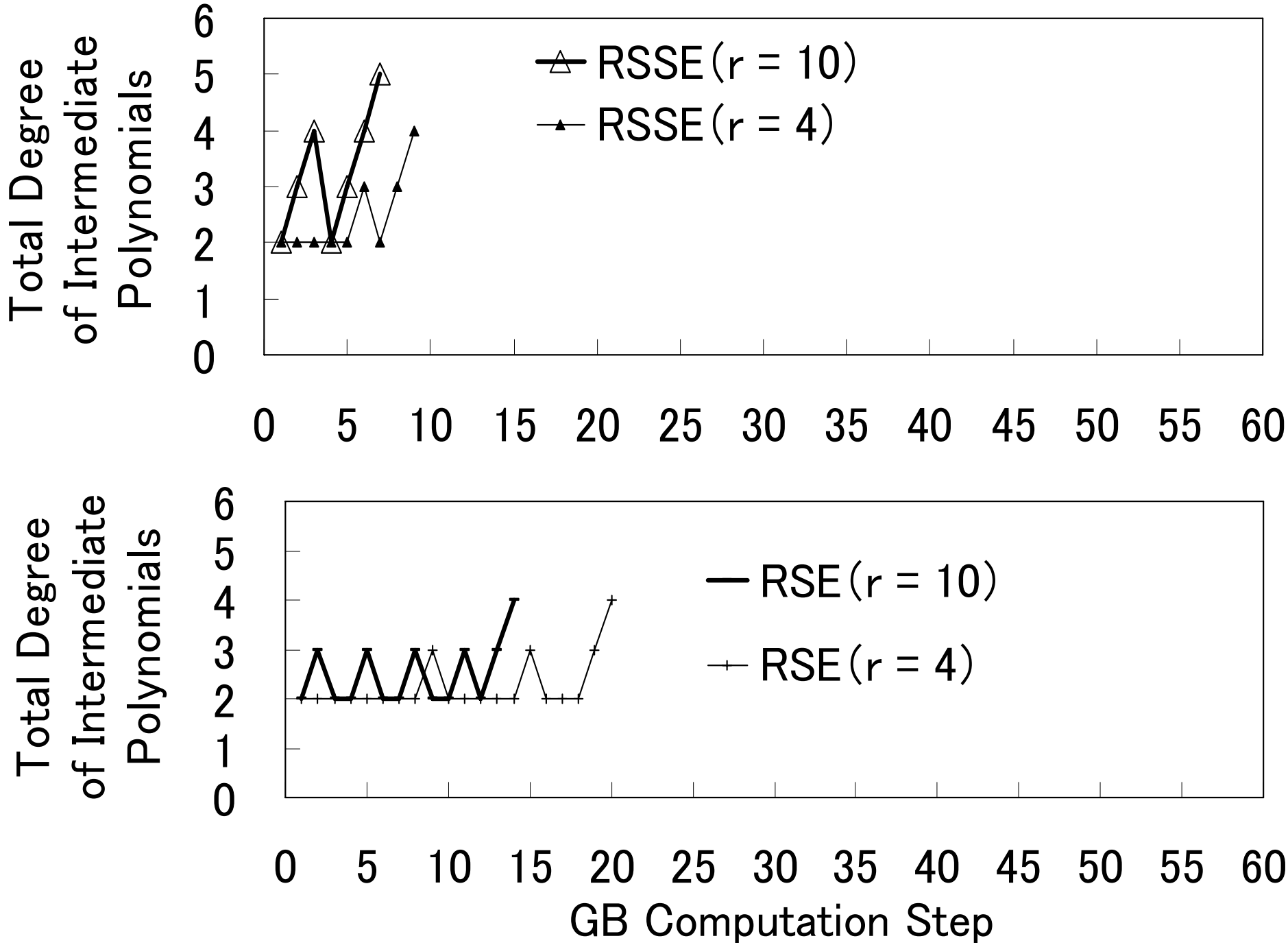
1. Introduction
2. Multivariate Quadratic
   Public Key Cryptosystems (MQPKCs)
   - rSTS type MPKC, R(S)SE
3. Algebraic Attack against MQPKC
4. Computer Experiments
   - Security of rSTS type MPKC
   - Security of R(S)SE
5. Concluding Remarks


rSTS
q = 2, r = 1, k = n = 40
1000
100
10
1
Computational Time in Second
15
20
25
30
35
40
Number of Linear Polynomials Included in GB


rSTS
q = 2, r = 4, k = n = 40
Computational Time in Second
1000
100
10
1
15
20
25
30
35
40
Number of Linear Polynomials Included in GB


rSTS
q = 2, r = 10, k = n = 40
1000
100
10
1
Computational Time in Second
15
20
25
30
35
40
Number of Linear Polynomials Included in GB


Total Degree
of Intermediate Polynomials
6
5
4
3
2
1
0
0
5
10
15
20
25
30
35
40
45
50
55
60
GB Computation Step
rSTS(r = 10)
rSTS(r = 4)
rSTS(r = 1)


Total Degree of Intermediate Polynomials
RSSE(r = 10)
RSSE(r = 4)
0
1
2
3
4
5
6
0 5 10 15 20 25 30 35 40 45 50 55 60
Total Degree of Intermediate Polynomials
RSE(r = 10)
RSE(r = 4)
0
1
2
3
4
5
6
0 5 10 15 20 25 30 35 40 45 50 55 60
GB Computation Step

Contents

1. Introduction
2. Multivariate Quadratic
   Public Key Cryptosystems (MQPKCs)
   - rSTS type MPKC, R(S)SE
3. Algebraic Attack against MQPKC
4. Computer Experiments
   - Security of rSTS type MPKC
   - Security of R(S)SE
5. Concluding Remarks

Concluding Remarks

- Security of rSTS type MPKCs
  against algebraic attacks

- R(S)SE = (?) rSTS type MPKCs
- intricate behavior
  of the degree of intermediate polynomials
  in GB computation
- We should not brush the matter off by saying that
  "Polynomial Time Complexity."

Challenges for the Future

- Research on Algebraic Attacks
  - Developing theories of GB attacks
  - Developing Efficient Algorithms,
    and Comparing their Performances:
    CS method, F5, PET SNAKE, PolyBoRi,
    MutantXL, HXL, Zhuang-Zi, …
- Theoretical Exploration of the Algebraic Structure
  - hypersurface over finite fields
- Security Analysis of the other type MPKCs
  - rSTS type MPKCs with several “modifiers”
  - STS (general STS) type MPKCs