Cryptosystems for Social Organizations based on TSK(Tsujii-Shamir-Kasahara) —MPKC

Shigeo Tsujii

Kohtaro Tadaki

Masahito Gotaishi

Ryo Fujita

Hiroshi Yamaguchi

Research & Development Initiative,
Chuo University

We are going to explain:

1. Introduction
2. Development of MPKC
3. Adaptability of TSK-MPKC to Social Organizations
4. Whole Structure of the Proposed System
5. Structure and Function of Perturbed TSK-MPKC
6. Structure and Function of PQ type TSK-MPKC
7. Simulation Result
8. Considerations for Security
9. Conclusion

1 Introduction

In secret communication, such as between a local government and a hospital, or among industrial companies, sending organizations are often unable to identify or decide the appropriate receiver in charge of the sending information.

In such a case, it is preferable that in the first place the sending organization sends an encrypted information to the representative (or secretary) of receiving organization

(e.g.. a hospital), then the representative of the hospital distributes

the received information and the corresponding key

to an adequate person who is responsible for the receiving information (e.g. a surgeon) without decrypting the encrypted Information.

While the application of public key cryptosystem to social organizations, Attribute Based Encryption and Functional Encryption are extensively being developed.

In such encryption systems, a sending organization has to identify or decide the qualified receiver in the receiving organization by

embedding the capacity of decryption of sending information in the encrypted data or the encryption key.

As an example, it is easy for broadcast companies to embed the capacity of viewing of charged television.

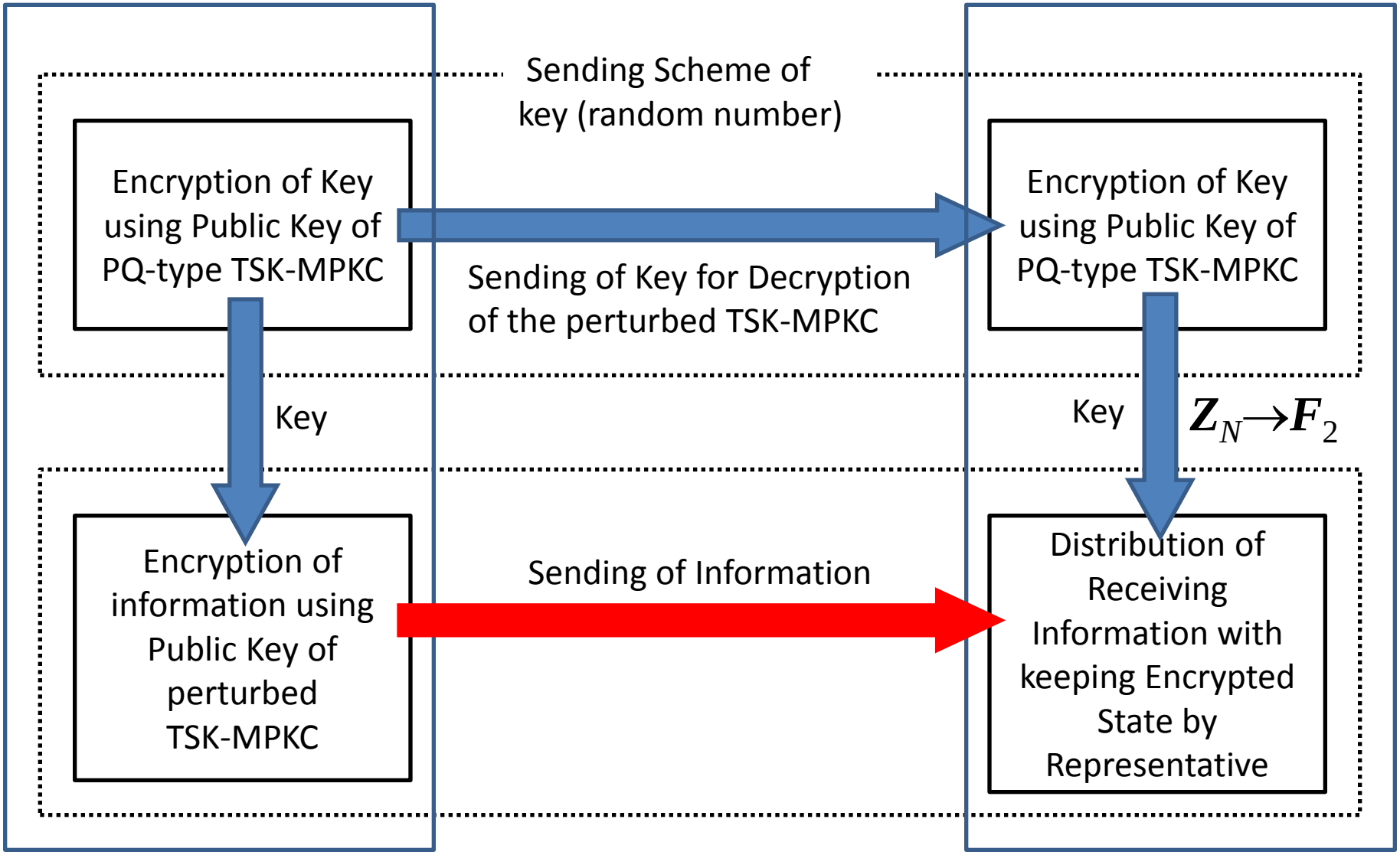
However, it is often difficult for sending organization to decide the qualified receiver.

In such cases, secret communication systems proposed in this presentation convince to be crucial.

Proposed system is composed of two subsystems;

Perturbed TSK-MPKC

PQ type TSK-MPKC

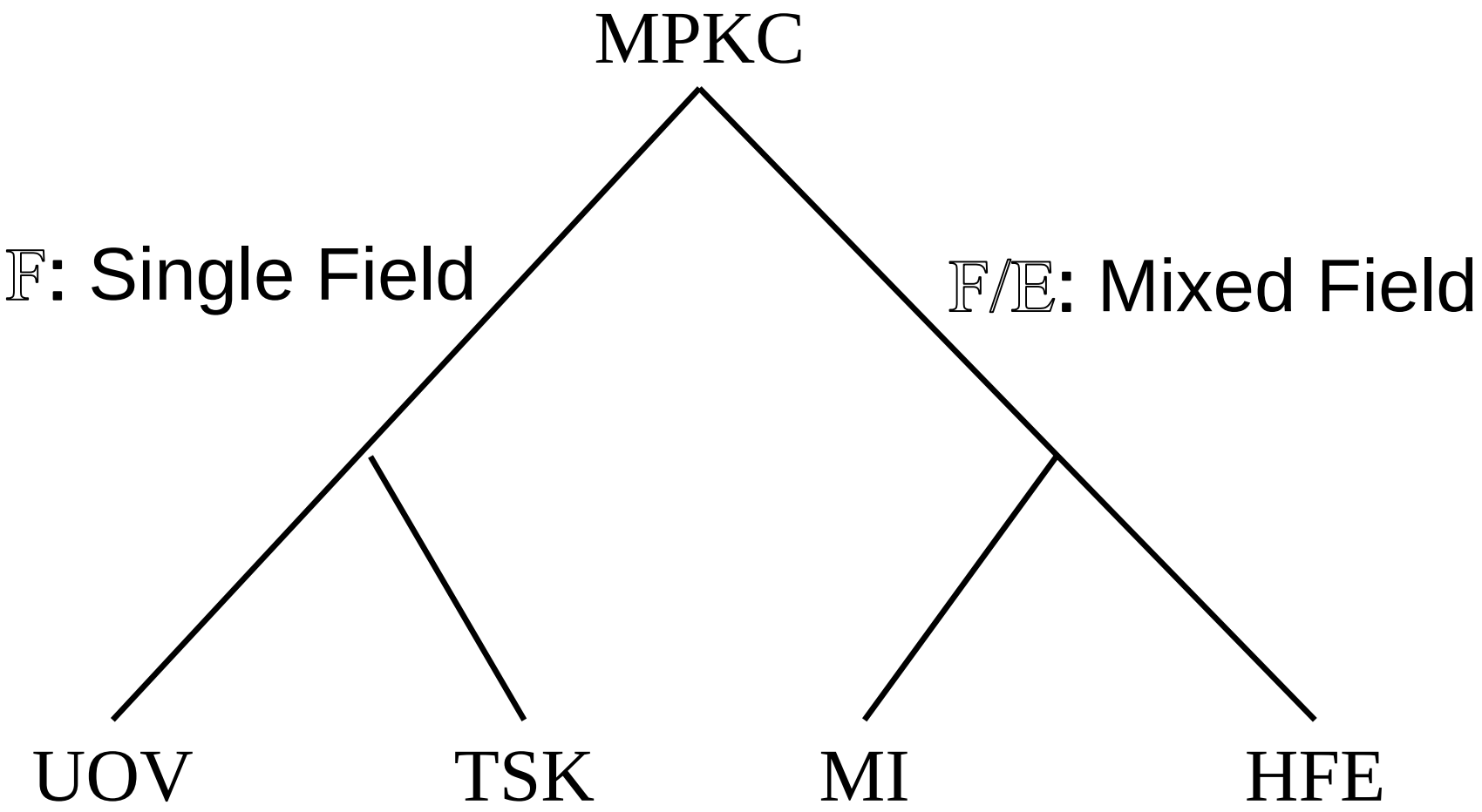

Sending Scheme of
key (random number)
Encryption of Key
using Public Key of
PQ-type TSK-MPKC
Sending of Key for Decryption
of the perturbed TSK-MPKC
Encryption of Key
using Public Key of
PQ-type TSK-MPKC
Key
Key
$Z_N \rightarrow F_2$
Encryption of
information using
Public Key of
perturbed
TSK-MPKC
Sending of Information
Distribution of
Receiving
Information with
keeping Encrypted
State by
Representative

2 Development of MPKC

Main Result of MPKC

type	1980s	1990s	2000s
MI-HFE SFLASHv3 signature (2003) (Matsumoto-Imai, Patarin)	MI Cryptosystem (1983) (encryption/signature) by Matsumoto, Imai, et al.	HFE Cryptosystem (1996) (encryption/signature) by Patarin	SFLASHv3 signature (2003) by Courtois et al. QUARTZ signature (2001) by Patarin et al.
TSK (Tsujii, Shamir, Kasahara-Sakai)	Sequential Solution Method (1985) (encryption) by Tsujii	Birational Permutation Signature Scheme (1993) by Shamir	Random (Singular) Simultaneous Equations (2004) (encryption/signature) by Kasahara-Sakai
OV-UOV signature (Patarin et al.)		OV signature (1997) by Patarin UOV signature (1999) by Kipnis et al.	Rainbow signature (2005) by Ding et al.
Algebraic Surface Cryptosystem (Akiyama et al.)			Algebraic Surface Cryptosystem (2009) by Akiyama et al.

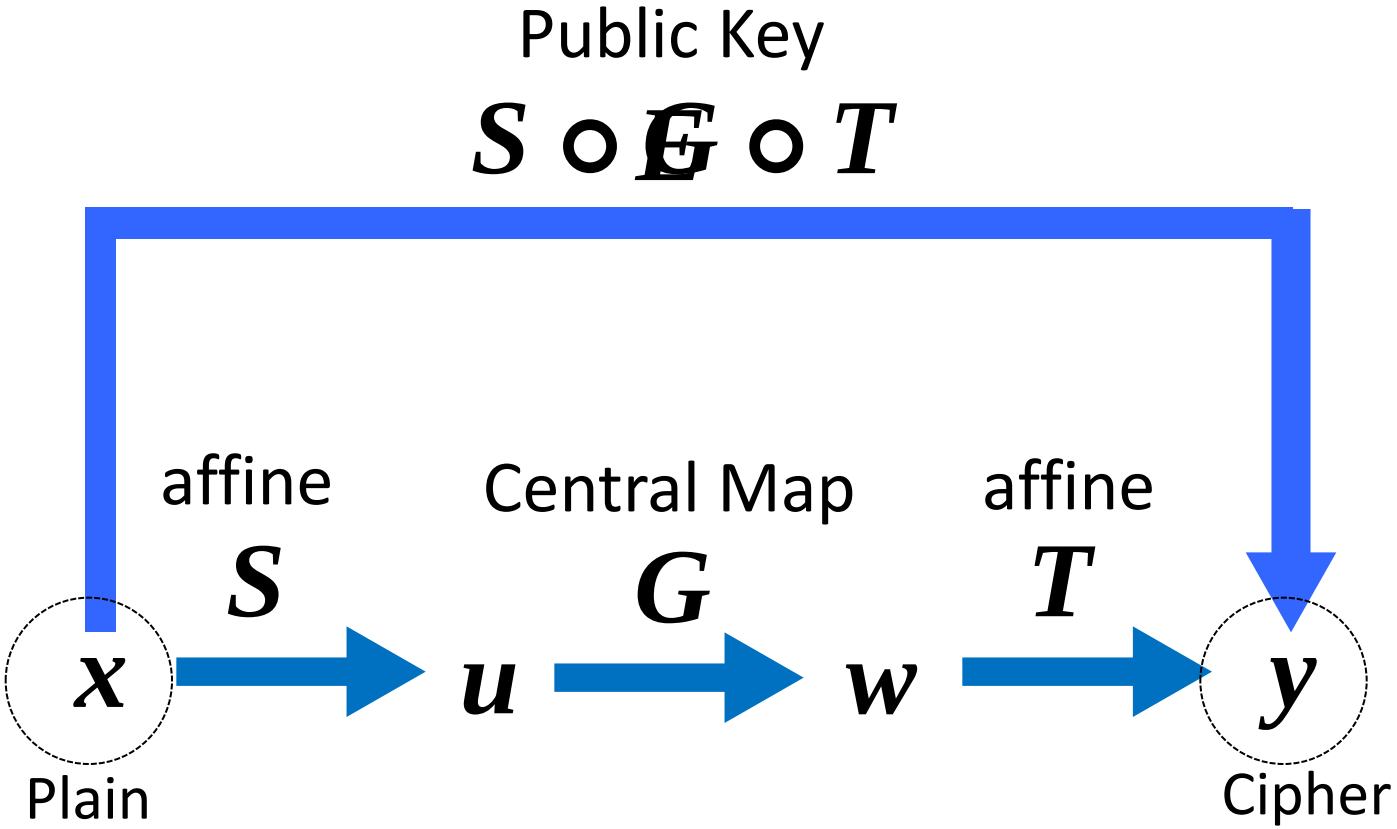
Classification of MPKC



Based on [Wolf, C., Preneel, B.: Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations. Cryptology ePrint Archive, Report 2005/077]

Background: Basic Information

Formulation of the Public Key



TSK-MPKC

Stepwise Triangular System of Central Map

$$
\begin{aligned}
w_1 &= f_1(x_1, \ldots, x_{m-1}, x_m) \\
w_2 &= f_2(x_1, \ldots, x_{m-1}) \\
&\vdots \\
w_{m-1} &= f_{m-1}(x_1, x_2) \\
w_m &= f_m(x_1)
\end{aligned}
$$

—Decrypted by solving univariate equation one by one.
—Quick decryption, but easily attacked
—Prey of Gröbner Base Attack which at that time (1985 ～1989）I did not notice.

cipher-text m dimensional vector $\boldsymbol{y}$ $=$ m degree affine transformation $\boldsymbol{y}=\boldsymbol{T}(\boldsymbol{v})$ $\circ$ m degree affine transformation $\boldsymbol{u}=\boldsymbol{S}(\boldsymbol{x})$ plain text m dimensional vector $\boldsymbol{x}$

$v_m = f_m(u_1, u_2, ...u_m)$
$v_{m-1} = f_{m-1}(u_1, u_2, ..u_{m-1})$
$\vdots$
$v_3 = f_3(u_1, u_2, u_3)$
$v_2 = f_2(u_1, u_2)$
$v_1 = f_1(u_1)$

$\boldsymbol{y}=(y_1, y_2, ...y_m)$
$y_i \in \boldsymbol{F}_2$, $i=1, 2, ...m$

$f_i(u_1, u_2, ...u_m)$, $i=1, 2, ...m$;
random quadratic polynomial
(only u_i is linear for all i)

$\boldsymbol{x}=(x_1, x_2, ...x_m)$
$x_i \in \boldsymbol{F}_2$, $i=1, 2, ...m$

3 Adaptaility of TSK-MPKC to Social Organizations

Comparison of Proposed system and Attribute-based Encryption (Functional Encryption)

	Proposed system	Attribute-based Encryption
Environ-ment	The sending organization is unable to identify an appropriate person in the receiving organization In the case for occasion demands	The sending organization accurately recognizes the qualification of each receiver in receiving group. routinely-used
Encryption method	TSK-MPKC, etc.	pairing , elliptic curve cryptosystem, ID-base

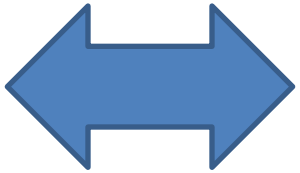
Analogy between MPKC(TSK)and Organization

infor-mation C	infor-mation B	infor-mation A
infor-mation C	infor-mation B	
infor-mation C		

The President has to access every information

Head of the Division in charge of info B & C

Section chief in charge of info C



$f_{3l}(v_1, v_2,.....v_{3l})$
.....
$f_{2l+2}(v_1, v_2,.....v_{2l+2})$
$f_{2l+1}(v_1, v_2,.....v_{2l+1})$

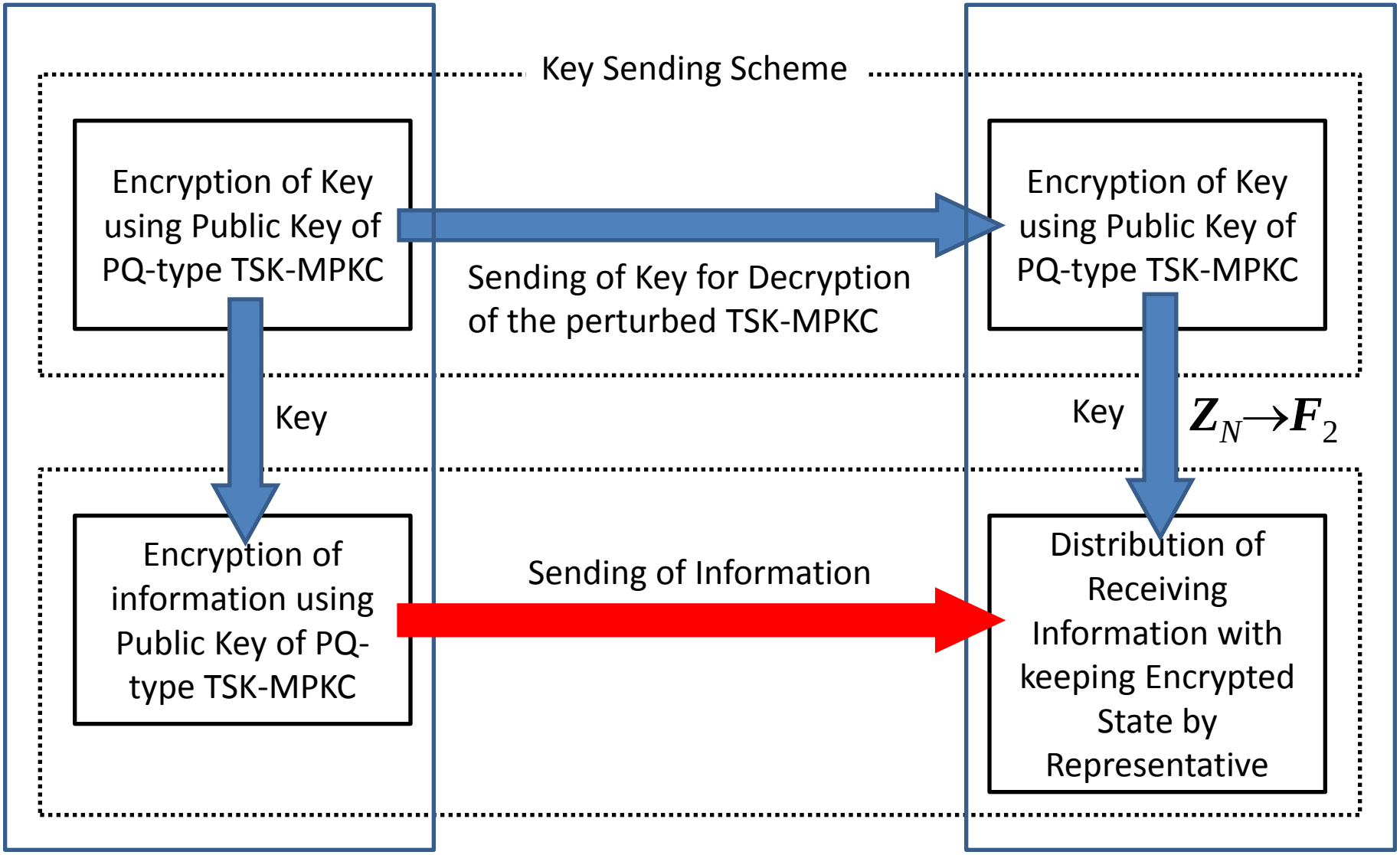
$f_{2l}(v_1, v_2,.....v_{2l})$
.....
$f_{l+2}(v_1, v_2,.....v_{l+2})$
$f_{l+1}(v_1, v_2,.....v_{l+1})$

$f_l(v_1, v_2,.....v_l)$
.....
$f_2(v_1, v_2)$
$f_1(v_1)$

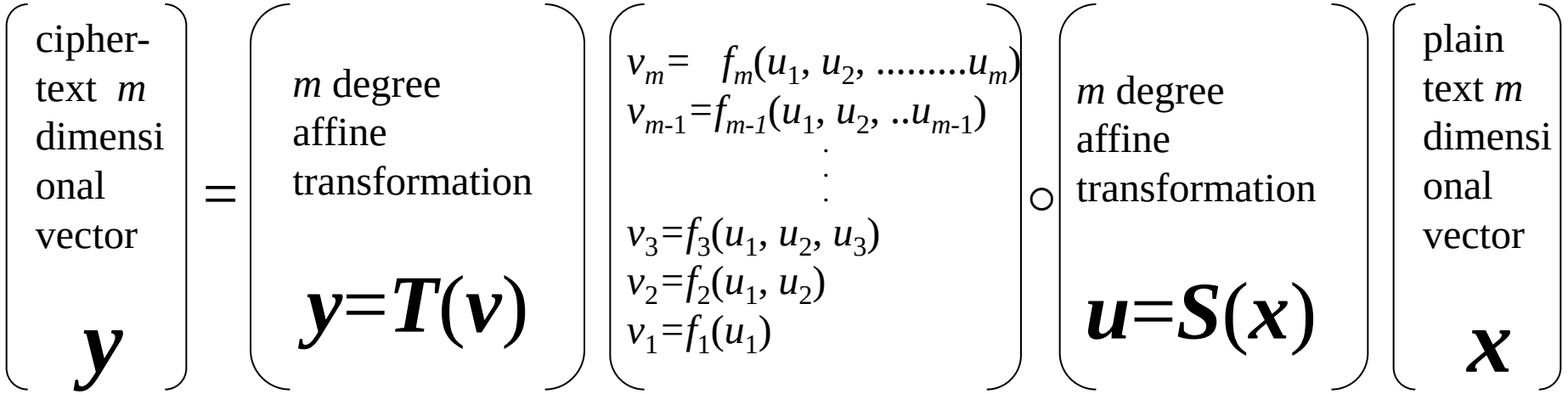
Example of Hierarchical Structure of social organizations

Structure of TSK-MPKC; hierarchical decryption

4 Whole Structure of Proposed System


Key Sending Scheme
Encryption of Key using Public Key of PQ-type TSK-MPKC
Sending of Key for Decryption of the perturbed TSK-MPKC
Encryption of Key using Public Key of PQ-type TSK-MPKC
Key
Key
$Z_N \rightarrow F_2$
Encryption of information using Public Key of PQ-type TSK-MPKC
Sending of Information
Distribution of Receiving Information with keeping Encrypted State by Representative

5 Structure and Function of Perturbed TSK-MPKC

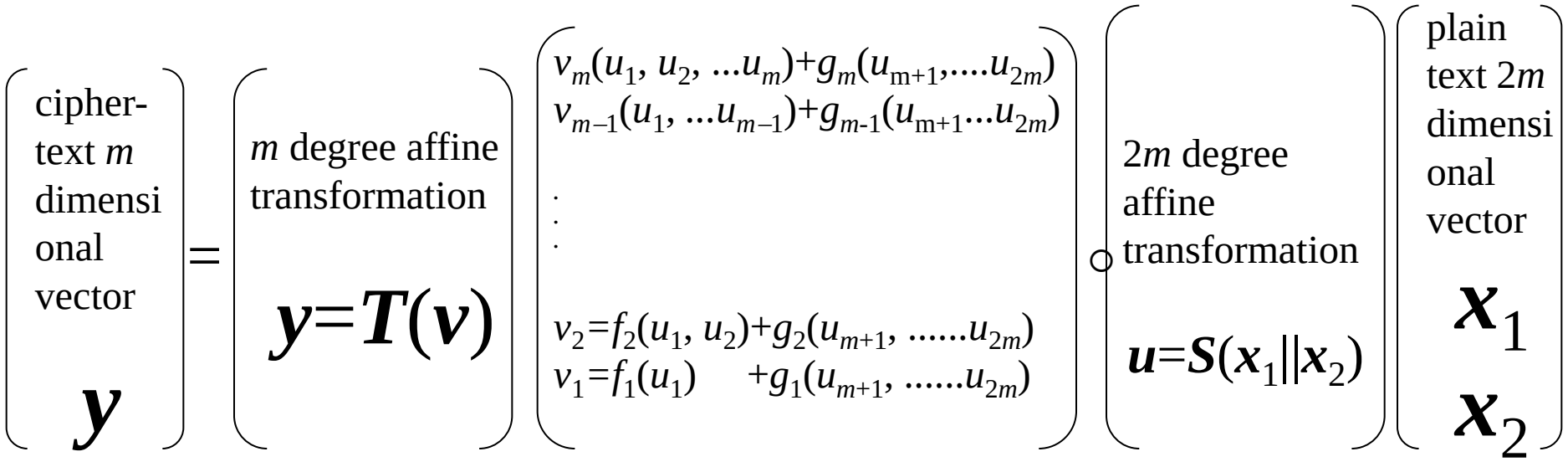


$\boldsymbol{y}=(y_1, y_2, ...y_m)$
$y_i \in \boldsymbol{F}_2$, i=1, 2, ...m

$f_i(u_1, u_2, ...u_m)$, i=1, 2, ...m;
random quadratic polynomial
(only u_i is linear for all i)

$\boldsymbol{x}=(x_1, x_2, ...x_m)$
$x_i \in \boldsymbol{F}_2$, i=1, 2, ...m

Original TSK-MPKC



$\boldsymbol{y}=(y_1, y_2, ...y_n)$
$y_i \in \boldsymbol{F}_2$, i=1, 2, ...m

$f_i(u_1, u_2, ...u_i)$, i=1, 2, ...m;
random quadratic polynomial
(only u_i is linear for all i)
$g_i(u_{m+1}, u_{m+2}, ..., u_{2m})$;
random quadratic n-variate
polynomial for all i.

$\boldsymbol{x}_1=(x_1, x_2, ...x_m)$
$\boldsymbol{x}_2=(x_{m+1}, ...x_{2m})$
$x_i \in \boldsymbol{F}_2$, i=1, 2, ...2m

Perturbed TSK-MPKC

Securuty of Perturbed TSK-MPKC

- The number of variables is $2m$
- The number of equations is $m \geqq 200$
- Groebner base attack is impossible.
- Unlike the cases of signature system, attackers do not have any freedom of assigning values to the extra variables in encryption systems. So rank attack is impossible.

6 Structure of PQ type TSK-MPKC

(1) Its security against quantum computing attack is given up

(2) Security is based on the difficulty of prime factorization

(SCC2013 “Construction of the Tsujii-Shamir-Kasahara (TSK) Type Multivariate Public Key Cryptosystem, which relies on the Difficulty of Prime Factorization”)

Theorem

Let $\boldsymbol{A}(\boldsymbol{x})$, $\boldsymbol{B}(\boldsymbol{x})$ be random systems of polynomials defined on the residual ring $\boldsymbol{Z}_N$ (N=pq)

Only $\boldsymbol{C}(\boldsymbol{x})$ is disclosed:

$$\boldsymbol{C}(\boldsymbol{x}):=p\boldsymbol{A}(\boldsymbol{x})+q\boldsymbol{B}(\boldsymbol{x})$$

– then:

It is as difficult as factoring N to find $\boldsymbol{A}(\boldsymbol{x})$ and $\boldsymbol{B}(\boldsymbol{x})$

($\boldsymbol{C}(\boldsymbol{x})$ does not have any term whose coefficient is divisible by p or q.)

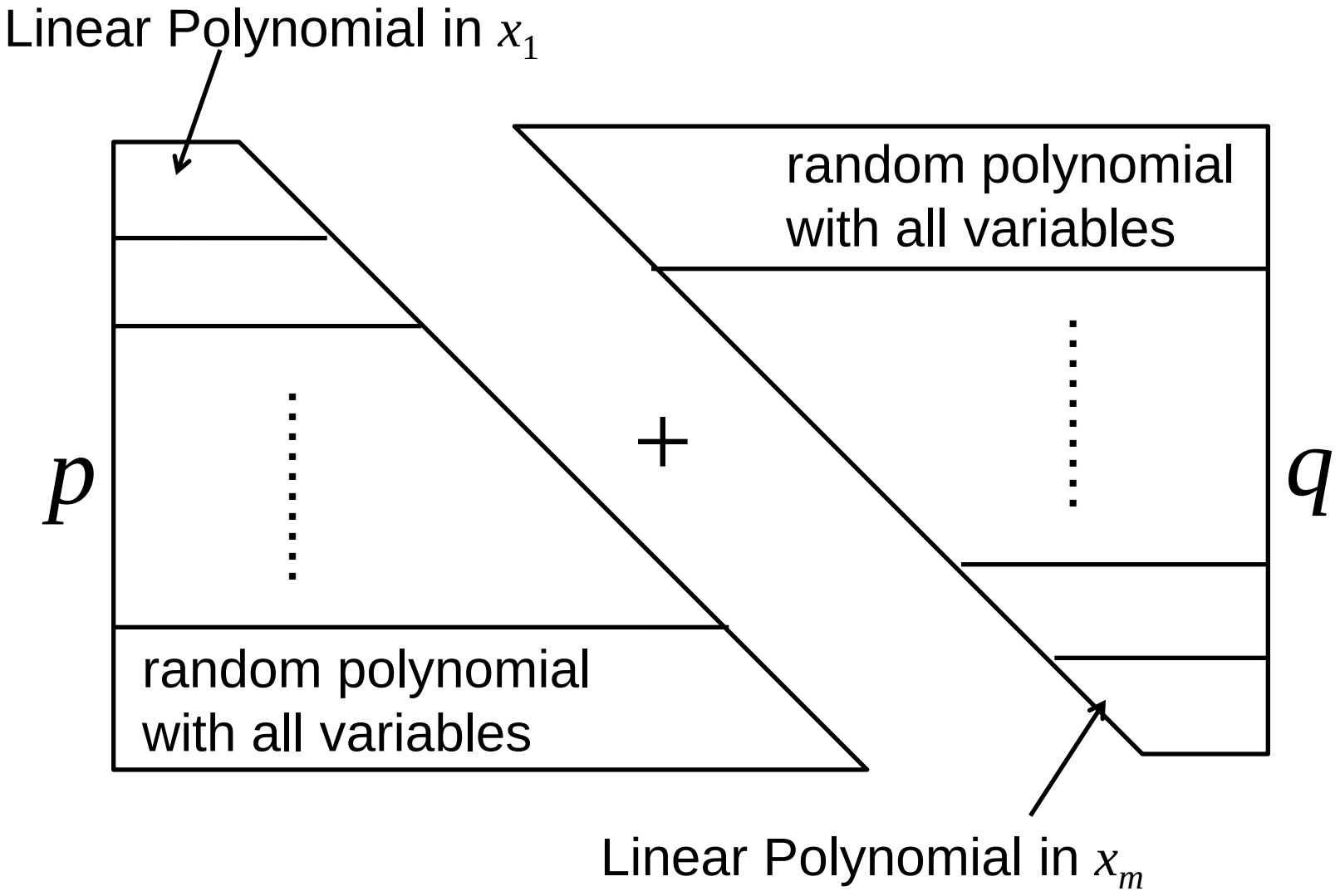
The Proposed System

- Combining two TSK together (p and q term)

$$p\begin{pmatrix} a_1(x_1, x_2, \ldots, x_m) \\ \boldsymbol{A}(\boldsymbol{x}) \\ a_m(x_m) \end{pmatrix} + q\begin{pmatrix} b_1(x_m) \\ \boldsymbol{B}(\boldsymbol{x}) \\ b_m(x_1, x_2, \ldots, x_m) \end{pmatrix}$$

- Residue Class Ring is used
- Above polynomial system is the central map and public key is generated by applying affine transformation

Structure of the Central Map



The Proposed PQ type TSK-MPKC

The Polynomial System defined on $Z_N(N=pq)$

$$p\begin{pmatrix} a_1(x_1,\ldots,x_m) \\ \vdots \\ \vdots \\ a_m(x_m) \end{pmatrix} + q\begin{pmatrix} b_1(x_m) \\ \vdots \\ \vdots \\ b_m(x_1,\ldots,x_m) \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

Each system is solved by transforming it to subfields, and afterwards plain text is computed using Chinese Remainder Theorem

The Proposed System

There is a unique pair of elements α, β such that $\alpha p+\beta q=1$ ($\alpha<q$, $\beta<p$).

$$\begin{pmatrix} a_1(x_1, x_2, \ldots, x_m) \bmod q \\ \vdots \\ \vdots \\ a_m(x_m) \bmod q \end{pmatrix} = \begin{pmatrix} \alpha \times y_1 \bmod q \\ \alpha \times y_2 \bmod q \\ \vdots \\ \alpha \times y_m \bmod q \end{pmatrix}$$

The equation system defined on the subfield $GF(q)$

Background: Theorem

Theorem:

Let $\boldsymbol{A}(\boldsymbol{x})$, $\boldsymbol{B}(\boldsymbol{x})$ be random systems of polynomials defined on the residual ring $\boldsymbol{Z}_N$ (N=pq)

Only $\boldsymbol{C}(\boldsymbol{x})$ is disclosed:

$$\boldsymbol{C}(\boldsymbol{x}):=p\boldsymbol{A}(\boldsymbol{x})+q\boldsymbol{B}(\boldsymbol{x})$$

– then:

It is as difficult as factoring N to find $\boldsymbol{A}(\boldsymbol{x})$ and $\boldsymbol{B}(\boldsymbol{x})$

($\boldsymbol{C}(\boldsymbol{x})$ does not have any term whose coefficient is divisible by p or q.)

Problem of Polynomial Algebra, with the equivalent difficulty as the Prime Factoring

A basic problem of polynomial algebra with the equivalent difficulty as the prime factorization is proposed.

Two prime numbers p, q are selected. $N:=pq$

The plain text vector $\boldsymbol{x}$ is an m-dimensional vector, with each element defined on the residue class ring $\boldsymbol{Z}_N$.

$$x=(x_1, x_2, ..., x_m)^T, x_i \in \boldsymbol{Z}_N, i=1, 2, ..., m$$

Two m-dimensional random polynomial vector $\mathbf{A}(\boldsymbol{x})$, $\boldsymbol{B}(\boldsymbol{x})$ are generated:

$$\boldsymbol{A}(\boldsymbol{x})=(a_1(\boldsymbol{x}), a_2(\boldsymbol{x}), ..., a_m(\boldsymbol{x}))^T$$

$$\boldsymbol{B}(\boldsymbol{x})=(b_1(\boldsymbol{x}), b_2(\boldsymbol{x}), ..., b_m(\boldsymbol{x}))^T$$

Subsequently, an m-dimensional quadratic polynomial vector $\boldsymbol{C}(\boldsymbol{x})$ on the residue class ring $\boldsymbol{Z}_N$ is defined using p, q, $\boldsymbol{A}(\boldsymbol{x})$, $\boldsymbol{B}(\boldsymbol{x})$

$$\boldsymbol{C}(\boldsymbol{x})=(c_1(\boldsymbol{x}),\ c_2(\boldsymbol{x}),\ \ldots,\ c_m(\boldsymbol{x}))^T=\boldsymbol{A}(\boldsymbol{x})p+\boldsymbol{B}(\boldsymbol{x})q$$

With the above assumption, the problem of finding the prime numbers p, q from the value of $\boldsymbol{C}(\boldsymbol{x})$ for a given value of $\boldsymbol{x}$, with $\boldsymbol{A}(\boldsymbol{x})$ and $\boldsymbol{B}(\boldsymbol{x})$ confidential, is discussed. This problem is called "prime factorization problem with additional information." Then the following theorem is proved:

Theorem: The following two conditions are equivalent.

(i)Prime factorization is difficult.

(ii)Prime factorization with additional information is difficult.

Proof of the Theorem

n is a security parameter. And for all positive integer l, $\mathbf{Z}_l$ is a set $\{0, 1, 2, ..., l-1\}$. First of all, the following experiment about the probabilistic algorithm A and the security parameter n is discussed:

$\text{Factor}_{\text{A}}(n)$:

1. Choose a pair (p, q) of two distinct $n/2$-bits prime uniformly.
2. Set $N:=pq$.
3. A is given N, and outputs $p'q'>1$.
4. The output of the experiment is defined to be 1 if $p'q'=N$, and 0 otherwise.

Definition 3.2. The remark that "A prime factoring problem is difficult" means that following proposition is true:

For all probabilistic algorithm A and security parameter d, exists a certain positive integer n_0 such that the following inequation is true for any $n > n_0$,

$$\Pr[\text{Factor}_{\text{A}}(n)=1] \leq 1/n^d$$

Let ℓ be a certain univariate polynomial with all its coefficients are positive integers. The following experiment is discussed about a given probabilistic polynomial time algorithm A and a security parameter n:

The factoring experiment with additional information Factor-AddInfo$_A(n)$:

1. Choose a pair (p, q) of two distinct $n/2$-bits prime uniformly.
2. Set $N := pq$.
3. Set $m := \ell(n)$.
4. Choose $\boldsymbol{a} \in \boldsymbol{Z}_N[x_1, x_2, ..., x_m]^m$ of total degree two uniformly.
5. Choose $\boldsymbol{b} \in \boldsymbol{Z}_N[x_1, x_2, ..., x_m]^m$ of total degree two uniformly.
6. Set $\boldsymbol{c} := p\boldsymbol{a} + q\boldsymbol{b}$
7. A is given N, c, and outputs $p'q' > 1$
8. The output of the experiment is defined to be 1 if $p'q' = N$, and 0 otherwise.

Background: Outline of the Proof

Prime Factorization of Additional Information

1. Choose a pair (p, q) of two distinct n=2-bits primes uniformly.
2. Set $N := pq$.
3. Set $m := \ell(n)$.
4. Choose $\boldsymbol{a}, \boldsymbol{b} \in Z_N[x_1,\ldots, x_m]^m$ of total degree two uniformly.
5. Set $c := p\boldsymbol{a} + q\boldsymbol{b}$.
6. A is given N, $\boldsymbol{c}$ and outputs $p_0, q_0 > 1$.
7. The output of the experiment is defined to be 1 if $p_0 q_0 = N$, and 0 otherwise.

Problem of Polynomial Algebra, with the equivalent difficulty as the Prime Factoring

A basic problem of polynomial algebra with the equivalent difficulty as the prime factorization is proposed.

Two prime umbers p, q are selected. $N:=pq$

The plain text vector $\boldsymbol{x}$ is an m-dimensional vector, with each element defined on the residue class ring $\boldsymbol{Z}_N$.

$$x=(x_1, x_2, ..., x_m)^T, x_i \in \boldsymbol{Z}_N, i=1, 2, ..., m$$

Two m-dimensional random polynomial vector $\mathbf{A}(\boldsymbol{x})$, $\boldsymbol{B}(\boldsymbol{x})$ are generated:

$$\boldsymbol{A}(\boldsymbol{x})=(a_1(\boldsymbol{x}), a_2(\boldsymbol{x}), ..., a_m(\boldsymbol{x}))^T$$

$$\boldsymbol{B}(\boldsymbol{x})=(b_1(\boldsymbol{x}), b_2(\boldsymbol{x}), ..., b_m(\boldsymbol{x}))^T$$

Definition 3.3. The remark that "A prime factoring problem with additional information is difficult" means that following proposition is true:

For all probabilistic polynomial time algorithm A and all positive integer d, exists a positive integer n_0 such that following inequation is true.

$$\Pr[\text{Factor-Addinfo}_{A'}(n)=1] \leq 1/n^d$$

With the above preparation, the following theorem is proved.

Theorem 3.4. The following two conditions are equivalent.

(i) Prime factorization is difficult

(ii) Prime factorization with additional information is difficult.

The proposition that (ii)→(i) is obvious.

Next (i)→(ii) is proved. Beforehand following Lemma needs to be proved. Here #S means the number of the elements of a given finite set S.

Lemma 3.5. Let p and q be two prime numbers. Let $N{:=}pq$. Mapping F: $\boldsymbol{Z}_N \times \boldsymbol{Z}_N \rightarrow \boldsymbol{Z}_N$ is defined as follows:

$$F(x, y)=(px+qy) \mod N$$

Then we have following equality for all $z \in \boldsymbol{Z}_N$.

$$F(\{z\})=N \qquad (3)$$

[Proof] Since both p and q are prime, there exist integers x_0, y_0 such that $px_0+qy_0=1$. Subsequently , a subset S_z of $\boldsymbol{Z}_N \times \boldsymbol{Z}_N$ is defined as:

$$S_z := \{(x_0 z+q\alpha) \bmod N, (y_0 z+p\beta \bmod N) \mid \alpha \in \boldsymbol{Z}_p, \beta \in \boldsymbol{Z}_q\}$$

It should be noted that for all $z \in \boldsymbol{Z}_N$, we have the equality:

$$F(S_z)=z$$

Therefore for any different elements z, $z' \in \boldsymbol{Z}_N$, we have the equality:

$$S_z \cap S_{z'} = \phi$$

On the other hand, since $\#\boldsymbol{Z}_p=p$ and $\#\boldsymbol{Z}_q=q$, for all $z \in \boldsymbol{Z}_N$, we have the following relation:

$$\#S_z=pq=N$$

(end of the proof)

Based on the Lemma 3.5, (i)→(ii) in the Theorem is proved as follows:

Here following experiment about a given probabilistic polynomial time algorithm A and n:

The factoring experiment with dummy information Factor-DmmyInfo$_A(n)$:

1.Choose a pair of two distinct $n/2$-bits prime uniformly.

2.Set $N{:=}pq$.

3.Set $m{:=}\ell(n)$.

4.Choose $\boldsymbol{c}\in\boldsymbol{Z}_N[x_1, x_2, ..., x_m]^m$ of total degree two uniformly.

5.A is given N, $\boldsymbol{c}$, and outputs p', $q' > 1$

6.The output of the experiment is defined to be 1 if $p'q'{=}N$, and 0 otherwise.

Based on the Lemma 3.5, the polynomial vector c generated by the step 4-6 of the Factor-AddInfo$_A(n)$ is homogeneously generated from a set of quadratic polynomial vectors in $\boldsymbol{a} \in \boldsymbol{Z}_N[x_1, x_2, ..., x_m]^m$. Consequently for a given probabilistic polynomial time algorithm A and a security parameter n, we have the following equality:

$$\Pr[\text{Factor-Dmmyinfo}_{A'}(n)=1] = \Pr[\text{Factor}_{A'}(n)=1]$$

Here let A be a given probabilistic polynomial-time algorithm, which has positive integers and polynomial vectors as its inputs. Based on the algorithm A, a probabilistic polynomial-time algorithm A′ is structured as follows:

A' has the positive integer N as its input. A' gnerates a quadratic polynomial vector c homogeneously. After that, it invokes the algorithm A inputing N and $\boldsymbol{c}$. Then we have the following equality for a given security parameter n:

$$\Pr[\text{Factor-Dmmyinfo}_{A'}(n)=1] = \Pr[\text{Factor}_{A'}(n)=1] \quad (4)$$

Here it is assumed that the prime factorization is difficult. Then for all positive integer d, there exists a positive integer n_0 such that for all $n>n_0$,

$$\Pr[\text{Factor-Addinfo}_{A'}(n)=1] \leq 1/n^d \quad (5)$$

Since A can be any algorithm, it is led from the equation (4) and (5) that a prime factorization problem with additional information is difficult.

Discussion of Security of PQ-TSK 1

- Direct Attack
  - Polynomials of public key are transformed by two affine transformation so that no coefficient is divisible by p or q
  - The public key is virtually the same as random systems from attakers.

Discussion of Security of PQ-TSK 2

1）It is impossible to separate the public key $\boldsymbol{C}(\boldsymbol{x})$ into $\boldsymbol{A}(\boldsymbol{x})$ and $\boldsymbol{B}(\boldsymbol{x})$ without knowing p or q.

2) Neither p nor q is worked out with any probabilistic algorithm with the public key as the input (Theorem).

3) Although two polynomial systems have the TSK trapdoor structure, all polynomials of central map have the same rank and rank attack is impossible. So extracting any p term or q term is convinced to be impossible

Discussion
efficiency of whole system

- PQ-TSK ; although encryption and decryption take time due to residue ring, PQ-TSK is used for key (random number for perturbation in perturbed TSK). So in advance of transmission of information , key can be sent using PQ-TSK.

- The same key (random number for perturbation) could be used repeatedly for different perturbed TSK.

Discussion
security of whole system

- PQ-TSK is secure
- Perturbed TSK is secure
- Whole system is secure

Conclusion

- Cryptosystem for Social Organizations based on PQ type TSK-MPKC and Perturbed TSK-MPKC is proposed.

  Practical applications in the fields of electronic government and electronic medicare systems are now being considered.

Thank you for listening

ANY QUESTIONS?