PQC 2016 Hot Topic Session

Multi-Prime Numbers MPKC for Post-Quantum Cryptosystem

Shigeo Tsujii, Masahito Gotaishi, Ryo Fujita

Chuo University

100～200 prime numbers

(1) **We prepare set P including many prime numbers and the product of all these prime numbers is set as the public modulus *N* of the proposed system.**

- **Since every prime number is small, it is easy for attackers to reveal them although prime numbers are not disclosed.**

$$\begin{pmatrix} K\text{-th ciphertext vector} \\ \boldsymbol{y} \end{pmatrix} = \begin{pmatrix} K\text{-th regular transformation} \\ T \end{pmatrix} \begin{pmatrix} x_1 + h_1(\boldsymbol{x})\,[G_1\,(G_1^{-1} \bmod F_1)] \\ \qquad + 2\,h_1(\boldsymbol{x})\,[F_1\,(F_1^{-1} \bmod G_1)] \\ x_2 + h_2(\boldsymbol{x})\,[G_2\,(G_2^{-1} \bmod F_2)] \\ \qquad + 2\,h_2(\boldsymbol{x})\,[F_2\,(F_2^{-1} \bmod G_2)] \\ \cdots\cdots \\ x_K + h_K(\boldsymbol{x})\,[G_K\,(G_K^{-1} \bmod F_K)] \\ \qquad + 2\,h_K(\boldsymbol{x})\,[F_K\,(F_K^{-1} \bmod G_K)] \end{pmatrix} \begin{pmatrix} K\text{-th plaintext vector} \\ \boldsymbol{x} \end{pmatrix} \bmod N$$

F_i and G_i ($i = 1, 2, ..., K$) are mutually prime.

$h_i(\boldsymbol{x})$: random quadratic polynomials in K variables ($i = 1, 2, \ldots, K$)

Toy Example ($L = 7$, K＝3)

$P = \{11,13,17,19,23,29,31\}$
$N = 11 \times 13 \times 17 \times 19 \times 23 \times 29 \times 31$
$\quad = 955{,}049{,}953$

k	F_k	G_k
1	$F_1 = 11 \times 13 \times 19 \times 31$ $= 84{,}227$	$G_1 = 17 \times 23 \times 29$ $= 11{,}339$
2	$F_2 = 11 \times 17 \times 23 \times 31$ $= 133{,}331$	$G_2 = 13 \times 19 \times 29$ $= 7{,}163$
3	$F_3 = 13 \times 29 \times 31$ $= 11{,}687$	$G_3 = 11 \times 17 \times 19 \times 23$ $= 81{,}719$

Note (1) F_k and G_k have no common prime number for same k
(2) For different k, common prime number(s) are included in F_k and G_k

Practical Example

P; {2,3,5, ・ ・ ・ ,337,347, ・ ・ ・ ,1217,1223}

There are 196 prime numbers between 2 and 1223,

modulus N is about 2000 bits.

Structure of the Central Map

- **2K subsets P_{Fk} and P_{Gk} are chosen from P and kept secret against brute force attack,**

- **where K is the degree of central map vector**
- **and k=1, 2, …, K**
- **For the same k, P_{Fk} and P_{Gk}, they do not share any divisor.**

Security against prime number substitution attack

- **Each polynomial of central map vector is sum of an element,**
- **x_i of plaintext vector X and a quadratic polynomial with all variables of plaintext**
- **Every quadratic polynomial includes F_k and G_k (secret products of all elements of each subset corresponding to P_{Fk} and P_{Gk}**
- **where F_k and G_k are coprime.**
- **Against this structure for attackers it is impossible to eliminate each quadratic polynomial and endures prime number substitution attack.**

Table 2 Comparison of the Time to Compute Gröbner Bases

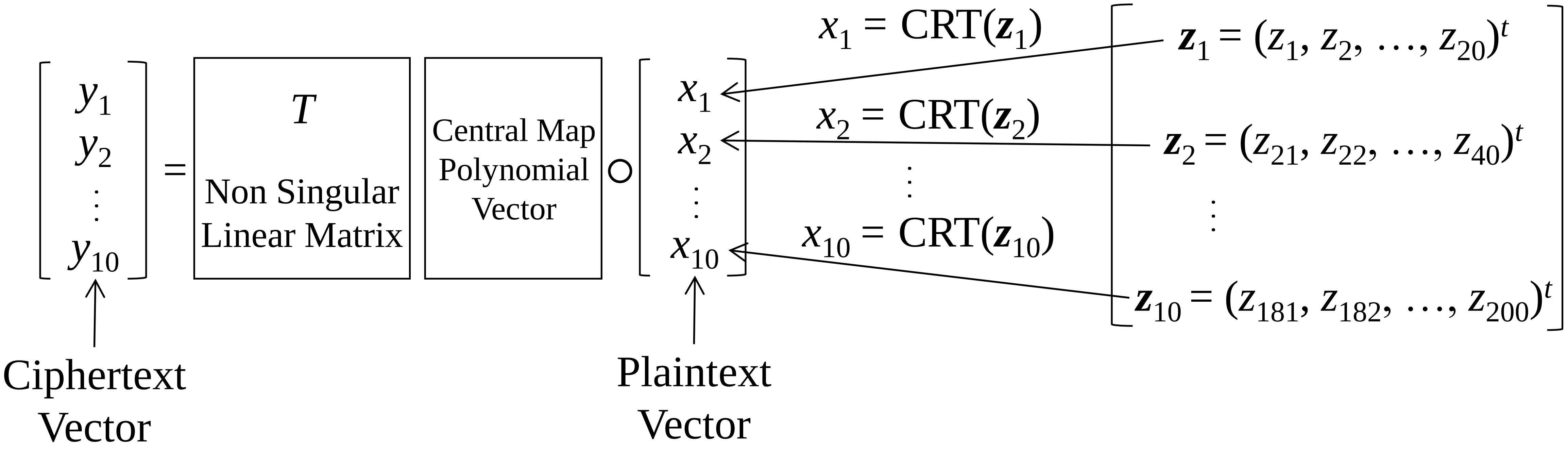
	$K=8$ $N \approx 2^{160}$	$K=9$ $N \approx 2^{180}$	$K=10$ $N \approx 2^{200}$	$K=11$ $N \approx 2^{220}$	$K=12$ $N \approx 2^{240}$	$K=13$ $N \approx 2^{260}$	$K=14$ $N \approx 2^{280}$
Proposed Scheme	0.07 sec.	0.36 sec.	2 sec.	15 sec.	118 sec.	901 sec.	6872 sec.
Random System	0.07 sec.	0.37 sec.	2 sec.	15 sec.	115 sec.	900 sec.	6858 sec.

Table 3 Comparison of the Maximum Degree of Polynomials to Compute Gröbner Bases

	$K=8$ $N \approx 2^{160}$	$K=9$ $N \approx 2^{180}$	$K=10$ $N \approx 2^{200}$	$K=11$ $N \approx 2^{220}$	$K=12$ $N \approx 2^{240}$	$K=13$ $N \approx 2^{260}$	$K=14$ $N \approx 2^{280}$
Proposed Scheme	$d_{max}=10$	$d_{max}=11$	$d_{max}=12$	$d_{max}=13$	$d_{max}=14$	$d_{max}=15$	$d_{max}=16$
Random System	$d_{max}=10$	$d_{max}=11$	$d_{max}=12$	$d_{max}=13$	$d_{max}=14$	$d_{max}=15$	$d_{max}=16$

Introduction of CRT Part in Front Stage

- **Considering the recent growth of IoT(Internet of Things), where many small size data are gathered and processed, it may be desirable that CRT(Chinese Remainder Theorem) is installed at front stage**
- **Since CRT is linear processing and central part is quadratic polynomial,**
  Introducing this CRT section sharply reduce the size of central map instead of that the size of each plaintext x_k has to be reduced according to the number of variables of each CRT part z_k.



$$x_k = \mathrm{CRT}(\boldsymbol{z}_k) = \sum_{i=1}^{20} \left(z_i \prod_{\substack{j=1 \\ j \neq i}}^{20} N_{kj} \cdot (N_{kj}^{-1} \bmod N_{ki}) \right)$$

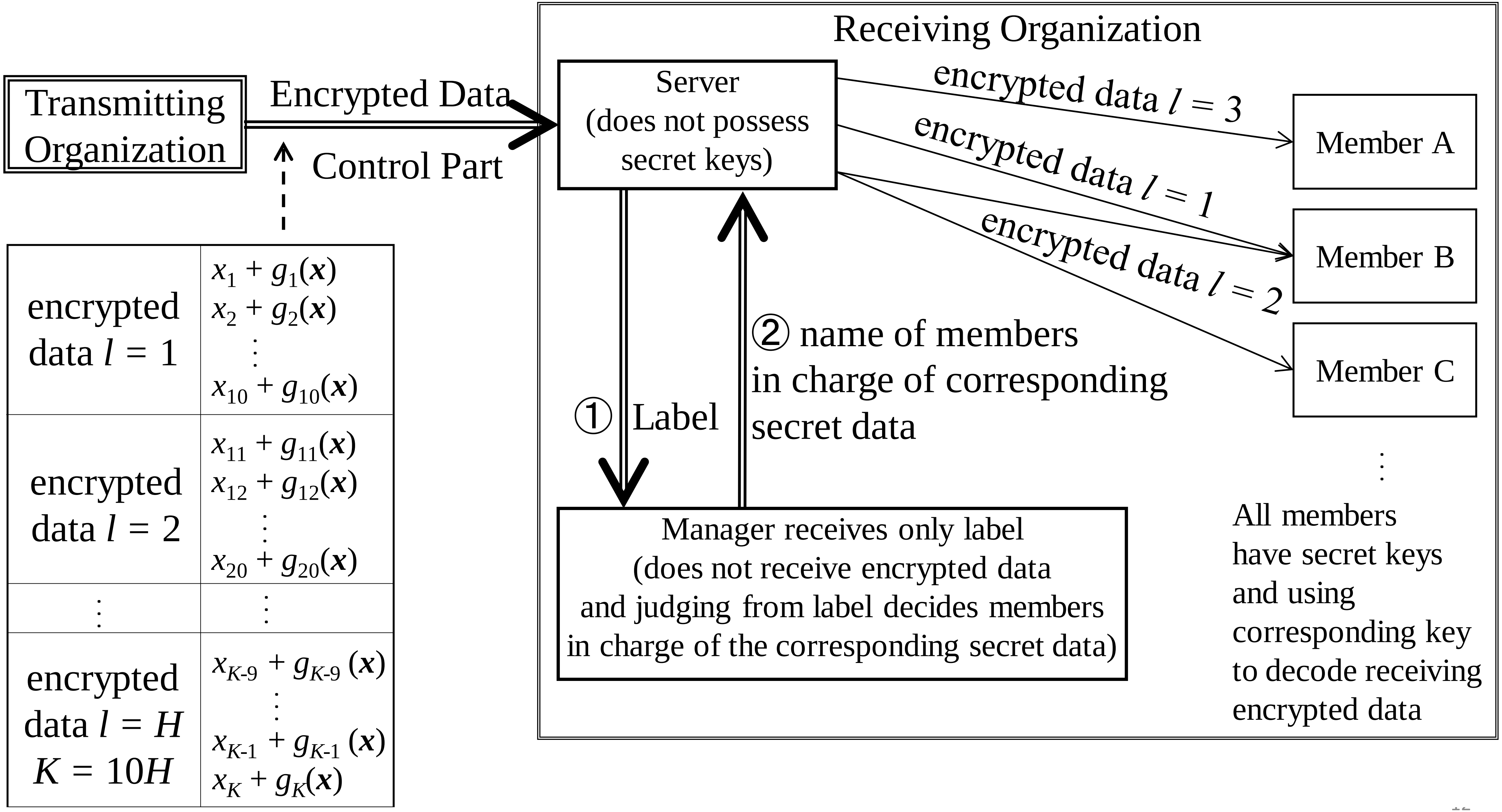
$$N = \prod_{i=1}^{20} N_{ki} \qquad (k = 1, 2, \ldots, 10)$$

N_{ki} and N_{kj} $(i \neq j)$ are co-prime each other.

Application to organizational communications

Unlike ordinary public key cryptosystems such as RSA, the proposed MPKC has special advantage in application to organizational communications.

The proposed multi-prime MPKC can be applied to distributing system of encrypted data (without decoding) to plaintext to appropriate members who are in charge of the receiving data in a organization.


Transmitting Organization
Encrypted Data
Control Part
encrypted data $l = 1$
$x_1 + g_1(\boldsymbol{x})$
$x_2 + g_2(\boldsymbol{x})$
⋮
$x_{10} + g_{10}(\boldsymbol{x})$
encrypted data $l = 2$
$x_{11} + g_{11}(\boldsymbol{x})$
$x_{12} + g_{12}(\boldsymbol{x})$
⋮
$x_{20} + g_{20}(\boldsymbol{x})$
⋮
encrypted data $l = H$
$K = 10H$
$x_{K\text{-}9} + g_{K\text{-}9}(\boldsymbol{x})$
⋮
$x_{K\text{-}1} + g_{K\text{-}1}(\boldsymbol{x})$
$x_K + g_K(\boldsymbol{x})$
Receiving Organization
Server
(does not possess secret keys)
encrypted data $l = 3$
encrypted data $l = 1$
encrypted data $l = 2$
Member A
Member B
Member C
⋮
① Label
② name of members in charge of corresponding secret data
Manager receives only label
(does not receive encrypted data
and judging from label decides members
in charge of the corresponding secret data)
All members have secret keys and using corresponding key to decode receiving encrypted data

Literature

(1) Shigeo TSUJII), Kohtaro TADAKI), Ryo FUJITA),*and* Masahito GOTAISHI;
Proposal of the Multivariate Public Key Cryptosystem
relying on the difficulty of Factoring a product of Two Large Prime numbers,
IEICE transactions on Fundamentals of Electronics,Communications,
and Computer Sciences Vol.E99-A No.1 JANUARY 2016

(2) Shigeo Tsujii, Ryo Fujita, Masahito Gotaishi, and Masao Kasahara;
Proposal of Multivariate Public Key Cryptosystem (MPKC) based on Random
Quadratic Polynomials using Chinese Remainder
Theorem with Numerous Prime Numbers,
SCIS (symposium on Cryptography and informarion Security)2016,
JANUARY 2016 KUMAMOTO).