

# Nonlinear Piece In Hand Perturbation Vector Method for Enhancing Security of Multivariate Public Key Cryptosystems

October 19, 2008

The Second International Workshop on  
Post-Quantum Cryptography (PQCrypto 2008)  
University of Cincinnati

Osamu Fujita	Institute of Information Security
Kohtaro Tadaki	Chuo University
Shigeo Tsujii	Institute of Information Security

Supported by SCOPE  
from the Ministry of Internal Affairs and Communications of Japan

# Contents

## 1. Piece In Hand (PH) Method

- Piece In Hand Concept
- Purpose of PH Method

## 2. NonLinear PH Perturbation Vector (NLPHPV) Method

- Schemes of Multivariate Public Key Cryptosystems
- Design Principle of NLPHPV Method
- Public Key Construction, Decryption
- Security of NLPHPV Method

## 3. Future Study

# Contents

## 1. Piece In Hand (PH) Method

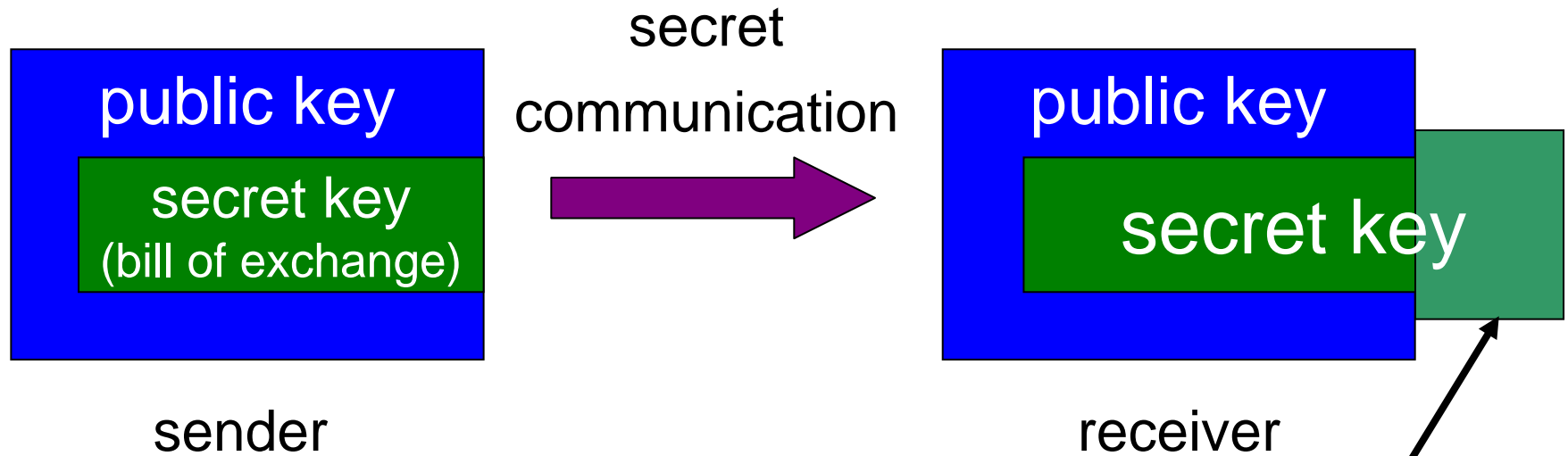
- Piece In Hand Concept
- Purpose of PH Method

## 2. NonLinear PH Perturbation Vector (NLPHPV) Method

- Schemes of Multivariate Public Key Cryptosystems
- Design Principle of NLPHPV Method
- Public Key Construction, Decryption
- Security of NLPHPV Method

## 3. Future Study

# What is the Piece In Hand Concept? (1/2)



aim to enhance the security by using effectively random variables

PH:  
Piece In  
Hand

# What is the Piece In Hand Concept? (2/2)

enhancing security of MPKC

Piece In  
Hand:  
PH



PH



PH



PH



PH



...

Sequential  
Solution  
Method

MI

TTM

R(S)SE

QIC

etc.

general concept which is applicable to any MPKC

# What is the PH Method ?

- A method to realize the Piece In Hand Concept (Tsuji, Tadaki, Fujita)

2003 Piece In Hand Concept

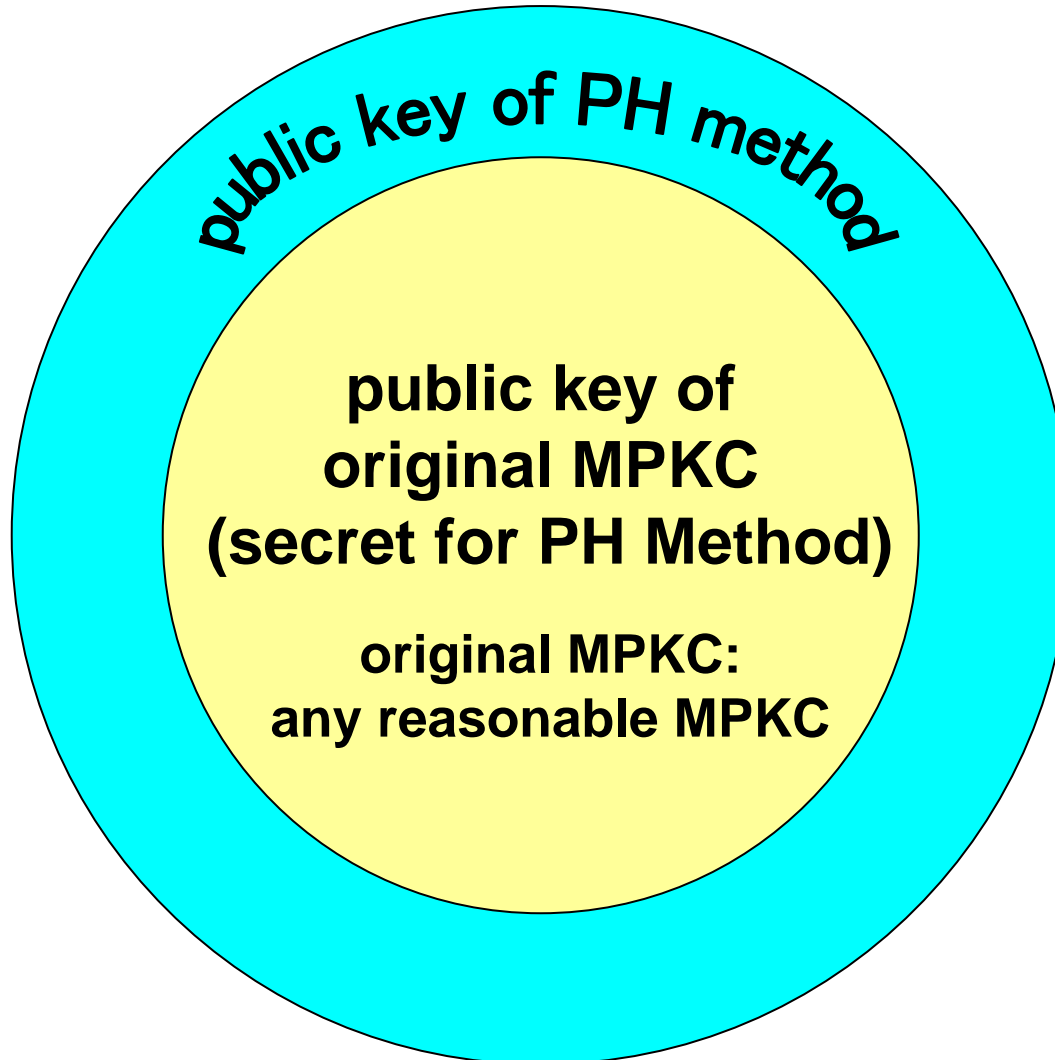
2005 Primitive Linear PH Matrix Method

2006 Linear PH Matrix Method with  
Random Variables

2008 Nonlinear PH Matrix Method

2008 Nonlinear PH Perturbation Vector Method

# Concept of PH Method



# Approach to NP-hardness of (Inversion Problem of) MPKC (1/6)

↑  
increase of randomness  
|

Many MPKCs

generalized sequential solution method,  
MI, TTM, R(S)SE, ...

# Approach to NP-hardness of (Inversion Problem of) MPKC (2/6)

↑  
increase of randomness  
|

Random Polynomials [Equations]

$$\begin{pmatrix} y_1 = \\ \vdots \\ y_m = \end{pmatrix} \begin{pmatrix} f_1(x_1, x_2, \dots, x_n) \\ \vdots \\ f_m(x_1, x_2, \dots, x_n) \end{pmatrix}$$

← NP-hard

Many MPKCs

generalized sequential solution method,  
MI, TTM, R(S)SE, ...

# Approach to NP-hardness of (Inversion Problem of) MPKC (3/6)

↑  
increase of randomness  
|

Random Polynomials [Equations]

$$\begin{pmatrix} y_1 = \\ \vdots \\ y_m = \end{pmatrix} \begin{pmatrix} f_1(x_1, x_2, \dots, x_n) \\ \vdots \\ f_m(x_1, x_2, \dots, x_n) \end{pmatrix}$$

← NP-hard

Many MPKCs

generalized sequential solution method,  
MI, TTM, R(S)SE, ...

← not NP-hard  
(trapdoor structure)

# Approach to NP-hardness of (Inversion Problem of) MPKC (4/6)

↑ increase of randomness

Random Polynomials [Equations]

$$\begin{pmatrix} y_1 = \\ \vdots \\ y_m = \end{pmatrix} \begin{pmatrix} f_1(x_1, x_2, \dots, x_n) \\ \vdots \\ f_m(x_1, x_2, \dots, x_n) \end{pmatrix}$$

← NP-hard

PH Method

$$\left( \begin{array}{|c|} \hline \text{cipher} \\ \hline \end{array} \right) = \left( \begin{array}{|c|} \hline \text{original MPKC part} \\ \hline \end{array} \right) + \left( \begin{array}{|c|} \hline \text{random polynomial part} \\ \hline \end{array} \right)$$

← totally internal perturbed?

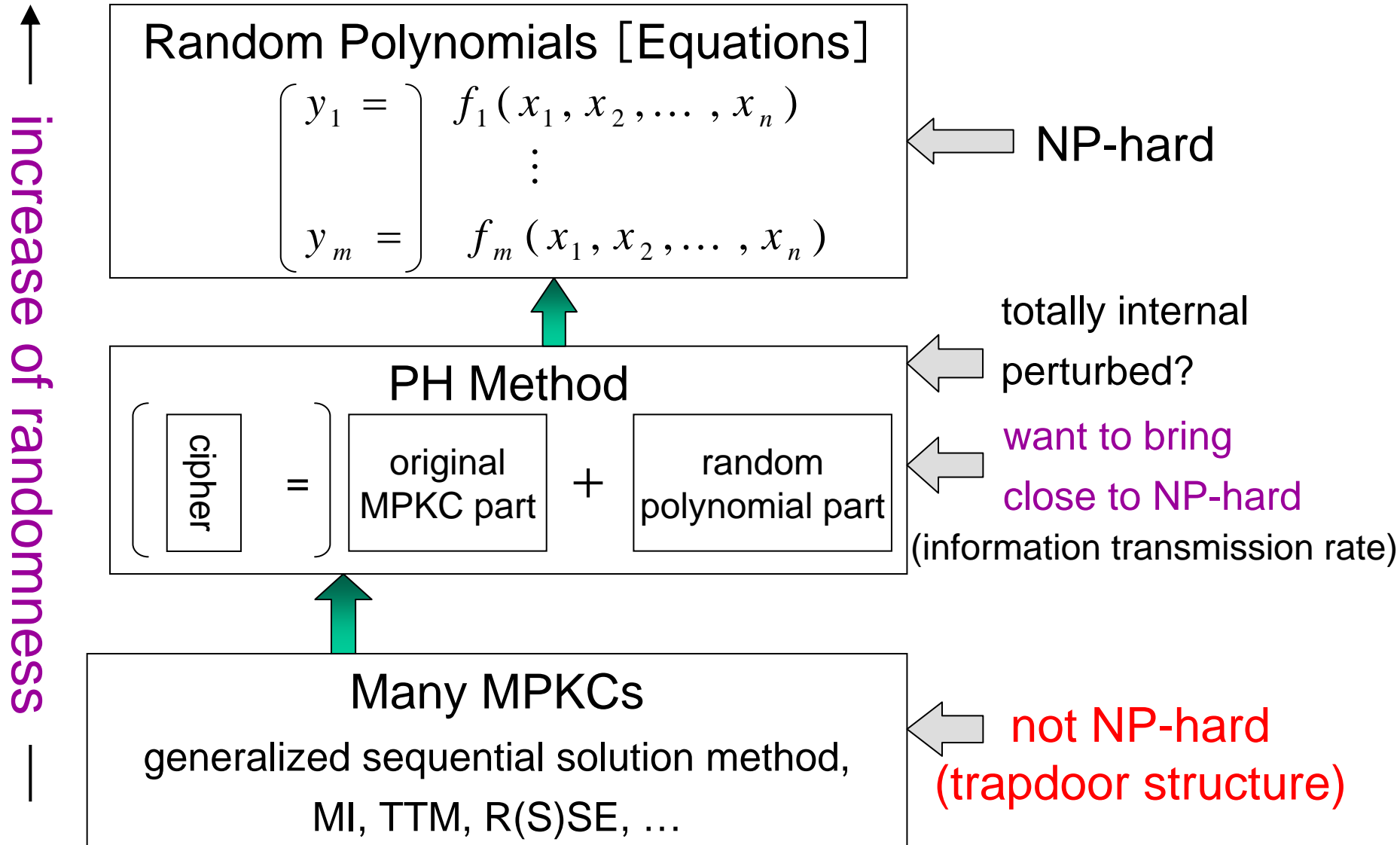
← want to bring close to NP-hard (information transmission rate)

Many MPKCs

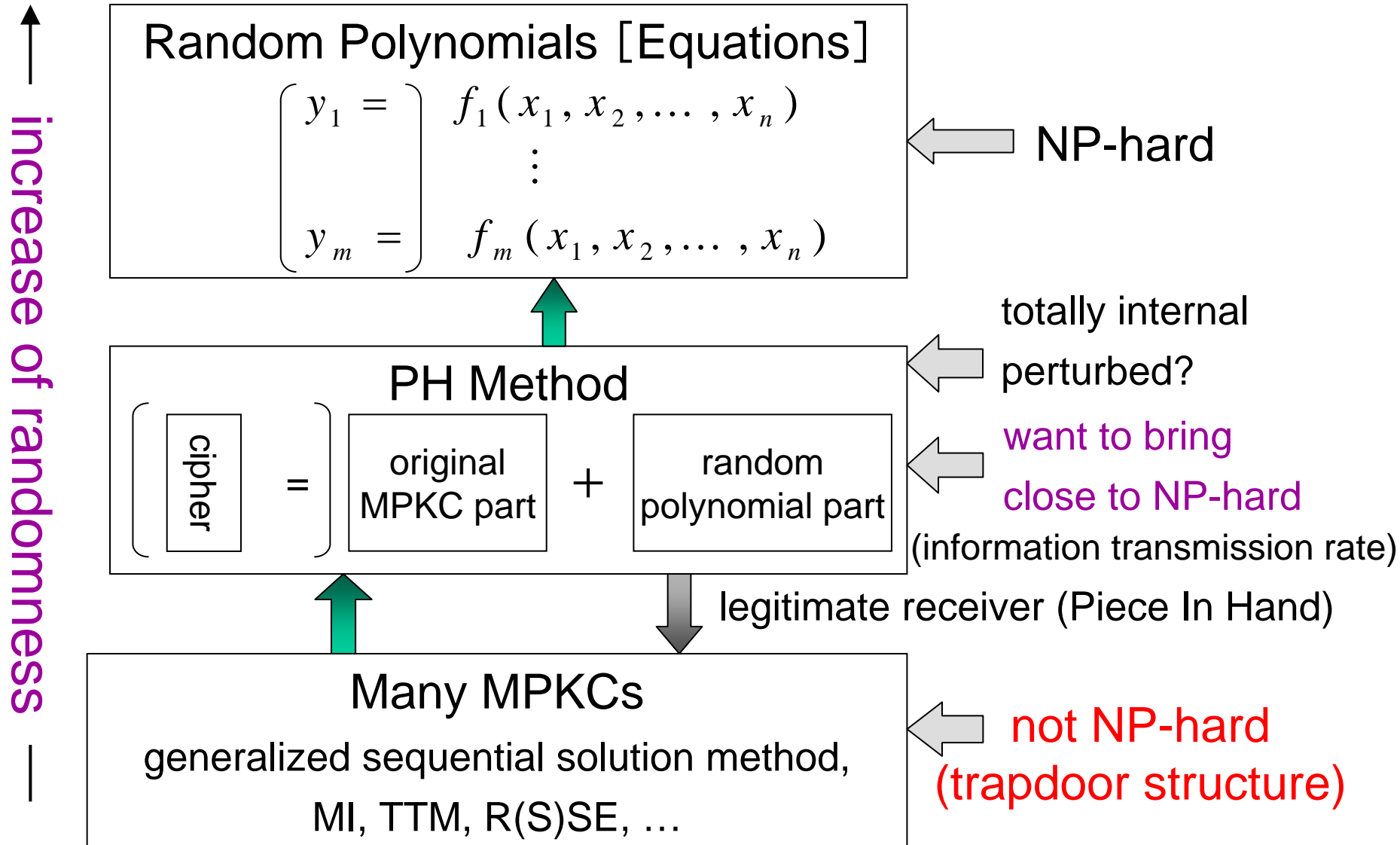
generalized sequential solution method,  
MI, TTM, R(S)SE, ...

← not NP-hard (trapdoor structure)

# Approach to NP-hardness of (Inversion Problem of) MPKC (5/6)



# Approach to NP-hardness of (Inversion Problem of) MPKC (6/6)



# Contents

## 1. Piece In Hand (PH) Method

- Piece In Hand Concept
- Purpose of PH Method

## 2. NonLinear PH Perturbation Vector (NLPHPV) Method

- Schemes of Multivariate Public Key Cryptosystems
- Design Principle of NLPHPV Method
- Public Key Construction, Decryption
- Security of NLPHPV Method

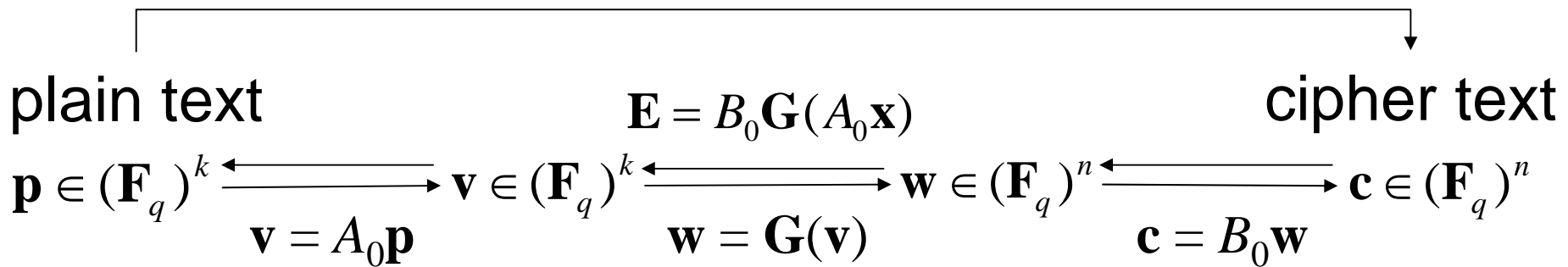
## 3. Future Study

# Multivariate Public Key Cryptosystem

Parameters:  $q$ : number of elements of the finite field,  
 $k$ : dim. of plain text (vector),  $n$ : dim. of cipher text (vector)

public key:  $\mathbf{E}$

$$\mathbf{c} = \mathbf{E}(\mathbf{p}), \quad \mathbf{E} \in \mathbf{F}_q[x_1, \dots, x_k]^n$$



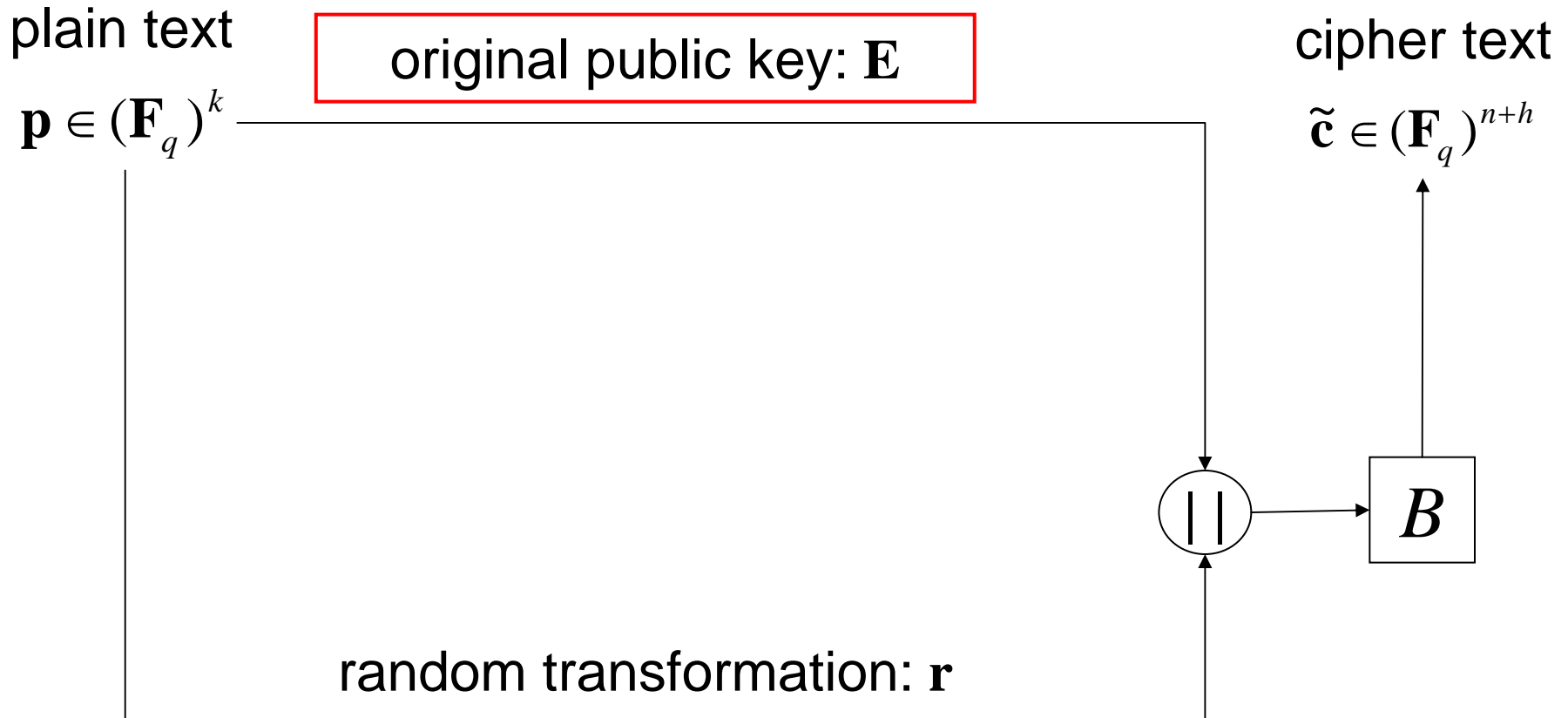
secret key:

$\mathbf{A}_0$

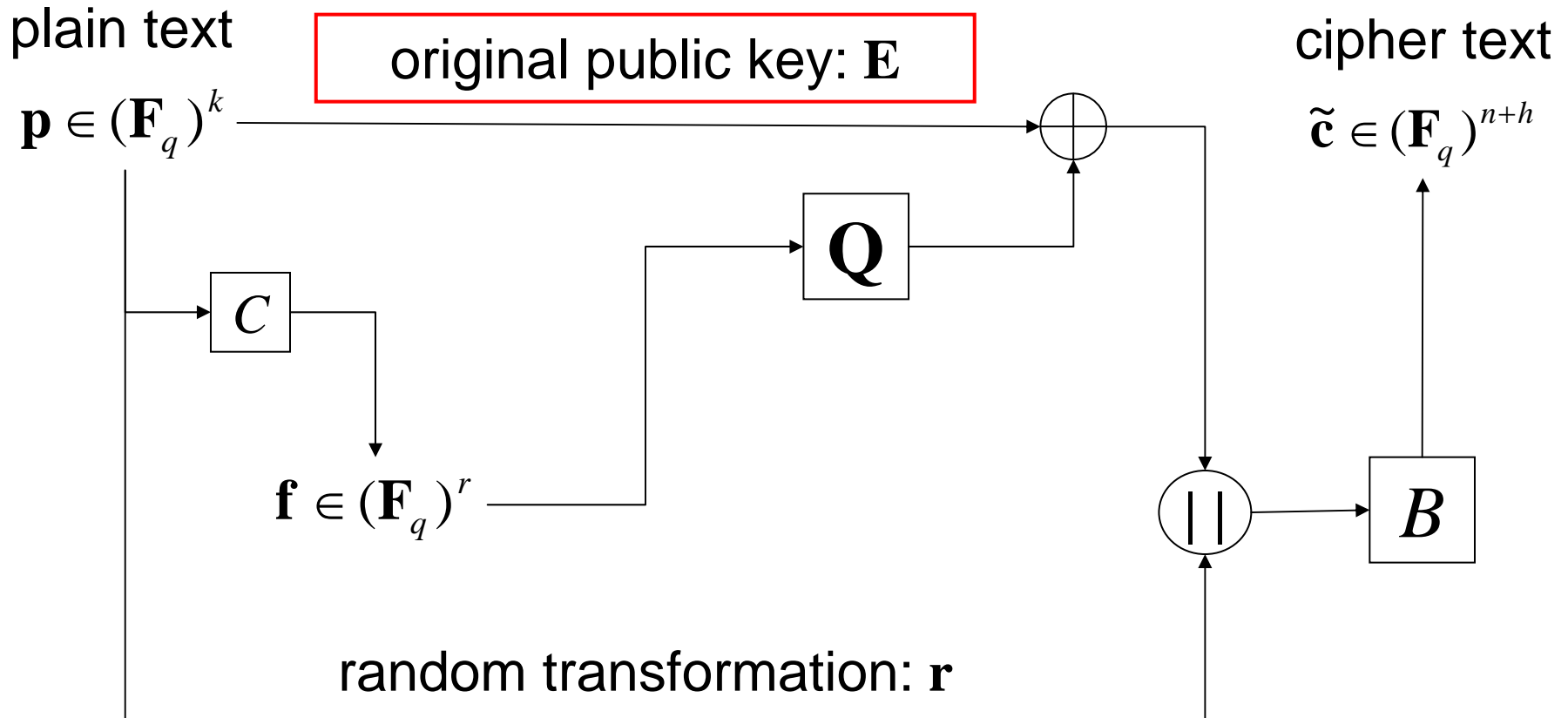
$\mathbf{G}$

$\mathbf{B}_0$

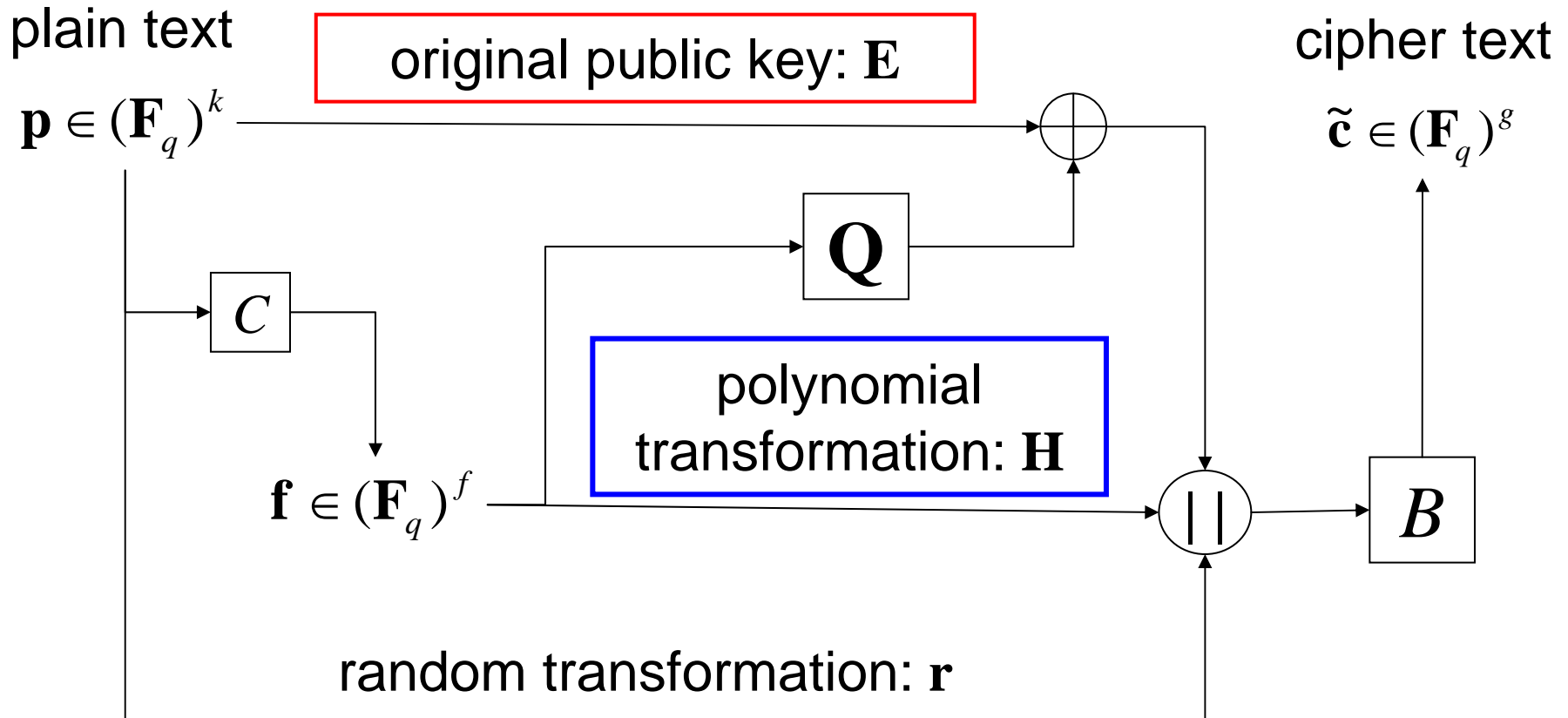
# Design Principle of NLPHPV Method (1/4)



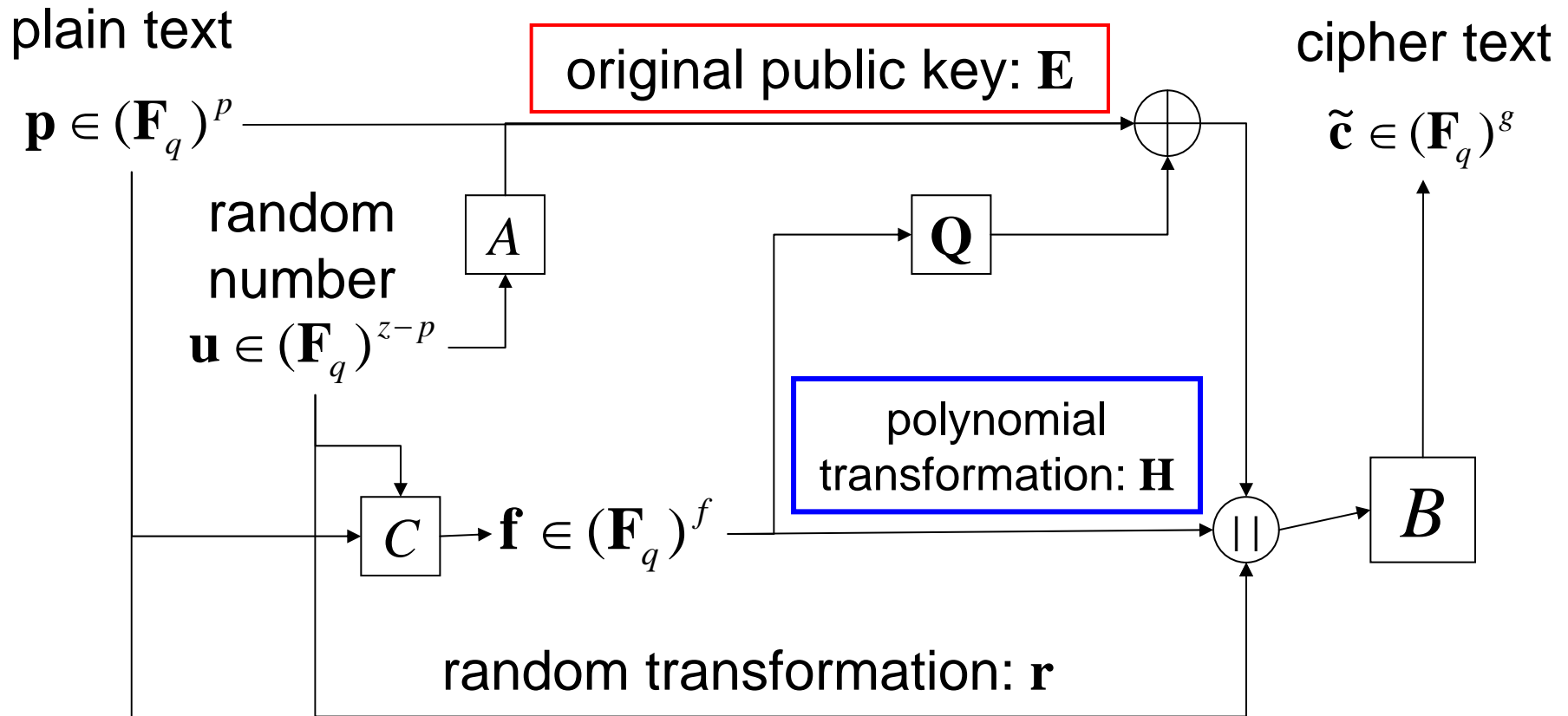
# Design Principle of NLPHPV Method (2/4)



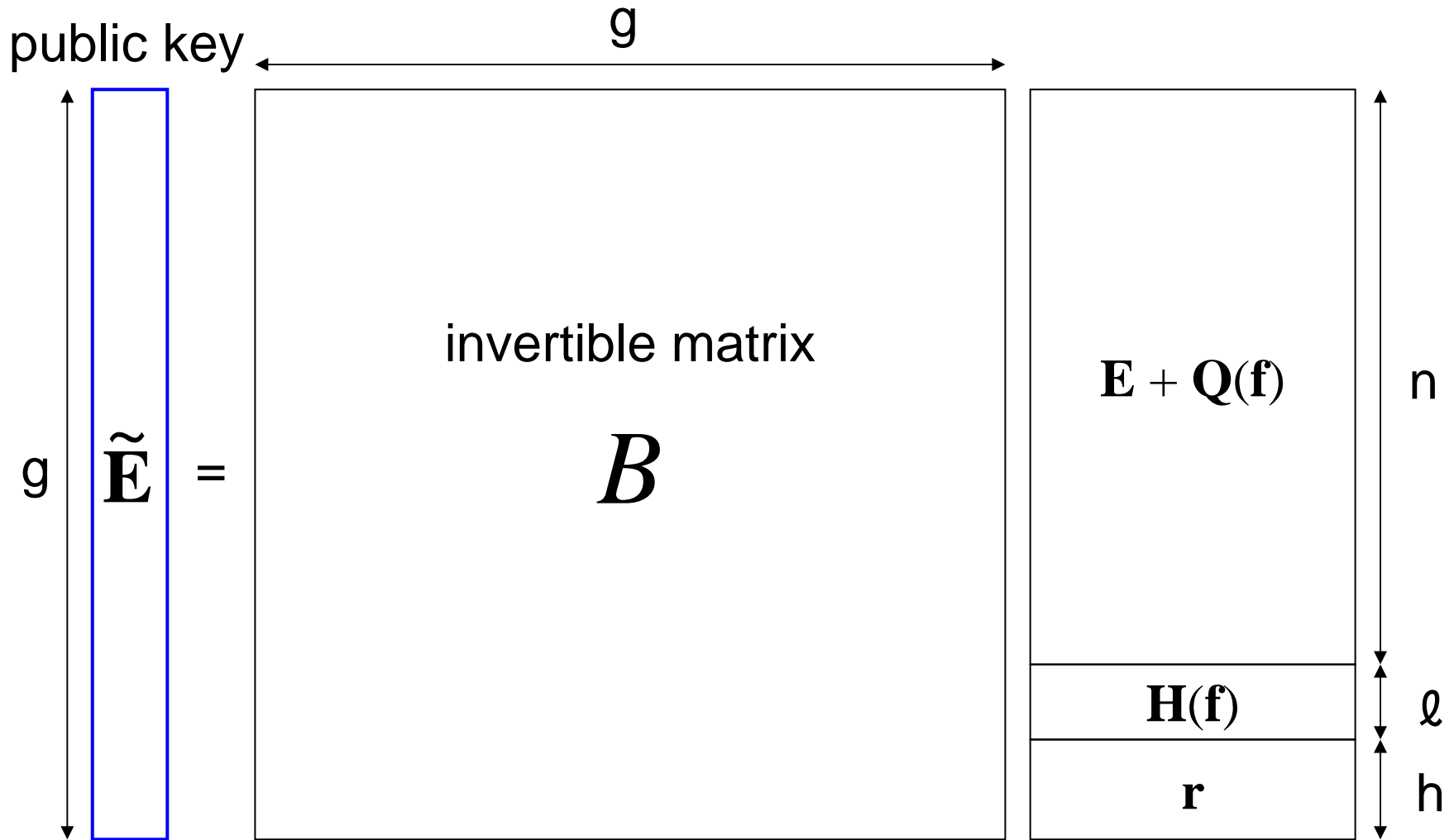
# Design Principle of NLPHPV Method (3/4)



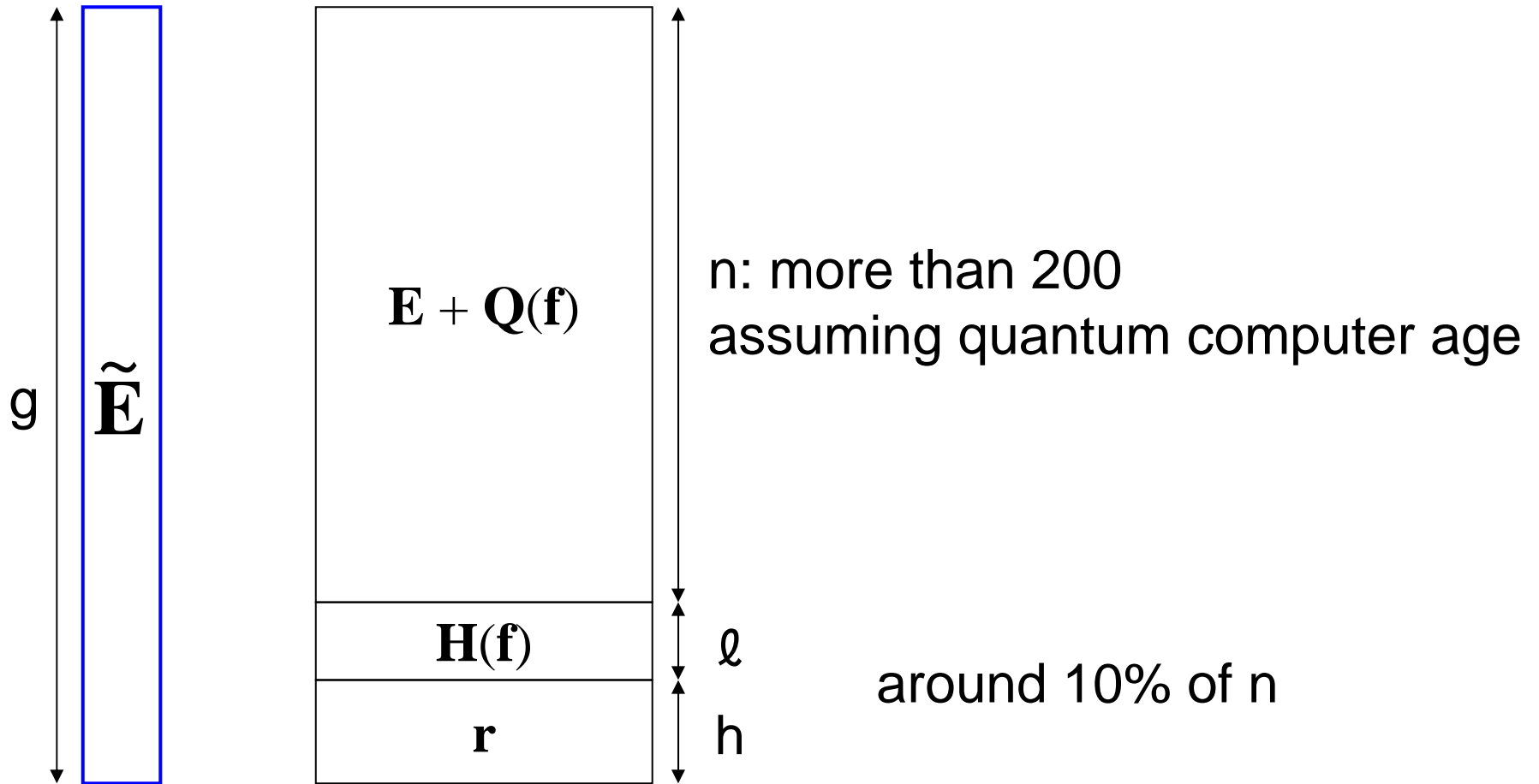
# Design Principle of NLPHPV Method (4/4)



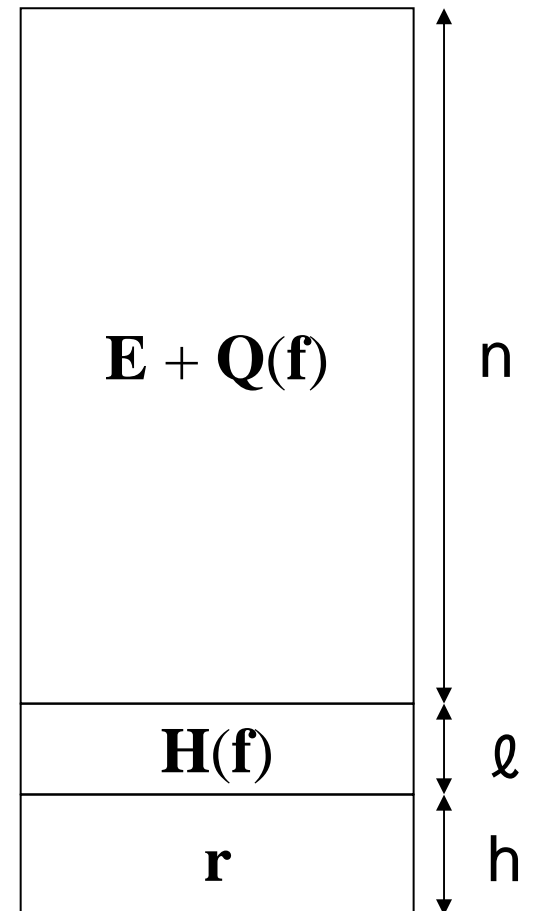
# Public Key Construction of NLPHPV Method



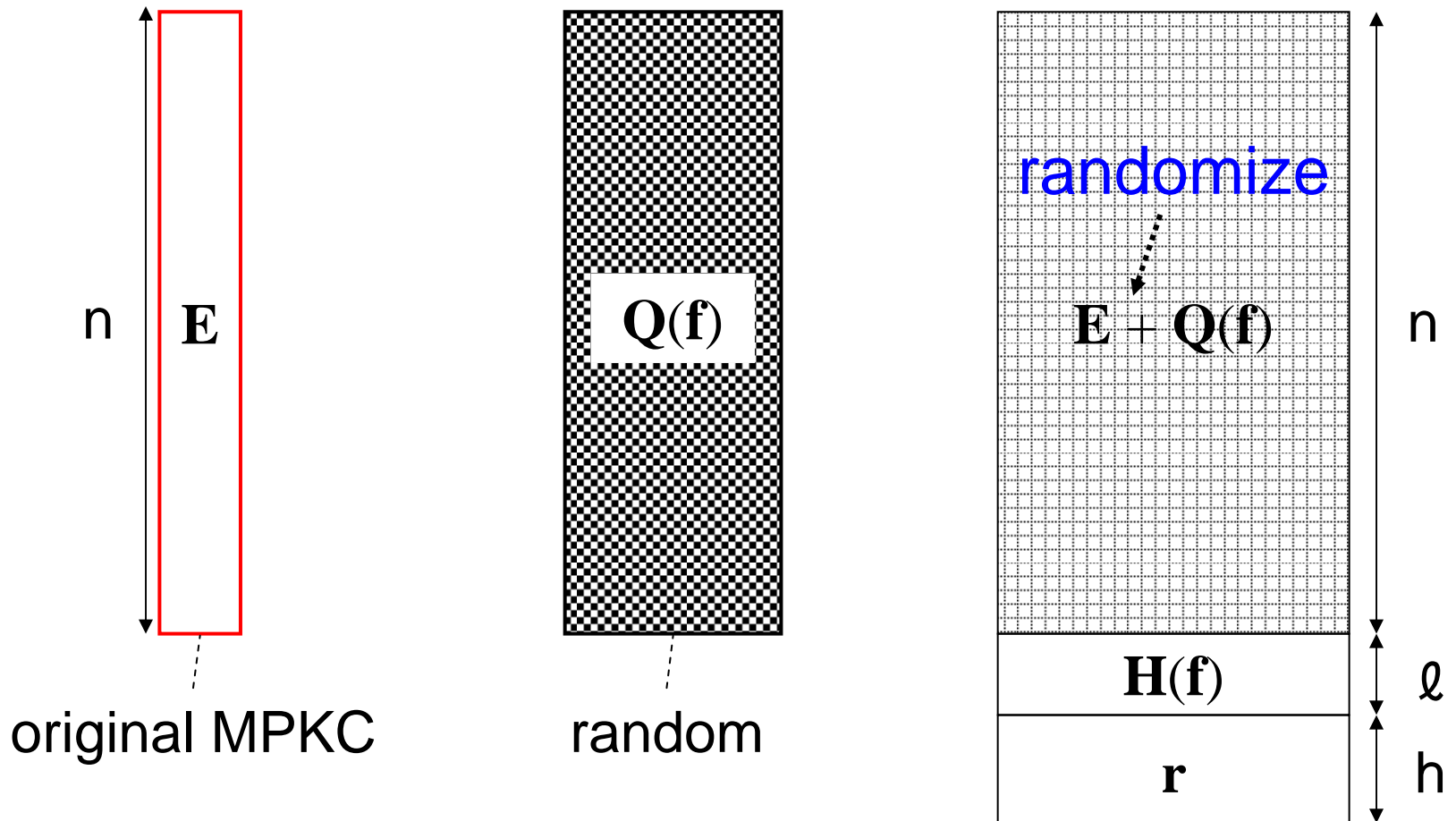
# Parameters of NLPHPV Method



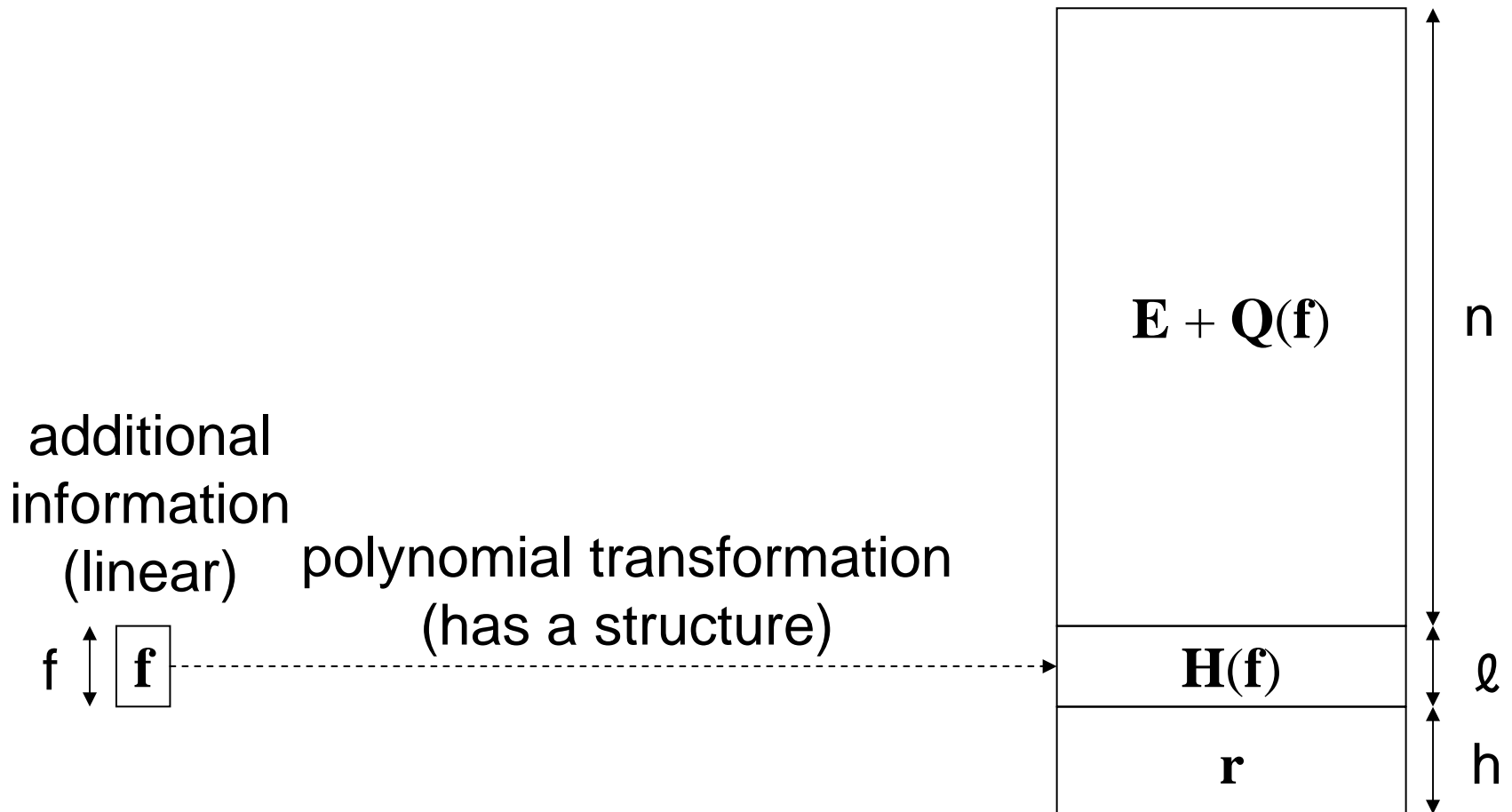
# Public Key Construction of NLPHPV Method



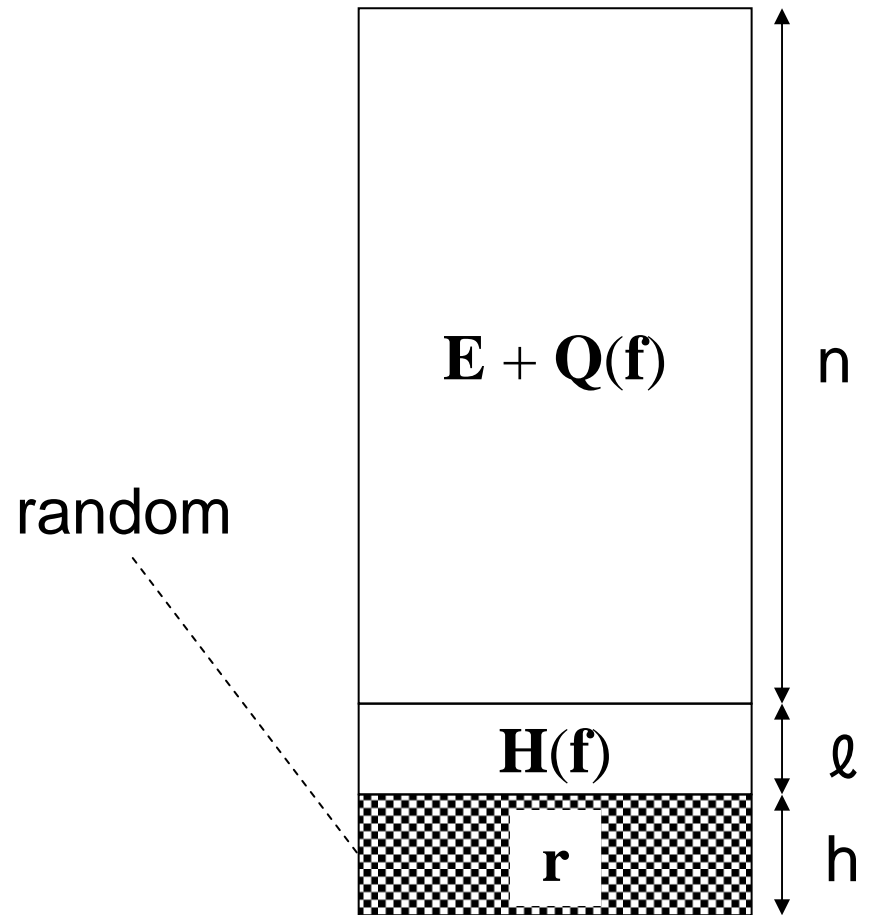
# Public Key Construction of NLPHPV Method (1/3)



# Public Key Construction of NLPHPV Method (2/3)



# Public Key Construction of NLPHPV Method (3/3)



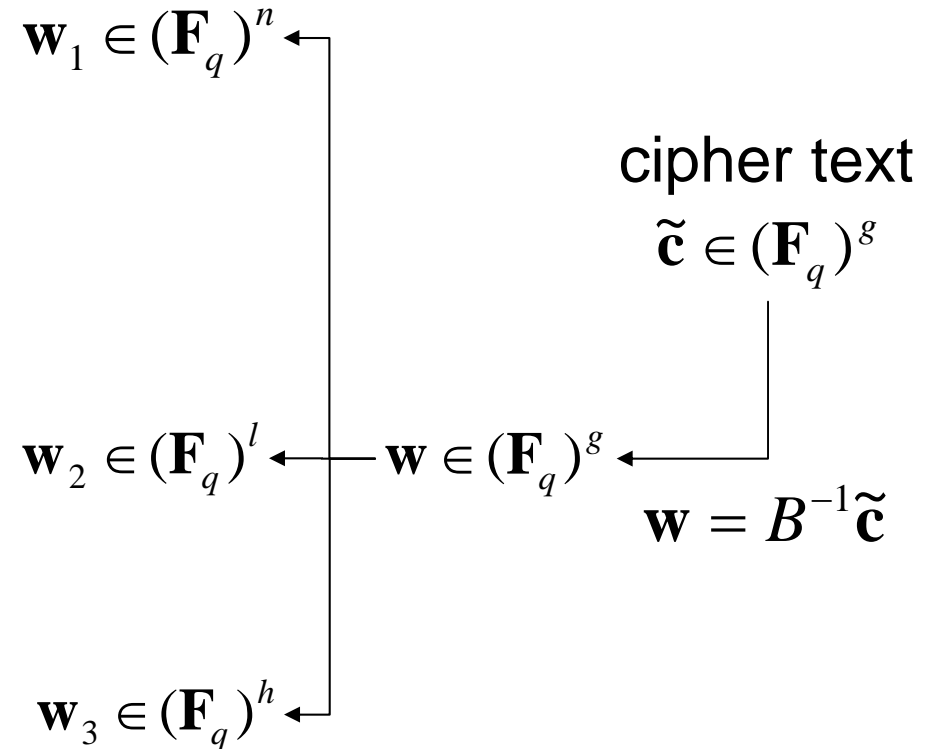
# Decryption of NLPHPV Method (1/5)

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

$\mathbf{w} \in (\mathbf{F}_q)^g$  ←  $\mathbf{w} = B^{-1}\tilde{\mathbf{c}}$

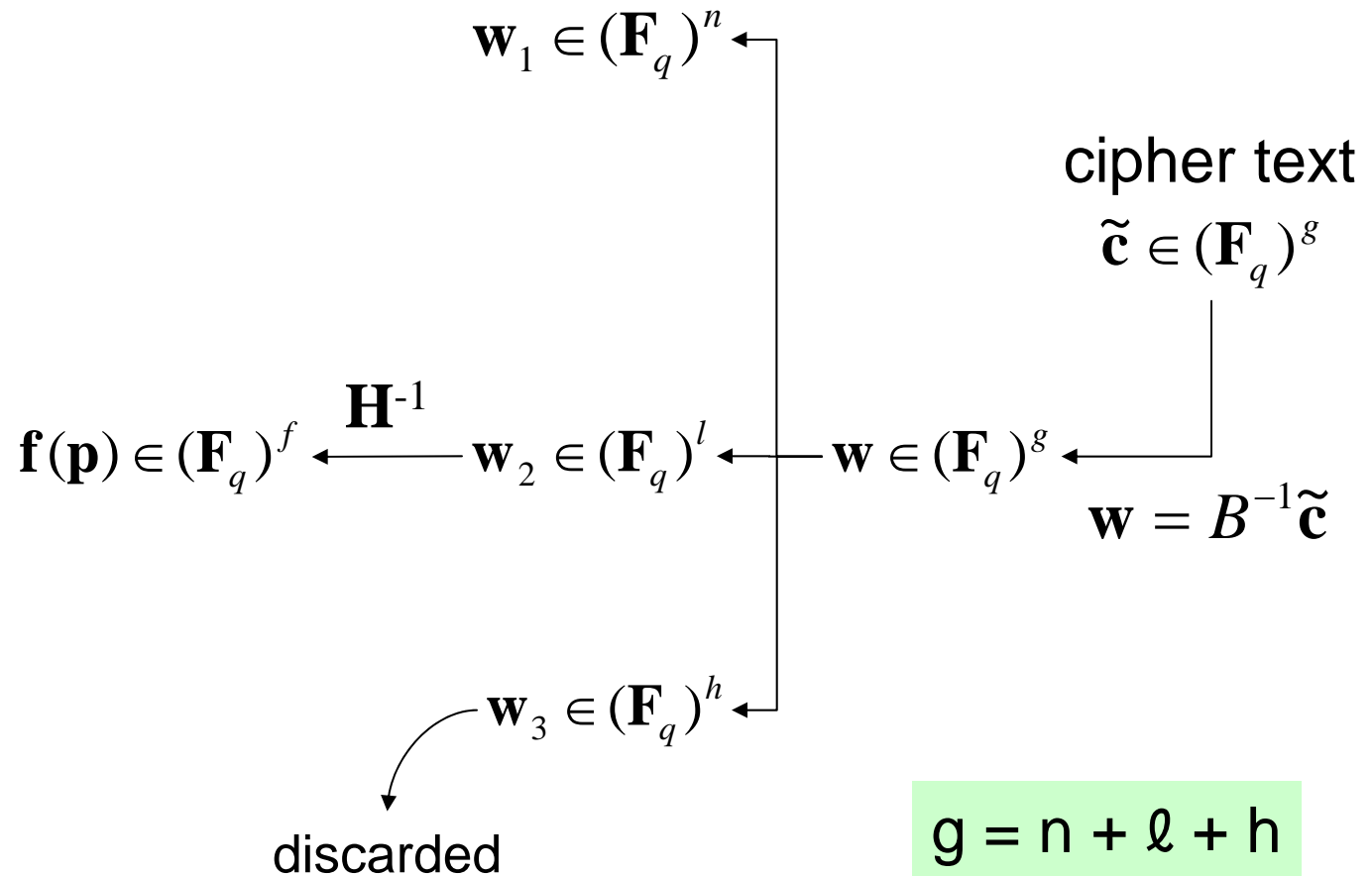
The diagram illustrates the decryption step. It shows a vertical line connecting the cipher text  $\tilde{\mathbf{c}} \in (\mathbf{F}_q)^g$  to the plaintext  $\mathbf{w} \in (\mathbf{F}_q)^g$ . A horizontal arrow points from the cipher text to the plaintext, with the equation  $\mathbf{w} = B^{-1}\tilde{\mathbf{c}}$  written below it.

# Decryption of NLPHPV Method (2/5)

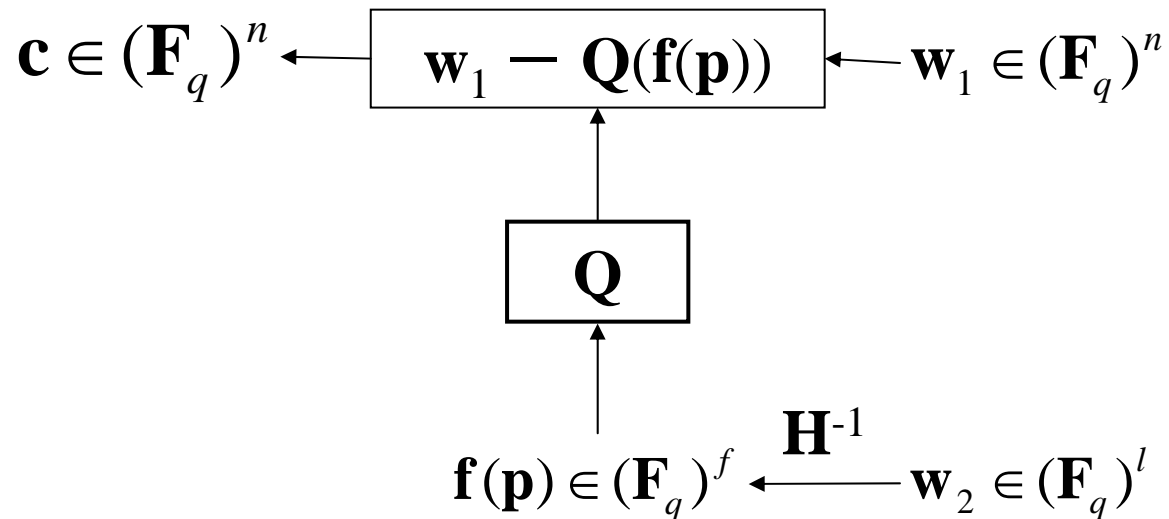


$$g = n + l + h$$

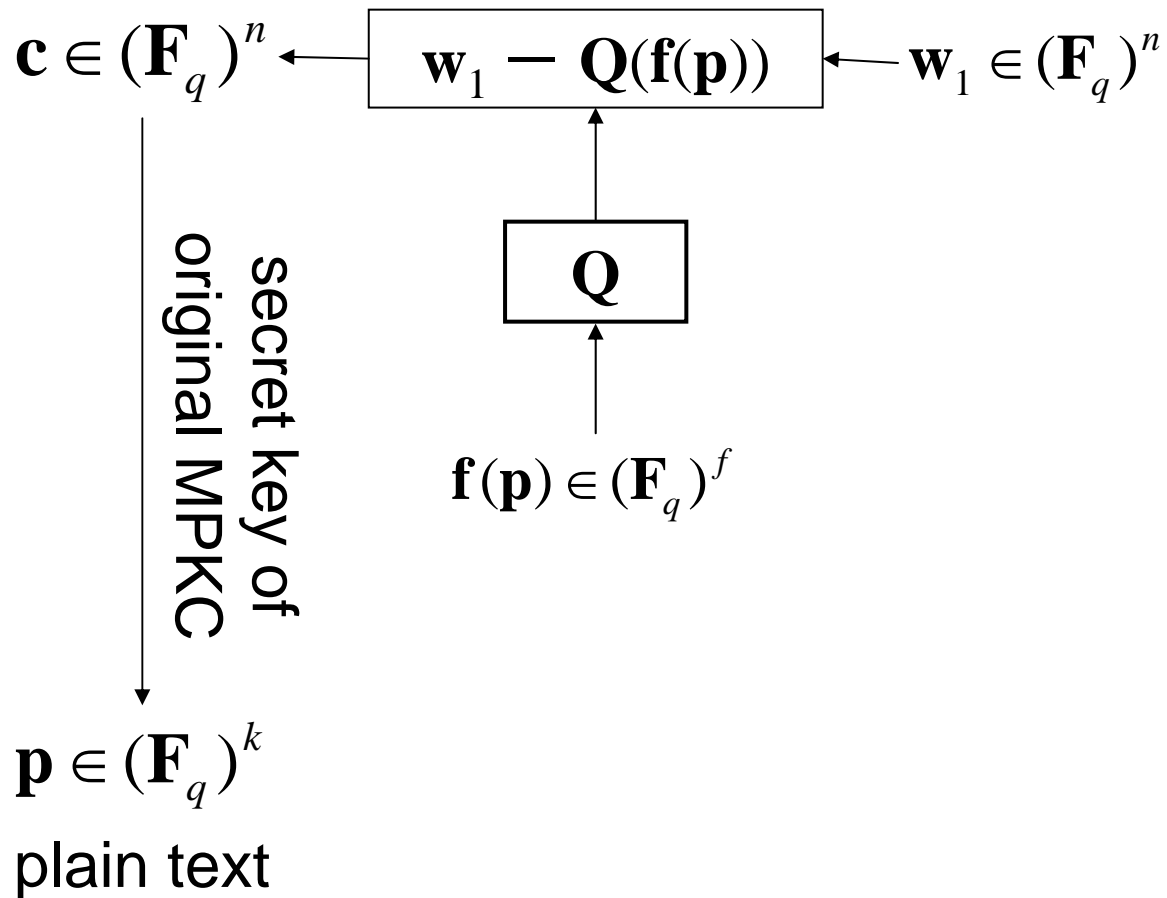
# Decryption of NLPHPV Method (3/5)



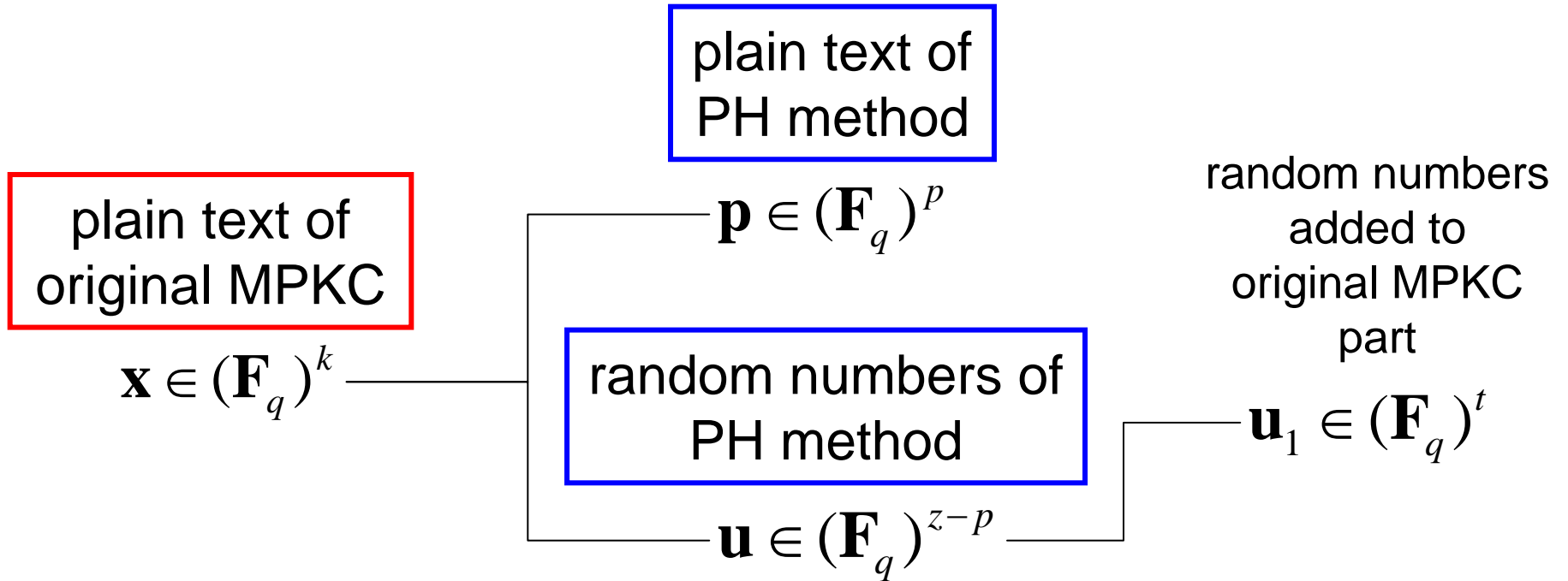
# Decryption of NLPHPV Method (4/5)



# Decryption of NLPHPV Method (5/5)



# Adding Random Numbers

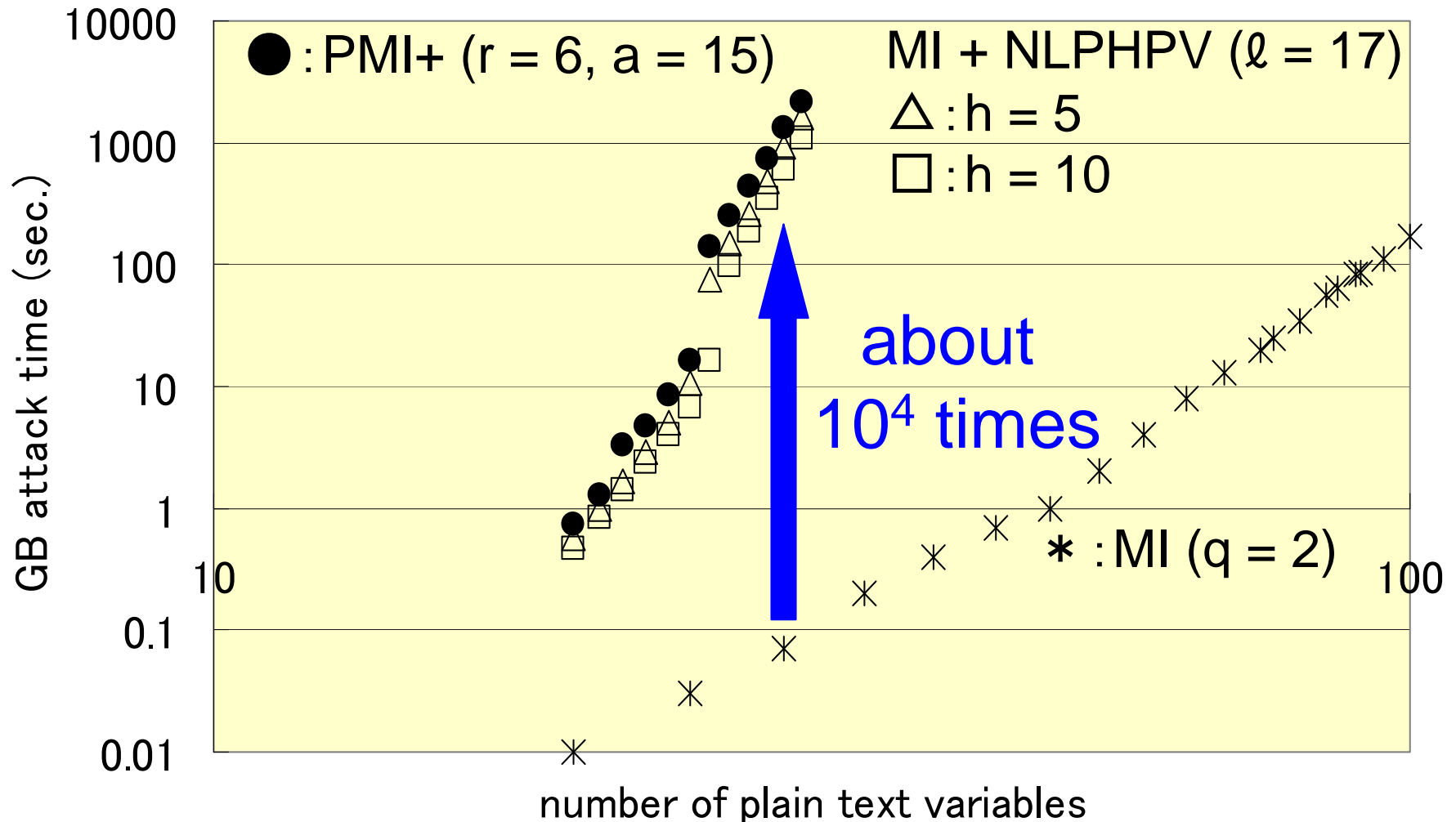


$$\mathbf{x} = \begin{pmatrix} \mathbf{p} \\ A\mathbf{u}_1 \end{pmatrix}, \quad \mathbf{u} = \begin{pmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \end{pmatrix}, \quad A \in \mathbf{F}_q^{(k-p) \times t}$$

$$p \leq k \leq z$$

$$t \leq z - p$$

# Security of NLPHPV Method



# Secure Parameter Setting (Encryption Scheme)

- **original encryption scheme** ( $q = 256$ ):
- 260 input/output variables
- public key size: 8.89 MB

- **the enhanced encryption scheme:**
- plain text size: 2048 bits
- public key size: 26.65 MB
- information transmission rate: 85.3%

about  
3 times



# Secure Parameter Setting (Signature Scheme)

- **original signature scheme** ( $q = 256$ ):
- 20 input variables, 30 output variables
- public key size: 9.92 KB

- **the enhanced signature scheme:**
- signature size: 400 bits
- public key size: 39.78 KB

about  
4 times



# Contents

## 1. Piece In Hand (PH) Method

- Piece In Hand Concept
- Purpose of PH Method

## 2. NonLinear PH Perturbation Vector (NLPHPV) Method

- Schemes of Multivariate Public Key Cryptosystems
- Design Principle of NLPHPV Method
- Public Key Construction, Decryption
- Security of NLPHPV Method

## 3. Future Study

# Future Study (1/3)

- security against so-called “**combo**” attack (attack against TTS (UOV & minrank +  $\alpha$ ), “differential-rank” attack, ...), “**improved**” differential attack, ...
- IND-CCA level security evaluation

# Future Study (2/3)

- “2 Layer” nonlinear PH method  
has been proposed in Japanese
- random polynomial part is omitted  
from NLPHPV method
- polynomial transformation  $H$   
has no structure as much as possible

# Future Study (3/3)

- two research directions for PH method
- **practical** (fast, efficient) scheme for original MPKC
- **optimal choice** for invertible polynomial transformation  $H$