Piece In Hand Concept for Enhancing Security of Multivariate Public Key Cryptosystems and its Applications

March 3, 2013
Workshop on Solving Multivariate Polynomial Systems and Related Topics
ISIT, Fukuoka, Japan

Ryo Fujita
(Chuo University, Japan)

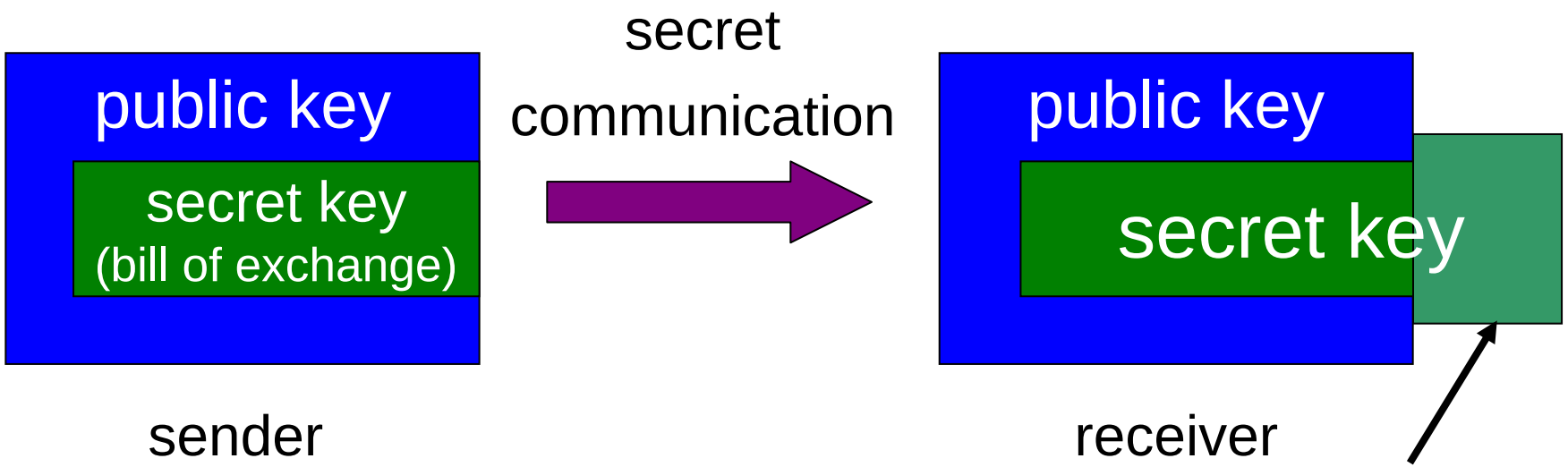
Joint work with Dr. Kohtaro Tadaki and Prof. Shigeo Tsujii

Supported by the Ministry of Economy, Trade and Industry of Japan.

Contents

1. Piece In Hand (PH) Concept
2. Future Study at PQCrypto 2008
3. Future Study

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

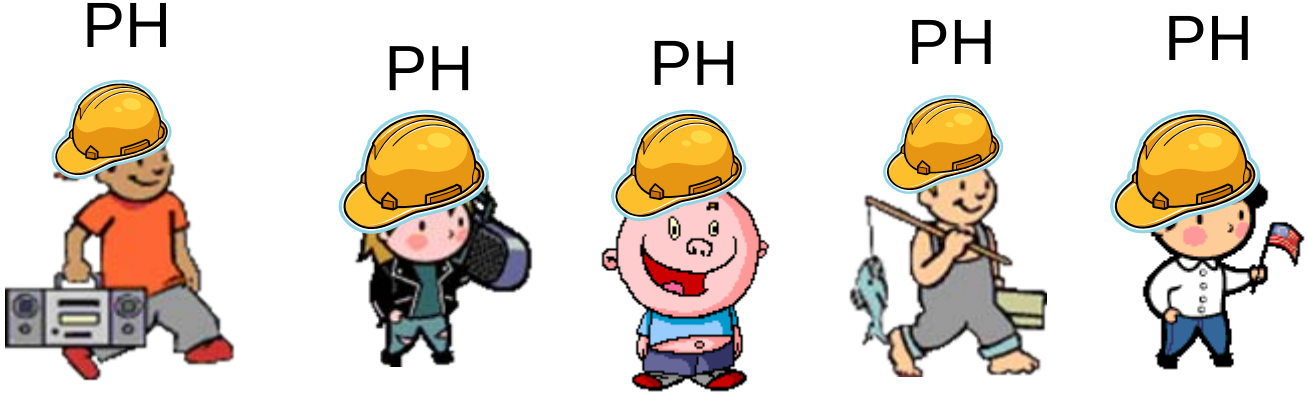


aim to enhance the security by using effectively random variables

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

enhancing security of MPKC

Piece In Hand:



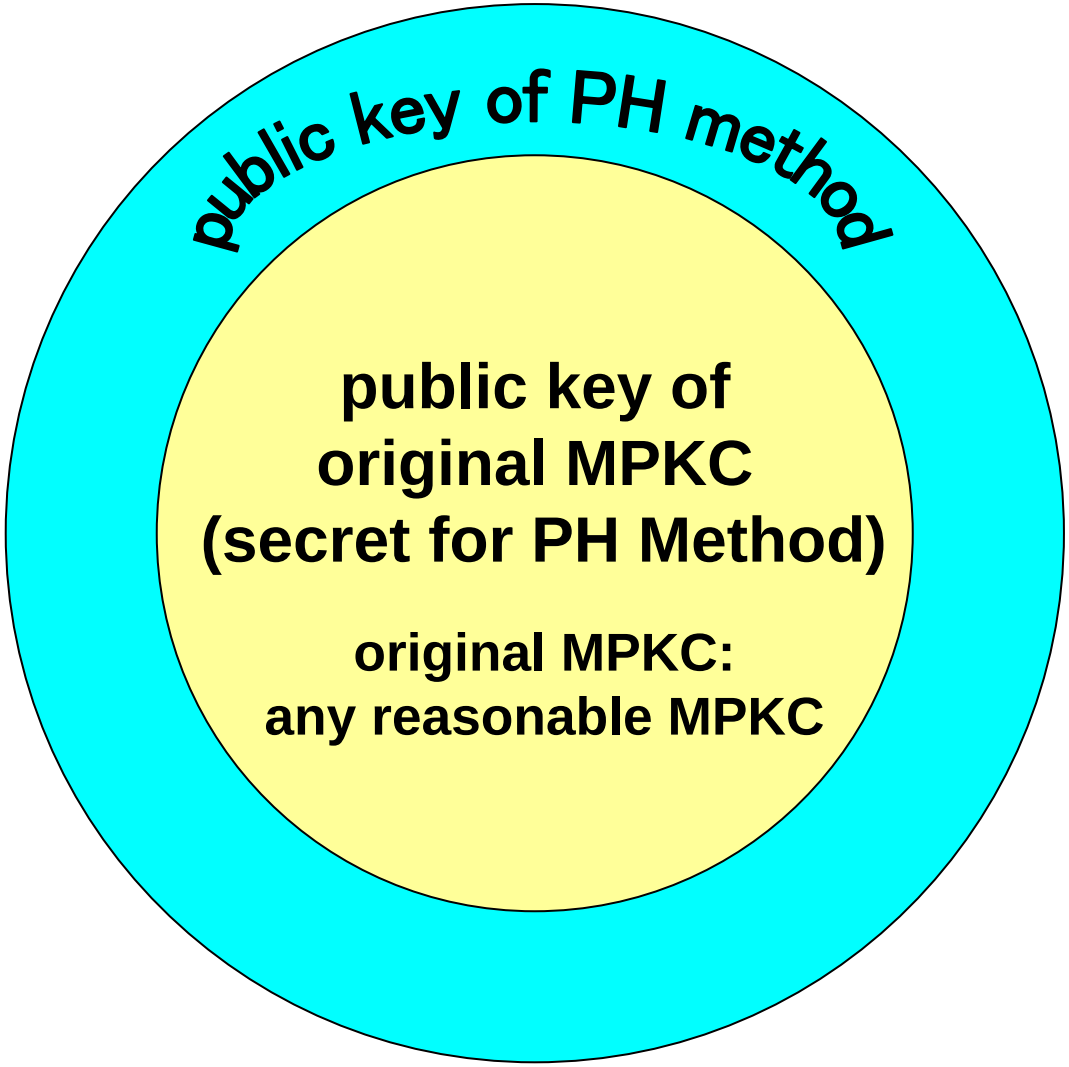
general concept which is applicable to any MPKC

What is the PH Method ?

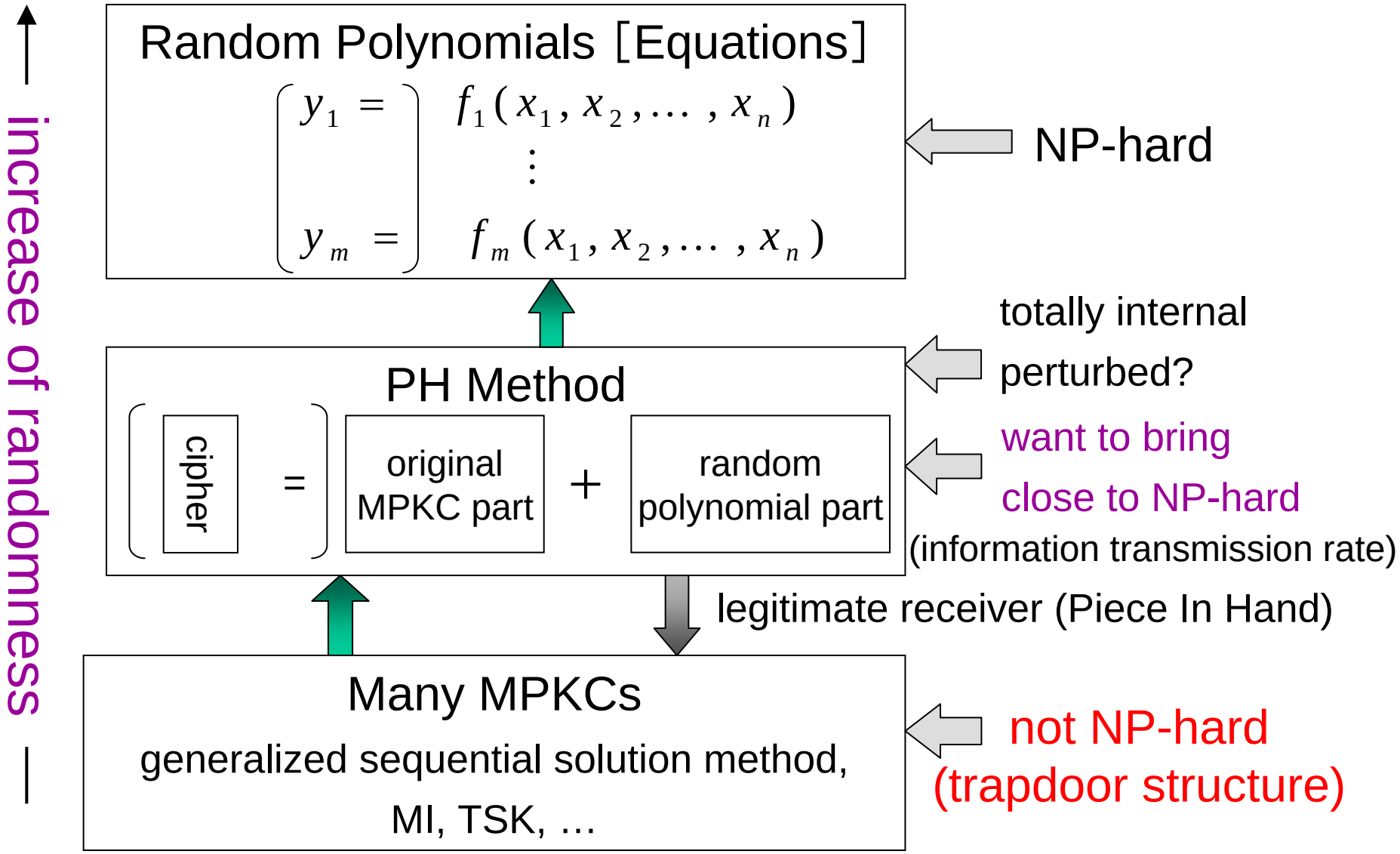
- A method to realize the Piece In Hand Concept (Tsujii, Tadaki, Fujita)

2003	Piece In Hand Concept
2005	Primitive Linear PH Matrix Method
2006	Linear PH Matrix Method with Random Variables (PQCrypto 2006)
2008	Nonlinear PH Matrix Method (SCC 2008)
2008	Nonlinear PH Perturbation Vector Method (PQCrypto 2008)
2009	2-layer nonlinear PH method (IEICE Trans. EA)

Concept of PH Method



Approach to NP-hardness of (Inversion Problem of) MPKC



Future Study at PQCrypto 2008

https://math.uc.edu/~aac/pqcrypto2008/presentations/NLPHPVfujita.pdf

- security against so-called "combo" attack
  (attack against TTS (UOV & minrank + α),
  "differential-rank" attack, …),
  "improved" differential attack, ...

  --> cryptanalysis of double-layer Square and Square+
  [Thomae-Wolf, PQCrypto 2011]
  【Revisited】solving underdetermined systems
  of multivariate quadratic equations
  [Thomae-Wolf, PKC 2012]

Future Study at PQCrypto 2008

https://math.uc.edu/~aac/pqcrypto2008/presentations/NLPHPVfujita.pdf

- security against so-called "combo" attack
  (attack against TTS (UOV & minrank + α),
  "differential-rank" attack, …),
  "improved" differential attack, ...

  --> cryptanalysis of enhanced TTS, STS and all its variants
  [Thomae-Wolf, AFRICACRYPT 2012]
  cryptanalysis of Rainbow over non-commutative rings
  [Thomae, SCN 2012]

Future Study at PQCrypto 2008

https://math.uc.edu/~aac/pqcrypto2008/presentations/NLPHPVfujita.pdf

- IND-CCA level security evaluation

  --> provably secure schemes:

  provable security of UOV and HFE signature schemes
  against chosen-message attack
  [Sakumoto-Shirai-Hiwatari, PQCrypto 2011]
  public-key identification schemes
  based on multivariate quadratic polynomials
  [Sakumoto-Shirai-Hiwatari, CRYPTO 2011]

Future Study at PQCrypto 2008

https://math.uc.edu/~aac/pqcrypto2008/presentations/NLPHPVfujita.pdf

- IND-CCA level security evaluation

  --> provably secure schemes:

  public-key identification schemes

  based on multivariate cubic polynomials

  [Sakumoto, PKC 2012]

  public-key cryptography

  from new multivariate quadratic assumptions

  [Huang-Liu-Yang, PKC 2012]

Future Study at PQCrypto 2008

https://math.uc.edu/~aac/pqcrypto2008/presentations/NLPHPVfujita.pdf

- "2 Layer" nonlinear PH method
  has been proposed in Japanese

- random polynomial part is omitted
  from NLPHPV method
- polynomial transformation has no structure
  as much as possible
  --> security enhancement of various MPKCs
  by 2-layer nonlinear Piece in Hand method
  [Tsujii-Tadaki-Fujita-Gotaishi-Kaneko,
  IEICE Trans. Fundamentals, 2009]

Future Study at PQCrypto 2008

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

--> See “Multivariate Cryptography” web page
URL: http://c-faculty.chuo-u.ac.jp/~rfujita/mpkc.html

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: $\mathbf{E}$

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

plain text

cipher text

$$\mathbf{E} = B_0\mathbf{G}(A_0\mathbf{x})$$

$$\mathbf{p} \in (\mathbf{F}_q)^k \xleftrightarrow[\mathbf{v} = A_0\mathbf{p}]{} \mathbf{v} \in (\mathbf{F}_q)^k \xleftrightarrow[\mathbf{w} = \mathbf{G}(\mathbf{v})]{} \mathbf{w} \in (\mathbf{F}_q)^n \xleftrightarrow[\mathbf{c} = B_0\mathbf{w}]{} \mathbf{c} \in (\mathbf{F}_q)^n$$

secret key:

A_0 $\quad$ $\mathbf{G}$ $\quad$ B_0

Multivariate Public Key Cryptosystem

Although this direction in fact has been considered for the last **20 years**,
however, it has had a **rocky** history.
Many schemes were **proposed**, **broken**,
sometimes **patched**, and sometimes **broken again**.
One objection frequently voiced is that
the security of these systems is often **ad-hoc**,
and thus hard to evaluate.

[HLY12] Huang, Liu, Yang
Public-Key Cryptography from New Multivariate Quadratic Assumptions

Multivariate cryptographic schemes are very efficient
but have a lot of exploitable mathematical structure.

Their security is not fully understood,
and new attacks against them are found on a regular basis.

It would thus be prudent not to use them
in any security-critical applications.

[DFSS07] Dubois, Fouque, Shamir, Stern, Practical cryptanalysis of SFLASH

The development of research in theory and application
is the foundation to generate
new multivariate crytpographc schemes.

Future Study

- Promising approach I. II.

- I. MP: Multivariate Polynomial
  (MQ: Multivariate Quadratic, MC: Multivariate Cubic, …)
  assumption based approach:

  provably secure cryptographic primitives and protocols

- II. PH method collaborated with other cryptographic theories:

  relaxing some conditions, etc.

  oblivious transfer (OT),
  secure multiparty computation (MPC), …