Public-Key Identification Schemes based on Multivariate Polynomials

Koichi Sakumoto

Workshop on Solving Multivariate Polynomial Systems and Related Topics
@ ISIT, Fukuoka

2013/03/03

Outline

- What is MPKC?
- Another approach of MPKC

What is MPKC? (1/2)

- Multivariate Public-Key Cryptosystem
  - Public-key schemes using multivariate polynomials

$$f_1(x_1,\ldots,x_{10}) = x_1x_2 + x_1x_4 + x_1x_7 + x_2x_3 + x_2x_5 + x_3x_7 + x_4x_5 + x_1 + x_4$$
$$f_2(x_1,\ldots,x_{10}) = x_1x_3 + x_1x_8 + x_1x_{10} + x_2x_4 + x_4x_8 + x_5x_7 + x_6x_8 + x_2 + x_7$$
$$f_3(x_1,\ldots,x_{10}) = x_1x_5 + x_1x_9 + x_2x_5 + x_2x_{10} + x_3x_5 + x_7x_9 + x_1 + x_4 + x_5$$
$$f_4(x_1,\ldots,x_{10}) = x_1x_6 + x_2x_3 + x_3x_8 + x_3x_{10} + x_4x_6 + x_4x_9 + x_5x_7 + x_2 + x_6$$
$$f_5(x_1,\ldots,x_{10}) = x_1x_8 + x_2x_6 + x_3x_6 + x_4x_{10} + x_5x_9 + x_7x_8 + x_8x_9 + x_6 + x_9$$
$$f_6(x_1,\ldots,x_{10}) = x_1x_3 + x_2x_{10} + x_3x_5 + x_3x_9 + x_4x_7 + x_6x_7 + x_6x_{10} + x_3 + x_8$$
$$f_7(x_1,\ldots,x_{10}) = x_1x_{10} + x_2x_8 + x_2x_9 + x_3x_4 + x_5x_6 + x_5x_8 + x_7x_{10} + x_7 + x_9$$
$$f_8(x_1,\ldots,x_{10}) = x_2x_3 + x_2x_4 + x_2x_7 + x_3x_6 + x_5x_9 + x_8x_{10} + x_1 + x_4 + x_{10}$$

  - Example
    - Public-Key Encryption
    - Digital Signature
    - Public-Key Identification

- Other Multivariate Cryptosystems
    - Stream Cipher (C. Berbain, H. Gilbert, J. Patarin, 2006)
    - Hash function (J. Ding, B. Yang, 2007)

What is MPKC? (2/2)

- Strong point
  - Possible to be very efficiently implemented
    - FPGA
      - A. Bogdanov, T. Eisenbarth, A. Rupp, C. Wolf, 2008
    - SW
      - C. Berbain, O. Billet, H. Gilbert, 2006
      - A. I. Chen, M. Chen, T. Chen, C. Cheng, J. Ding, E. L. Kuo, F. Y. Lee, and B. Yang, 2009
  - Short Signature
    - Originally, this was the strong point of HFE, when it was proposed
  - Post-quantum
    - Shor's algorithm, 1994
- Controversial point
  - How to assure security

How to assure security

- Checking that your scheme is secure against all known attacks
  - AES-128/192/256
  - SHA-256/384/512
  - Almost all MPKC

- Proving that security of your scheme is reducible to some reasonable assumption
  - RSA-PSS ⇦ Factoring (or RSA assumption)
  - Schnorr signature ⇦ Discrete Log
  - ??? ⇦ Multivariate Problem

Simple Observation

- RSA-PSS

pk : $N = pq$ —— = Factoring ——→ sk : p, q

- Schnorr signature

pk : $Y = g^x$ —— = Solving DL ——→ sk : x

- Standard approach of MPKC

pk : $P = T \circ F \circ S$ —— ≠ Solving MQ problem ——→ sk : T, F, S

Composite function $P = T \circ F \circ S$

easily invertible map S	easily invertible map F	easily invertible map T
$\Sigma_i s_{1i} x_i = z_1$	$\Sigma_{ij} \alpha_{1ij} z_i z_j + \Sigma_i \beta_{1i} z_i = w_1$	$\Sigma_i t_{1i} w_i = y_1$
⋮	⋮	⋮
$\Sigma_i s_{mi} x_i = z_m$	$\Sigma_{ij} \alpha_{mij} z_i z_j + \Sigma_i \beta_{mi} z_i = w_m$	$\Sigma_i t_{mi} w_i = y_m$

Simple Observation

- RSA-PSS

 pk : $N = pq$ —— = Factoring ——> sk : p, q 

- Schnorr signature

 pk : $Y = g^x$ —— = Solving DL ——> sk : x 

- Standard approach of MPKC

 pk : $P = T \circ F \circ S$ —— ≠ Solving MQ problem ——> sk : T, F, S 

- Another approach of MPKC

 pk : $y = F(x)$ —— = Solving MQ problem ——> sk : x 

$$F(x) = \begin{pmatrix} \Sigma_{ij}\, a_{1ij}\, x_i x_j + \Sigma_i\, b_{1i}\, x_i \\ \vdots \\ \Sigma_{ij}\, a_{mij}\, x_i x_j + \Sigma_i\, b_{mi}\, x_i \end{pmatrix}$$

About the new approach

- began in 2011

- There is still only a small number of studies
  - Standard Identification/Signature
    - Quadratic problem [S., Shirai, Hiwatari, 2011]
    - Cubic problem [S., 2012]
    - Any degree [V. Nachef, J. Patarin, E. Volte, 2012]
  - Threshold ring signature
    - Quadratic problem [A. Petzoldt, S. Bulygin, J. Buchmann, 2012]
  - Public-Key encryption
    - LWE-like new-type MQ assumption [Y. Huang, F. Liu, B. Yang, 2012]

About the new approach

- began in 2011

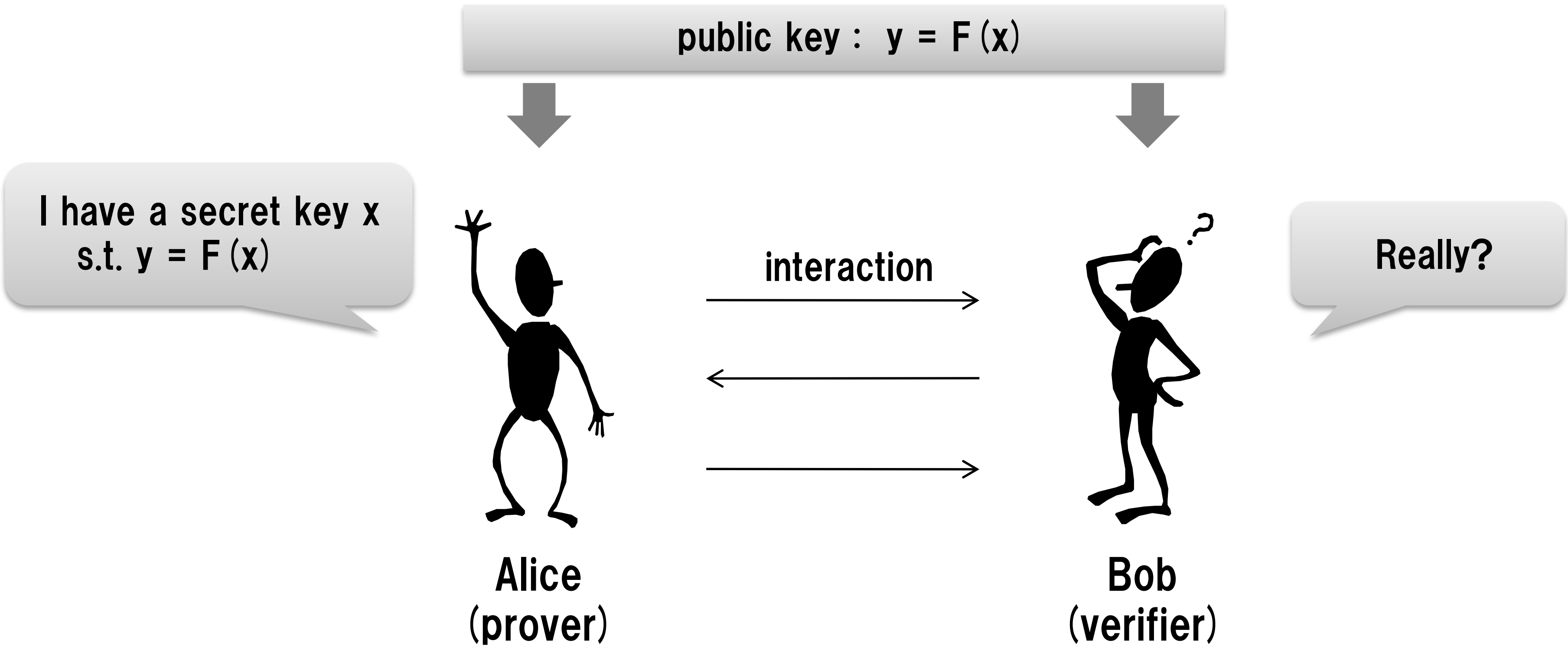
- There is still only a small number of studies
  - Standard Identification/Signature
    - Quadratic problem [S., Shirai, Hiwatari, 2011]
    - Cubic problem [S., 2012]
    - Any degree [V. Nachef, J. Patarin, E. Volte, 2012]
  - Threshold ring signature
    - Quadratic problem [A. Petzoldt, S. Bulygin, J. Buchmann, 2012]
  - Public-Key encryption
    - LWE-like new-type MQ assumption [Y. Huang, F. Liu, B. Yang, 2012]

Outline

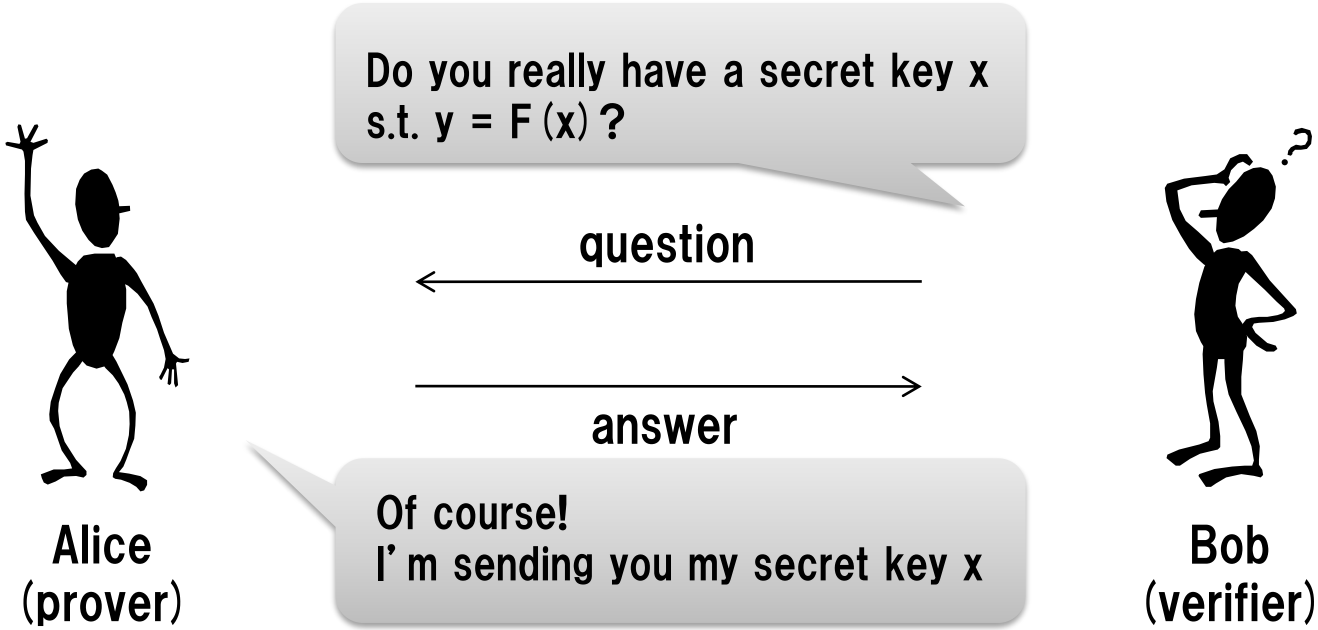
- What is MPKC?
- Another approach of MPKC

Model

- Alice (Prover)
  - asserts that she has a solution of the MQ problem
- Bob (Verifier)
  - checks whether the assertion is true or not through interaction with Alice



Wrong Solution

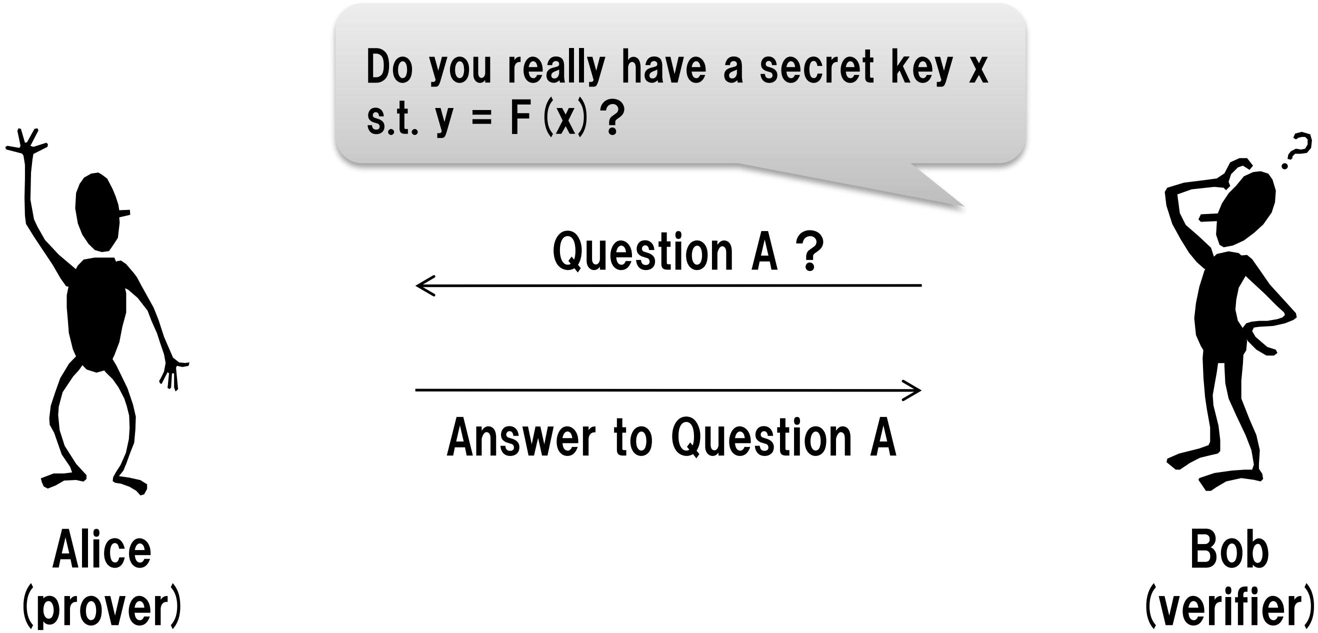


Cut and Choose (Intuition)

1. Cut   Question A   +   Question B

2. Ask only one out of the two questions

3. Answer to the chosen one

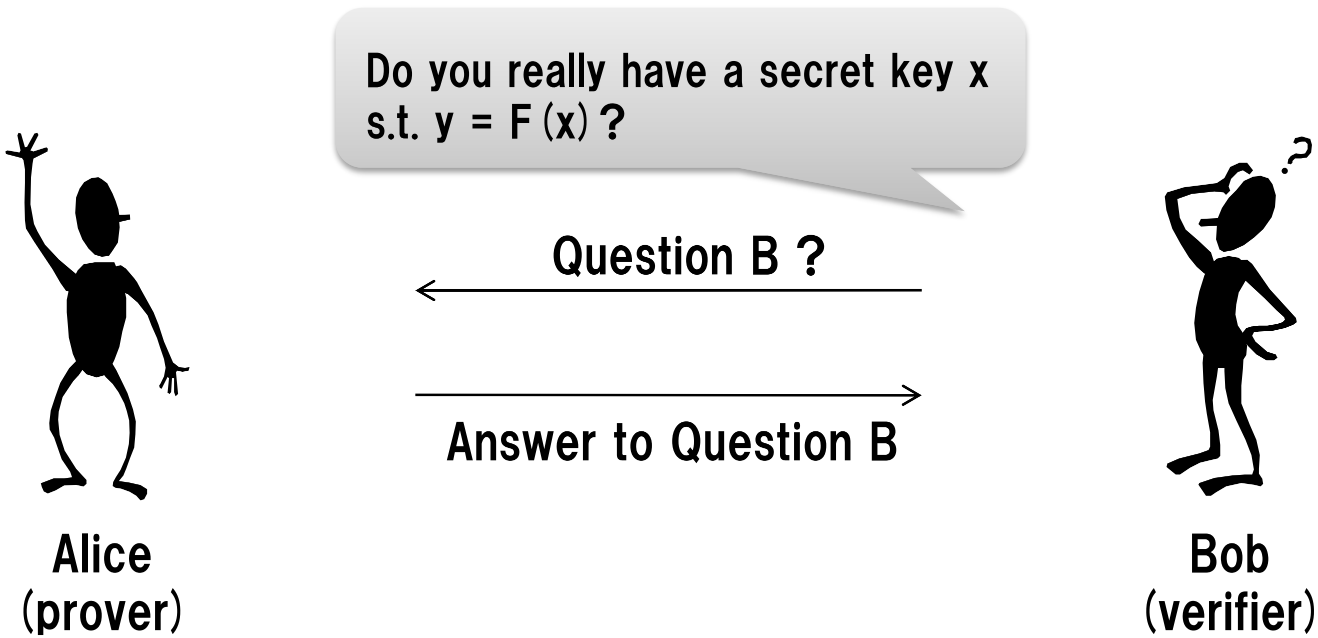


Cut and Choose (Intuition)

1. Cut   Question A + Question B

2. Ask only one out of the two questions

3. Answer to the chosen one



Cut and Choose (DL)

Question A :
Do you have X_A satisfying $r = g^{X_A}$?

Question B :
Do you have X_B satisfying $y = rg^{X_B}$?

I’m using a random number r

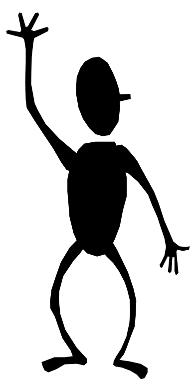
commit →

Do you have really have a secret key x
s.t. $y = g^x$?

← question

answer →

public key : $y = g^x$
secret key : x



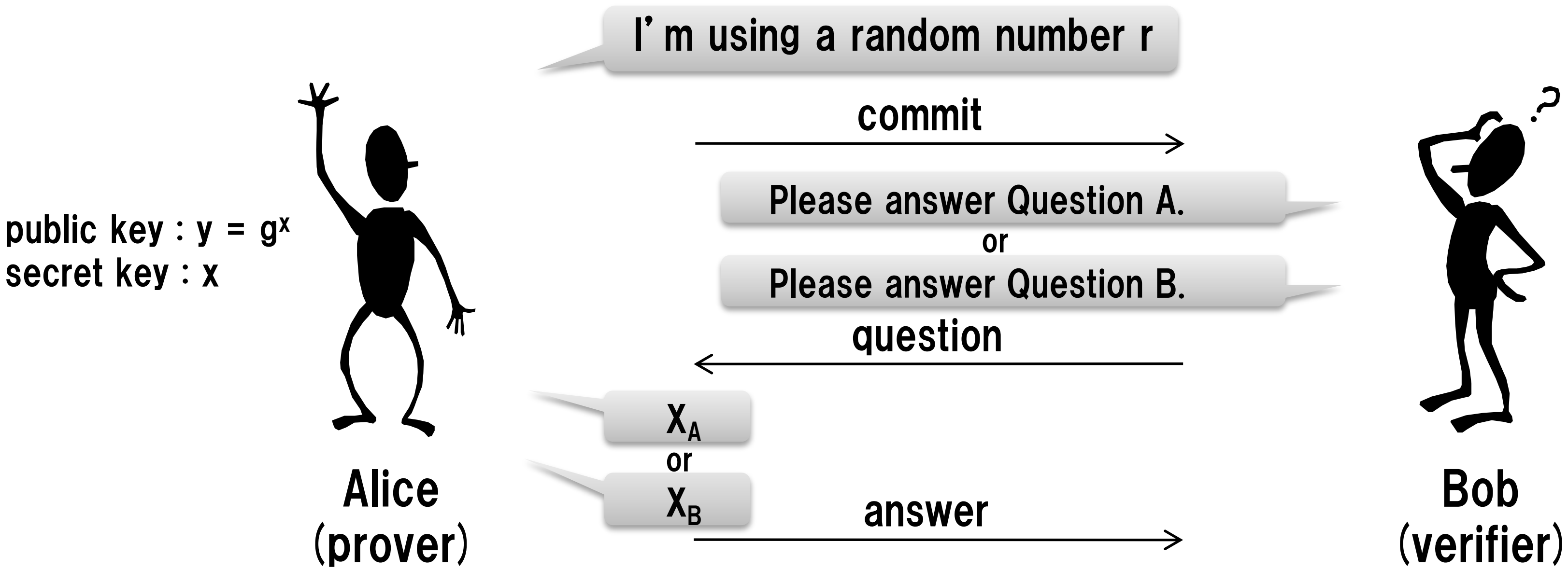
Alice
(prover)

Bob
(verifier)

Cut and Choose (DL)

Question A :
Do you have X_A satisfying $r = g^{X_A}$?

Question B :
Do you have X_B satisfying $y = rg^{X_B}$?



Cut and Choose (DL)

Question A :
Do you have X_A satisfying $r = g^{X_A}$?

Question B :
Do you have X_B satisfying $y = rg^{X_B}$?

If a prover has both correct answers X_A and X_B
Then she has a secret key $x = X_A+X_B$ s.t. $y = g^{X_A+X_B} = g^X$

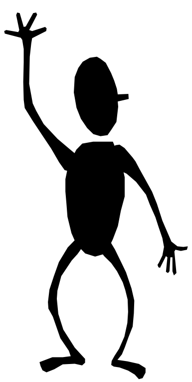
⬇ contraposition

If a prover doesn't have a secret key x s.t. $y = g^X$
Then she has only one out of X_A and X_B

Attacker can correctly answer only at most 1/2

I'm using a random number r

public key : $y = g^x$
secret key : x



Alice
(prover)

commit →

Please answer Question A.
or
Please answer Question B.

← question

X_A
or
X_B

answer →

Bob
(verifier)

Key point (Discrete Log)

DL problem

Given: y and g
Find: x
s.t.

$y = g^x$

→

Another form

Given: y and g
Find: r, x_A, x_B
s.t.

$r = g^{x_A}$
$y = rg^{x_B}$

Key point (Multivariate Quadratic)

- Multivariate Quadratic function F_{MQ}

$$F_{MQ}(x) = \begin{pmatrix} \Sigma_{ij} a_{1ij} x_i x_j + \Sigma_i b_{1i} x_i \\ \vdots \\ \Sigma_{ij} a_{mij} x_i x_j + \Sigma_i b_{mi} x_i \end{pmatrix}$$

$$G_{MQ}(x, y) = F_{MQ}(x+y) - F_{MQ}(x) - F_{MQ}(y)$$

$G_{MQ}(x, y)$ is linear in x

MQ problem

Given: y and F_{MQ}
Find: x
s.t.

$$y = F_{MQ}(x)$$

→

Another form

Given: y and F_{MQ}
Find: $r_0, r_1, t_0, t_1, e_0, e_1$
s.t.

$$G_{MQ}(t_0, r_1) + e_0 = y - F_{MQ}(r_1) - G_{MQ}(t_1, r_1) - e_1$$
$$t_0 = r_0 - t_1$$
$$e_0 = F_{MQ}(r_0) - e_1$$

Key point (Multivariate Cubic)

- Multivariate Cubic function F_{MC}

$$F_{MC}(x) = \begin{pmatrix} \Sigma_{ijk}\, a_{1ijk}\, x_i x_j x_k + \Sigma_{ij}\, b_{1ij}\, x_i x_j + \Sigma_i\, c_{1i}\, x_i \\ \vdots \\ \Sigma_{ijk}\, a_{mijk}\, x_i x_j x_k + \Sigma_{ij}\, b_{mij}\, x_i x_j + \Sigma_i\, c_{mi}\, x_i \end{pmatrix}$$

$$G_{MC}(x, y) + G_{MC}(y, x) = F_{MC}(x+y) - F_{MC}(x) - F_{MC}(y)$$

$G_{MC}(x, y)$ is linear in x

MC problem

Given: y and F_{MC}
Find: x
s.t.

$$y = F_{MC}(x)$$

→

Another form

Given: y and F_{MC}
Find: $r_0, r_1, t_0, t_1, u, e_0, e_1$
s.t.

$$G_{MC}(u, r_1) + e_1 = y - F_{MC}(r_1) - G_{MC}(t_0, r_1) - e_0$$
$$G_{MC}(u, r_0) - e_0 = e_1 - F_{MC}(r_0) - G_{MC}(t_1, r_0)$$
$$t_0 = r_0 - u$$
$$t_1 = r_1 - u$$

Key point (Multivariate Cubic) [V. Nachef, J. Patarin, E. Volte, 2012]

- Multivariate Cubic function F_{MC}

$$F_{MC}(x) = \begin{pmatrix} \Sigma_{ijk}\, a_{1ijk}\, x_i x_j x_k + \Sigma_{ij}\, b_{1ij}\, x_i x_j + \Sigma_i\, c_{1i}\, x_i \\ \vdots \\ \Sigma_{ijk}\, a_{mijk}\, x_i x_j x_k + \Sigma_{ij}\, b_{mij}\, x_i x_j + \Sigma_i\, c_{mi}\, x_i \end{pmatrix}$$

$G_{MC}(x, y, z)$ is linear in x

$$G_{MC}(x, y, z) = F_{MC}(x+y+z) - F_{MC}(x+y) - F_{MC}(x+z) - F_{MC}(y+z) + F_{MC}(x) + F_{MC}(y) + F_{MC}(z)$$

MC problem

Given: y and F_{MC}
Find: x
s.t.

$$y = F_{MC}(x)$$

Another form

Given: y and F_{MC}
Find: $r_0, r_1, r_2, t_0, t_1, e_0, e_1, f_0, f_1, h_0, h_1$
s.t.

$$y - G_{MC}(t_1, r_1, r_2) - f_1 - h_1 + e_1 - F_{MC}(r_1+r_2) - F_{MC}(r_1) - F_{MC}(r_2)$$
$$= G_{MC}(t_0, r_1, r_2) + f_0 + h_0 - e_0$$
$$t_0 = r_0 - t_1$$
$$F_{MC}(r_0) - e_1 = e_0$$
$$f_0 = F_{MC}(r_0+r_1) - f_1$$
$$h_0 = F_{MC}(r_0+r_2) - h_1$$

The MQ-based construction

Secret key: x
Public key: $y = F(x)$

Secret key x $\longrightarrow$ **Alice (prover)** | **Bob (verifier)**

Alice:

Randomly pick r_0, t_0, e_0
$r_1 \leftarrow x - r_0$, $t_1 \leftarrow r_0 - t_0$,
$e_1 \leftarrow F(r_0) - e_0$
$c_0 \leftarrow Com(r_1, G(t_0, r_1) + e_0)$
$c_1 \leftarrow Com(t_0, e_0)$
$c_2 \leftarrow Com(t_1, e_1)$

Alice $\rightarrow$ Bob: (c_0, c_1, c_2)

Bob: Randomly pick $Ch \in \{0,1,2\}$

Bob $\rightarrow$ Alice: Ch

Alice:

If Ch=0 then $\sigma = (r_0, t_1, e_1)$
If Ch=1 then $\sigma = (r_1, t_1, e_1)$
If Ch=2 then $\sigma = (r_1, t_0, e_0)$

Alice $\rightarrow$ Bob: σ

Bob:

If Ch=0 then check
$c_1 = Com(r_0 - t_1, F(r_0) - e_1)$, $c_2 = Com(t_1, e_1)$
If Ch=1 then check
$c_0 = Com(r_1, y - F(r_1) - G(t_1, r_1) - e_1)$
$c_2 = Com(t_1, e_1)$
If Ch=2 then check
$c_0 = Com(r_1, G(t_0, r_1) + e_0)$, $c_1 = Com(t_0, e_0)$

The MQ-based construction

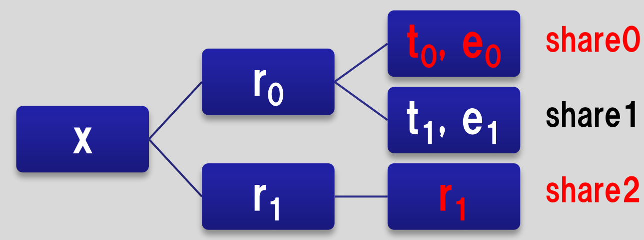
Secret key: x
Public key: $y = F(x)$

Secret key x → Alice (prover) | Bob (verifier)

Randomly pick r_0, t_0, e_0
$r_1 \leftarrow x - r_0$, $t_1 \leftarrow r_0 - t_0$,
$e_1 \leftarrow F(r_0) - e_0$
$c_0 \leftarrow \mathrm{Com}(r_1, G(t_0, r_1) + e_0)$
$c_1 \leftarrow \mathrm{Com}(t_0, e_0)$
$c_2 \leftarrow \mathrm{Com}(t_1, e_1)$

Commit these values

Divide x into three shares



Alice → Bob: (c_0, c_1, c_2)

Randomly pick $Ch \in \{0,1,2\}$

Bob → Alice: Ch

If Ch=0 then $\sigma = (r_0, t_1, e_1)$
If Ch=1 then $\sigma = (r_1, t_1, e_1)$
If Ch=2 then $\sigma = (r_1, t_0, e_0)$

Alice → Bob: σ

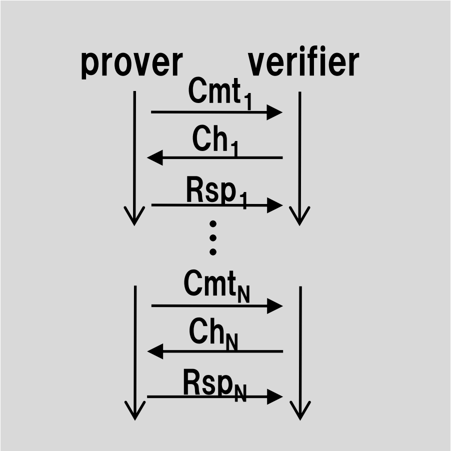
share0 and share1
If Ch=0 then check
$c_1 = \mathrm{Com}(r_0 - t_1, F(r_0) - e_1)$, $c_2 = \mathrm{Com}(t_1, e_1)$

share1 and share2
If Ch=1 then check
$c_0 = \mathrm{Com}(r_1, y - F(r_1) - G(t_1, r_1) - e_1)$
$c_2 = \mathrm{Com}(t_1, e_1)$

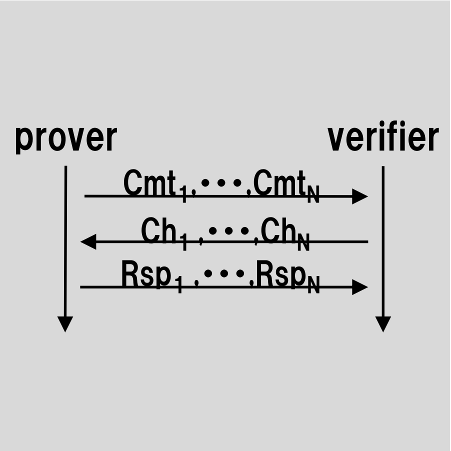
share0 and share2
If Ch=2 then check
$c_0 = \mathrm{Com}(r_1, G(t_0, r_1) + e_0)$, $c_1 = \mathrm{Com}(t_0, e_0)$

Public-key identification schemes

Sequential Composition



Parallel Composition



transform

Signature scheme

Comparison

	MI/HFE/UOV-type approach	Cut-and-Choose type approach
Speed	Very high	-
Security	Heuristic	Reduction
Post Quantum	○	○
Signature Size	Small	Large
Key size	Large	Small