General fault attacks on multivariate public key cryptosystems

Y. Hashimoto (Univ. of the Ryukyus)
T. Takagi (Kyushu Univ.)
K. Sakurai(ISIT)

Multivariate Public Key Cryptosystem (MPKC)

Public key consists of multivariate (quadratic) polynomials over a finite field k.

$$f_1(x_1, \cdots, x_n) = \sum_{i,j} a_{ij}^{(1)} x_i x_j + \sum_i b_i^{(1)} x_i + c^{(1)},$$

$$\vdots$$

$$f_m(x_1, \cdots, x_n) = \sum_{i,j} a_{ij}^{(m)} x_i x_j + \sum_i b_i^{(m)} x_i + c^{(m)}.$$

The security of MPKC is based on the difficulty of solving simultaneous multivariate equations.

$$f_1(x) = \cdots = f_n(x) = 0$$

Solving (randomly chosen) simultaneous multivariate quadratic equations is NP-hard.

$$\Downarrow$$

MPKC is expected as one of candidates of Post-Quantum Cryptography. (others : lattice-based cryptography, code-based cryptography, etc.)

MPKC is more efficient than RSA or ECC.

$$\Downarrow$$

We expect to apply MPKC to embedding systems.

Chen et al, CHES 2009.

Scheme	PubKey	SecKey	Encryp	Decryp
RSA(1024)	128B	1024B	22.4μs	813.5μs
ECDSA(160)	40B	60B	409.2μs	357.8μs
3HFE-p(31,9)	7KB	5KB	2.3μs	60.5μs
Rainbow(31,24,20,20)	57KB	150KB	17.7μs	70.6μs
TTS(31,24,20,20)	57KB	16KB	18.4μs	14.2μs

Attacks on MPKC.

1. Gröbner basis attacks,
2. Rank attacks,
3. Differential attacks,

etc.

Almost all attacks aim at evaluating the difficulty of problem of solving the multivariate equations or recovering secret keys.

There are no physical attacks except the side channel attack on the Sflash by Okeya-Takagi-Vuillaume, 2005.

Our goal is to evaluate the security against **Fault Attacks on MPKC**.

General construction of MPKC

k: a finite field of q elements.
n: # of variables, m: # of quadratic forms.

Secret keys: $S : k^n \to k^n$: an affine map.
$G : k^n \to k^m$: a quadratic map (G^{-1} is easy to compute).
$T : k^m \to k^m$: an affine map.

Public key: $F := T \circ G \circ S$.

$$F : k^n \xrightarrow{S} k^n \xrightarrow{G} k^m \xrightarrow{T} k^m$$

Encryption: $x(\text{message}) \mapsto F(x) = y(\text{cipher-text})$.

Decryption: $y \mapsto S^{-1}(G^{-1}(T^{-1}(y))) = x$.

One-way Function F

$$F : k^n \xrightarrow{S} k^n \xrightarrow{G} k^m \xrightarrow{T} k^m$$

It is easy to compute the inversion of the central map G^{-1}, but the map F becomes a one-way function by composing the random affine maps S and T.

$\Downarrow$

Attack target: (a part of) S and T.

The way of breaking S, T depends on the central map G.

Classification of MPKC

1. Big Field Type.

The polynomials over K, which is an extension field of k, are considered as those over k.
(Matsumoto - Imai, HFE, Sflash, I IC, Quarz, etc)

2. Stepwise Triangular System (STS) Type.

The multivariate quadratic equations can be solved step-by-step.
(Tsujii's STS scheme, Oil and vinegar, Rainbow, etc)

The proposed fault attack

Public-key $F : k^n \xrightarrow{S} k^n \xrightarrow{G} k^m \xrightarrow{T} k^m$

Fault attack on G.
We try to change a coefficient of G by a fault.

$$S, G, T \overset{\text{fault}}{\longmapsto} S, G', T$$

$$y \overset{S^{-1}, G'^{-1}, T^{-1}}{\longmapsto} x' \overset{F}{\longmapsto} y'$$

$\delta := y - y' = T \circ (G - G') \circ S(x).$

(1) # of Faults

Table: Our fault attacks on G

	Big Field	STS
#Fault	1	$n-1$
$\#(x,\delta)$	$\frac{1}{2}(n+1)(n+2)$	1
Recovering	parts of S, T	a part of T

Big Field type can be broken by a *single* fault.

(2) Success probability. The fault hits on G among the secrete parameters S, G, T. This is high enough.

Table: Success probability of our proposed fault attacks on some MPKCs.

Scheme	q	n	m	S	G	T
Quarz(2,103,129,3,4)	2	107	100	0.38	0.29	0.33
4HFE(31,10)	31	40	40	0.37	0.26	0.37
Rainbow(31,24,20,20)	31	64	40	0.07	0.90	0.03
Rainbow(256,18,12,12)	256	42	24	0.10	0.87	0.03

(3) Distinguishability. We give an algorithm that tells the fault hits the central map G or not.

Big field type

K : an extension field of k ($N := [K : k]$).
$\mathcal{G}$: a polynomial map over K.

$$G : k^n \overset{1-1}{\to} K^{n/N} \overset{\mathcal{G}}{\to} K^{m/N} \overset{1-1}{\to} k^m$$

Matsumoto-Imai Cryptosystem (1984, Eurocrypt'88)

$$\mathcal{G}(X) = X^{q^i+1} \quad (i \geq 0).$$

$\{1, w, \cdots, w^{n-1}\}$: a basis of K over k.
$x_1, \cdots, x_n \in k$.

$$\begin{aligned} X &= x_1 + x_2 w + \cdots + x_n w^{n-1}, \\ X^q &= (x_1, \cdots, x_n\text{-linear}) + \cdots + (x_1, \cdots, x_n\text{-linear}) w^{n-1}. \\ X^{q^i+1} &= (x_1, \cdots, x_n\text{-quadratic}) + \cdots + (x_1, \cdots, x_n\text{-quadratic}) w^{n-1} \end{aligned}$$

Patarin broke the one-wayness of G at Crypto'95.

HFE (Patarin, Eurocrypt'96)

$r \geq 1$.

$$\mathcal{G}(X) = \sum_{0 \leq i,j \leq r} \alpha_{ij} X^{q^i + q^j} + \sum_{0 \leq i \leq r} \beta_i X^{q^i} + \gamma, \quad (\alpha_{ij}, \beta_i, \gamma \in K).$$

Decryption: We solve equation $\mathcal{G}(X) = Y$ over K.
Its complexity is $O(q^{2r} \times (\text{polyn.}))$.

Attacks:

1. Kipnis-Shamir attack (Crypto'99): break the secret S, T.
2. Gröbner basis attack (F4): break the message.

Both attacks are effective for small r.

Stepwise Triangular System (STS) Type

$G(x) = (g_1(x), \cdots, g_m(x))$.
$1 \leq n_1 < \cdots < n_l = n$
$1 \leq m_1 < \cdots < m_l = m$

$$
\begin{aligned}
g_1(x), \cdots, g_{m_1}(x) &= (x_1, \cdots, x_{n_1}\text{-quadratic}) \\
g_{m_1+1}(x), \cdots, g_{m_2}(x) &= (x_1, \cdots, x_{n_1}, \cdots, x_{n_2}\text{-quadratic}) \\
&\vdots \\
g_{m_{l-1}+1}(x), \cdots, g_m(x) &= (x_1, \cdots, x_{n_1}, \cdots, x_{n_2}, \cdots, x_n\text{-quadratic})
\end{aligned}
$$

Tsujii's STS scheme (1986)

$$
\begin{aligned}
g_1(x) &= (x_1\text{-linear}) && (1)\\
g_2(x) &= (x_1\text{-quad.}) + x_2(x_1\text{-linear}) && (2)\\
&\vdots\\
g_n(x) &= (x_1, \cdots, x_{n-1}\text{-linear}) + x_n(x_1, \cdots, x_{n-1}\text{-linear}) && (n)
\end{aligned}
$$

Decryption:
Find x_1 using (1), then substitute x_1 to others,
Find x_2 using (2), then substitute x_2 to others, ...

Hasegawa-Kaneko proposed an attack to beak the one-wayness of this central map G (SITA'87).

UOV (Patarin, 1997)

$$g_l(x) = \sum_{1 \le i \le m} x_i(x_{m+1}, \cdots, x_n\text{-linear}) + (x_{m+1}, \cdots, x_n\text{-quadratic})$$
$$= x^t \begin{pmatrix} 0_m & * \\ * & * \end{pmatrix} x + (\text{linear}) \quad (1 \le l \le m).$$

Signature generation:

1. Choose random values for $x_{m+1}, \cdots, x_n$.
2. Solve the linear equation of $x_1, \cdots, x_m$.

Kipnis-Shamir attack (Crypto'98) recovers a part of S with $O(q^{n-2m} \times (\text{polyn.}))$-complexity.

$\Downarrow$

# of variables must be sufficiently larger than twice of that of equations.

Rainbow (Multi-layer UOV, Ding-Schmidt, PKC'05)

$$g_l(x) = \begin{cases} x^t \begin{pmatrix} 0_{m_1} & * \\ * & * \end{pmatrix} x + (\text{linear}), & (1 \le l \le m_1), \\ x^t \begin{pmatrix} 0_{m_1} & 0 & 0 \\ 0 & 0_{m-m_1} & * \\ 0 & * & *_{n-m} \end{pmatrix} x + (\text{linear}), & (m_1 + 1 \le l \le m), \end{cases}$$

Signature generation:

1. Choose random values for $x_{m+1}, \cdots, x_n$.
2. Solve the linear equation $g_{m_1+1} = \cdots = g_m(x) = 0$ of $x_{m_1+1}, \cdots, x_m$.
3. Solve the linear equation $g_1(x) = \cdots = g_{m_1}(x) = 0$ of $x_1, \cdots, x_{m_1}$.

Attacks:

1. Rank attacks recover a part of T.
2. K-S attack on UOV recovers a part of S.

Major attacks on MPKCs

1. **Direct attack:** we break the message y by solving $F(y) = x$ using Gröbner basis attack (F4/F5), XL algorithm, etc.
2. **Rank attack:** If the rank of matrix associated to the quadratic form has some special property, then we can find (a part of) the secret key T.
3. **Differential Attack:** Using the difference $F(x + t) - F(x) - F(t)$, we try to convert the BF type to its "minus" or "vinegar". This attack is effective to MI-,HFEv, Sflash ,etc.
4. **Attack on UOV:** If the central map G is equivalent to that of UOV, then we can break (a part of) the secret key S.

etc.

The proposed fault attack on G

Encryption function: $F : k^n \xrightarrow{S} k^n \xrightarrow{G} k^m \xrightarrow{T} k^m$

BF type (HFE case):

$$\mathcal{G}(X) = \sum_{0 \le i,j \le r} \alpha_{ij} X^{q^i + q^j} + \sum_{0 \le i \le r} \beta_i X^{q^i} + \gamma, \quad \text{(over } K\text{)}.$$

STS type

$$g_1(x_1, \cdots, x_n) = \sum_{i,j} a_{ij}^{(1)} x_i x_j + \sum_i b_i^{(1)} x_i + c^{(1)},$$

$$\vdots$$

$$g_m(x_1, \cdots, x_n) = \sum_{i,j} a_{ij}^{(m)} x_i x_j + \sum_i b_i^{(m)} x_i + c^{(m)}, \quad \text{(over } k\text{)}.$$

Step 1. Cause a fault on G, which changes one coefficient α_{ij} or $a_{ij}^{(l)}$.

$$F' : k^n \xrightarrow{S} k^n \xrightarrow{G'} k^m \xrightarrow{T} k^m$$

Step 2. For randomly chosen $y_1, \cdots, y_l \in k^m$, we decrypt $y_1, \cdots, y_l \in k^m$ using G'.

$$x_i := S^{-1}(G'^{-1}(T^{-1}(y_i))) = F'^{-1}(y_i).$$

Step 3. We re-encrypt x_i using F.

$$z_i := F(x_i).$$

Step 4. Find the secret key S and T by $\delta_i := y_i - z_i$.

$$\delta_i = y_i - z_i = (F - F')(x_i) = T \circ (G - G') \circ S(x_i)$$

Map $G - G'$

$(G - G')(x)$ is an extremely sparse polynomial, so that we can easily guess the secret key.

Big Field Type (HFE)

$$(\mathcal{G} - \mathcal{G}')(X) = cX^{q^i+q^j}$$

is almost same as Matsumoto-Imai.

$\Downarrow$

S and T can be recovered by Kipnis-Shamir attack.

Only one fault is necessary.

STS Type

$$(G - G')(x) = (0, \cdots, 0, cx_i x_j, 0, \cdots, 0)^t$$
$$\Rightarrow \delta_i = T \circ (G - G') \circ S(x_i) = T\left((0, \cdots, 0, \alpha, 0, \cdots, 0)^t\right).$$

$$\Downarrow$$

The ratio of the entries in δ_i leaks a column vector of T.

Recovering enough part of T with fault attacks in several times, rank attacks can recover T.

Straight-forward Countermeasures

Original Decryption Process:

Compute $y \overset{S^{-1},G^{-1},T^{-1}}{\longmapsto} x$.

Improved Decryption Process:

1. Check whether G is correct.
2. If correct, compute $y \overset{S^{-1},G^{-1},T^{-1}}{\longmapsto} x$.
3. If incorrect, stop the decryption.

How to check?

ex) Store $c := \sum(\text{coeff. in } G)$ and compare c with $\sum(\text{coeff. in } G)$.

Easy and low cost!

Conclusions

1. We proposed fault attacks on MPKC, which can find (a part of) secret key of both BF type and STS type.

2. We estimated the success probability of the proposed fault attack.

3. It is an open problem to apply this fault attack on the QUAD which is a stream cipher based on quadratic equations.