PQCrypto 2022

A New Fault Attack on UOV Multivariate Signature Scheme

Hiroki Furue[1], Yutaro Kiyomura[2], Tatsuya Nagasawa[1], Tsuyoshi Takagi[1]

1. The University of Tokyo, Japan
2. NTT Social Informatics Laboratories, Japan

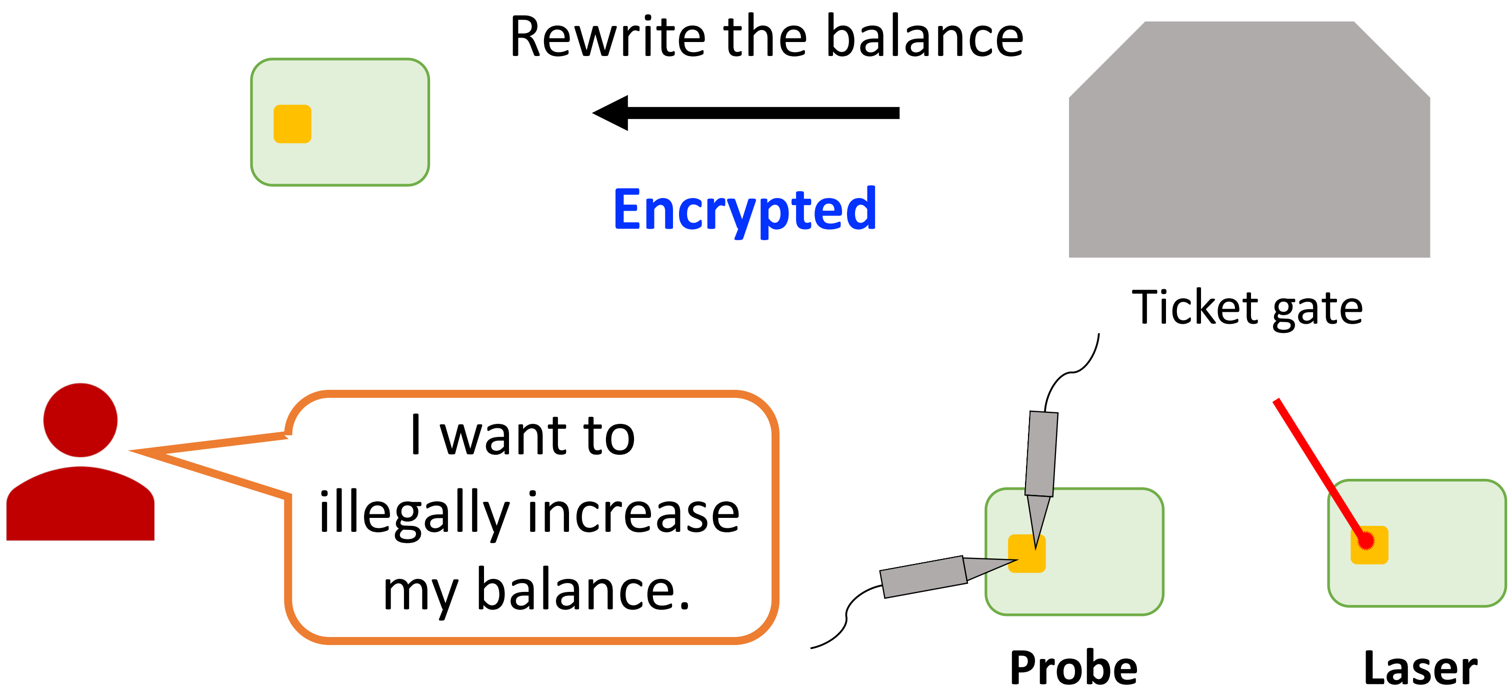
Outline

- **Fault Attacks**
- UOV
- Our Proposed Attack
- Conclusion

Physical Attacks

Physical Attacks:
utilize physical access to the cryptographic devices

Ex) Smart cards



Physical Attack

- **Probing attack**

  Extract sensitive information by direct access to the internal.

- **Fault attack**

  Stress the device by voltage or light and generate errors which lead to a security failure of the system.

- **Side-channel attack**

  Exploit timing information, power consumption, and electromagnetic leaks.

Outline

- Fault Attacks
- **UOV**
- Our Proposed Attack
- Conclusion

MPKC

- Multivariate Public Key Cryptosystems (MPKC)
  - based on the difficulty of **MQ problem**
  - candidates for **post quantum cryptosystems**
  - mainly used for **digital signature**

MQ (Multivariate Quadratic equations) problem

Given $\mathcal{F} = (f_1, \dots, f_m) \in \mathbb{F}_q[x_1, \dots, x_n]^m$ with $\deg f_i = 2$,

find *one* solution $(a_1, \dots, a_n) \in \mathbb{F}_q^n$ such that

$$\mathcal{F}(a_1, \dots, a_n) = \mathbf{0} \in \mathbb{F}_q^m.$$

Unbalanced Oil and Vinegar

[Kipnis et al., EUROCRYPT 1999]

- One of multivariate signature schemes
- UOV has essentially not been broken for over 20 years.
- Rainbow (third-round finalist) is a variant of UOV.

Advantage

- Small signature
- Short execution time

Disadvantage

- Large public key

Key Generation

$n, m \in \mathbb{N} \quad (n > m)$

n : the number of variables, m: the number of equations

① **Central map**

$\mathcal{F} = (f_1, \dots, f_m): \mathbb{F}_q^n \to \mathbb{F}_q^m$ **[invertible quadratic map]**

$$f_k = \sum_{i=1}^{n} \sum_{j=1}^{v} \alpha_{ij}^{(k)} x_i x_j \qquad (v = n - m)$$

② $\mathcal{T}: \mathbb{F}_q^n \to \mathbb{F}_q^n$ **[linear map]**

③ $\mathcal{P} = \mathcal{F} \circ \mathcal{T}$ **[quadratic map]**

Public Key: $\mathcal{P}$, **Secret Key:** $(\mathcal{F}, \mathcal{T})$

Unbalanced Oil and Vinegar

Message	$\boldsymbol{m} \in \mathbb{F}_q^m$
Signature	$\boldsymbol{s} = \mathcal{T}^{-1} \circ \mathcal{F}^{-1}(\boldsymbol{m})$
Verification	$\boldsymbol{m} \stackrel{?}{=} \mathcal{P}(\boldsymbol{s})$

Computing $\mathcal{F}^{-1}$

① Fix variables $x_1, \ldots, x_v$ randomly

$$f_k = \sum_{i=1}^{v} \sum_{j=1}^{v} \alpha_{ij}^{(k)} x_i x_j + \sum_{i=v+1}^{n} \sum_{j=1}^{v} \alpha_{ij}^{(k)} x_i x_j$$

② Solving a linear polynomial in $x_{v+1}, \ldots, x_n$
(m equations, m variables)

※ If there does not exist a solution, return to ①.

Representation Matrices

- $(p_1, \dots, p_m) = (f_1, \dots, f_m) \circ \mathcal{T}$

$$f_i(x) = (x_1 \cdots x_n) \begin{pmatrix} MF_i \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad \mathcal{T}(x) = \begin{pmatrix} MT \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$m \times m$ ⇧

$$p_i(x) = (x_1 \cdots x_n) \begin{pmatrix} MP_i \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$= (x_1 \cdots x_n) \begin{pmatrix} MT^{\top} \end{pmatrix} \begin{pmatrix} MF_i \end{pmatrix} \begin{pmatrix} MT \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Outline

- Fault Attacks
- UOV
- **Our Proposed Attack**
- Conclusion

Fault Attacks on UOV

- cause a fault to change a coefficient of the secret key
- cause a fault such that random values in computing $\mathcal{F}^{-1}$ are fixed to the same values.

signature scheme	fault on secret key	fault on random values
UOV	**Our Result**	①
Rainbow	①	①
LUOV	②*	(①)

① [Hashimoto et al., PQCrypto 2011]

② [Mus et al., CCS 2020]

Attack Model

(following ① [Hashimoto et al., PQCrypto 2011])

- One fault changes one coefficient of the secret key $\mathcal{F}, \mathcal{T}$.
- A coefficient of $\mathcal{F}, \mathcal{T}$ changed by a fault is randomly chosen.

  $\mathcal{F}: O(\lceil \log q \rceil \cdot n^2 \cdot m)$ bit, $\mathcal{T}: O(\lceil \log q \rceil \cdot n^2)$ bit

  ⇨ Faults are caused on $\mathcal{F}$ with high probability.

- The attacker cannot know the location of the faults.
- Coefficients changed by the faults do not return to the original values (even if new faults are injected).

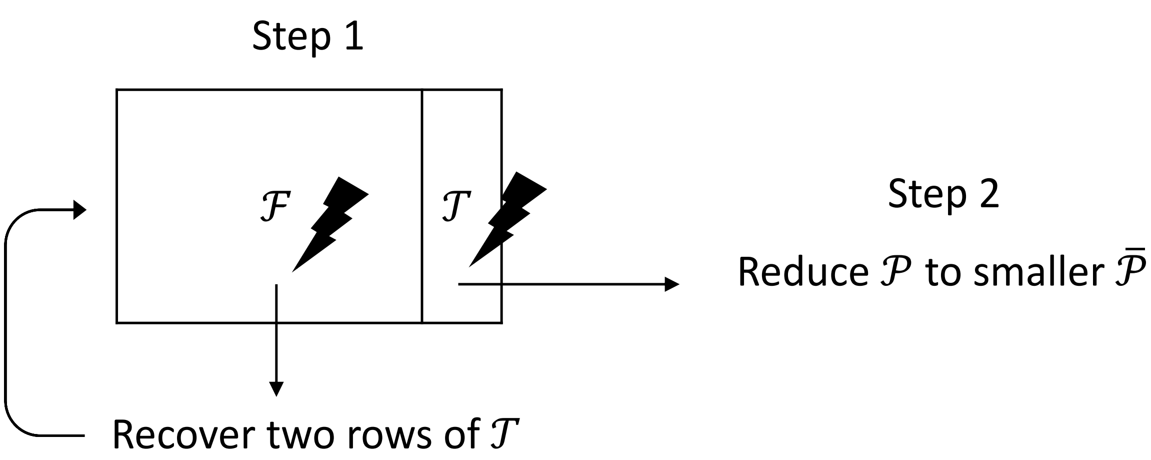
Rough Description

Step1: Recover some rows of the secret key $\mathcal{T}$

by utilizing faults caused on $\mathcal{F}$.

Step2: Transform the public key $\mathcal{P}$ into

a public key system $\bar{\mathcal{P}}$ with fewer variables.



Step1: Basic Strategy

Assumption: $\mathcal{F}$ is changed into $\mathcal{F}'$ by a fault.

$$\left(\alpha_{ij}^{(k)} \to \alpha'^{(k)}_{ij}:\ \ f_k = \sum_{i=1}^{n}\sum_{j=1}^{v}\alpha_{ij}^{(k)} x_i x_j\right)$$

① Randomly choose $m_\ell \in \mathbb{F}_q^m$.

② $s_\ell \coloneqq \mathcal{T}^{-1} \circ \mathcal{F}'^{-1}(m_\ell)$

(using signing oracle with the fault)

③ $\delta_\ell \coloneqq \mathcal{P}(s_\ell) - m_\ell$

Signing Oracle
(Secret Key)

- Input : Message
- Output: Signature

Step1: Basic Strategy

① $m_\ell \in \mathbb{F}_q^m$

② $s_\ell := \mathcal{T}^{-1} \circ \mathcal{F}'^{-1}(m_\ell)$

③ $\delta_\ell := \mathcal{P}(s_\ell) - m_\ell$

$$\delta_\ell = (\mathcal{F} \circ \mathcal{T})(s_\ell) - (\mathcal{F}' \circ \mathcal{T})(s_\ell)$$

$$= (\mathcal{F} - \mathcal{F}') \circ \mathcal{T}(s_\ell)$$

$$\left(0, \dots, 0, \left(\alpha_{ij}^{(k)} - \alpha'^{(k)}_{ij}\right) x_i x_j, 0, \dots, 0\right)$$

$$= \left(0, \dots, 0, \left(\alpha_{ij}^{(k)} - \alpha'^{(k)}_{ij}\right) \underline{\left(\mathcal{T}(s_\ell)\right)_i} \underline{\left(\mathcal{T}(s_\ell)\right)_j}, 0, \dots, 0\right)$$

The i-th and j-th elements of $\mathcal{T}(s_\ell)$

Step1: Basic Strategy

$$(\delta_\ell)_k = \underbrace{\left(\alpha_{ij}^{(k)} - \alpha'^{(k)}_{ij}\right)}_{=\beta} \underbrace{\left(\mathcal{T}(s_\ell)\right)_i}_{=\sum_{p=1}^{n} t_{ip}(s_\ell)_p} \left(\mathcal{T}(s_\ell)\right)_j$$

(t_{ij} : (i,j)-th element of MT)

$$= \beta\left(t_{i1}(s_\ell)_1 + \cdots + t_{in}(s_\ell)_n\right)\left(t_{j1}(s_\ell)_1 + \cdots + t_{jn}(s_\ell)_n\right)$$

$$= \beta \sum_{p \le q} (s_\ell)_p (s_\ell)_q \underbrace{\begin{cases} \left(t_{ip}t_{jq} + t_{iq}t_{jp}\right) & (p \ne q) \\ t_{ip}t_{jp} & (p = q) \end{cases}}_{= y_{pq}}$$

- $(\delta_\ell)_k, s_\ell$ are known ⇨ a linear polynomial in variables y_{pq}
- $\left(t_{i1}, \ldots, t_{in}\right), \left(t_{j1}, \ldots, t_{jn}\right)$ can be recovered from y_{pq}.

Step1: Description

① Cause a new fault $(\mathcal{F} \to \mathcal{F}')$

② Prepare $\left((\delta_1)_k, s_1\right), \dots, \left((\delta_N)_k, s_N\right)$. $\left(\delta_\ell = (\mathcal{F} - \mathcal{F}') \circ \mathcal{T}(s_\ell)\right)$

③ Solve a linear system

$$(\delta_\ell)_k = \sum_{p \le q} (s_\ell)_p (s_\ell)_q y_{pq} \quad (1 \le \ell \le N)$$

in $\{y_{pq}\}_{1 \le p \le q \le n}$

(If $N \ge n(n+1)/2$, then a solution will be uniquely determined.)

④ Obtain $(t_{i1}, \dots, t_{in}), \left(t_{j1}, \dots, t_{jn}\right)$ from $\{y_{pq}\}_{1 \le p \le q \le n}$

・①～④ is iterated until a new fault is caused on $\mathcal{T}$.

Step2: Description

Assumption: α rows of $\mathcal{T}$ are recovered in Step1.

① Transform $\mathcal{T}$ into a special form

② Reduce the public key $\mathcal{P}$ into a smaller system

It can be broken with **smaller complexity**
than the original system.

Step2: Transformation of $\mathcal{T}$

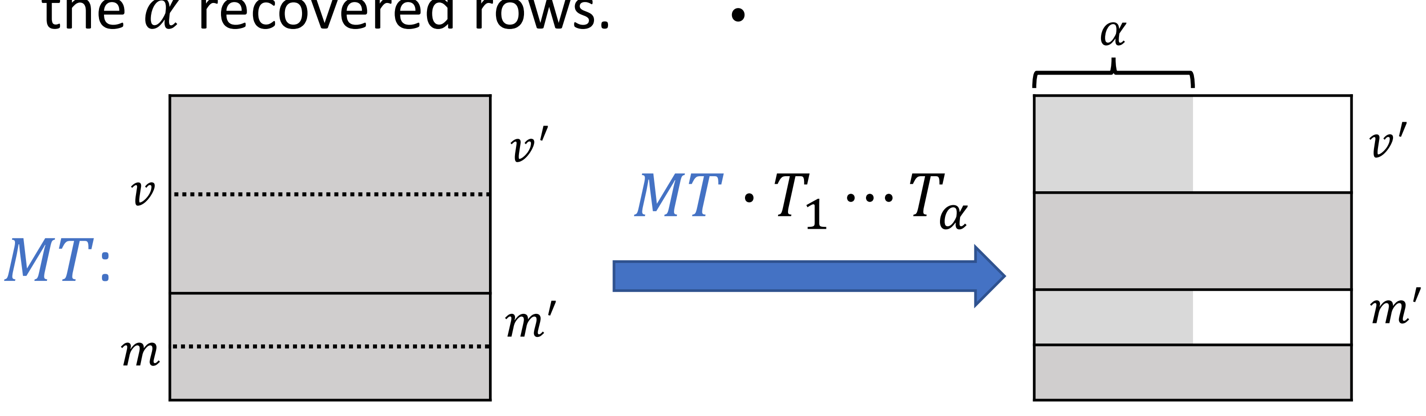
$(t_{i1}, \dots, t_{in})$: the i-th row vector of MT recovered in Step1

$$T_1: \begin{bmatrix} 1 & -\frac{t_{i2}}{t_{i1}} & \cdots & -\frac{t_{in}}{t_{i1}} \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} \Rightarrow MT \cdot T_1: \begin{bmatrix} t_{i1} & 0 & \cdots & 0 \\ & & & \\ & & & \end{bmatrix}$$

$$\left(t_{i1} \cdot \left(-\frac{t_{ij}}{t_{i1}}\right) + t_{ij} = 0\right)$$

Iterate for
the α recovered rows.

$\vdots$



$(\alpha = v' + m')$

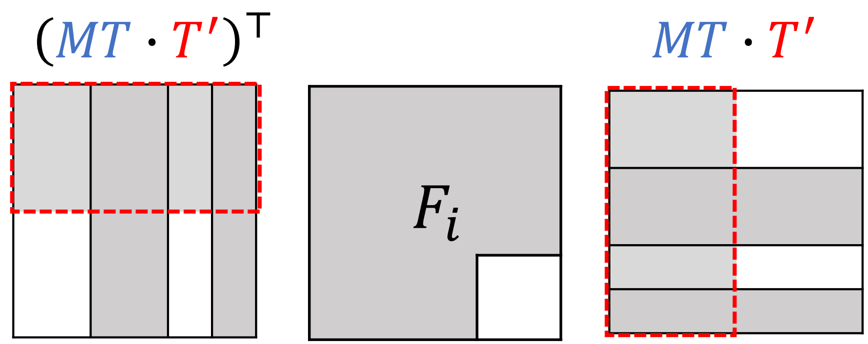
Step2: Reduction

$T' := T_1 \cdots T_\alpha$

$p_i(T'(x_1, \dots, x_n)^\top)$

$$= (x_1 \cdots x_n) \cdot T'^\top \cdot \overbrace{MT^\top \cdot MF_i \cdot MT}^{MP_i} \cdot T' \cdot (x_1 \cdots x_n)^\top$$

$$= (x_1 \cdots x_n)$$



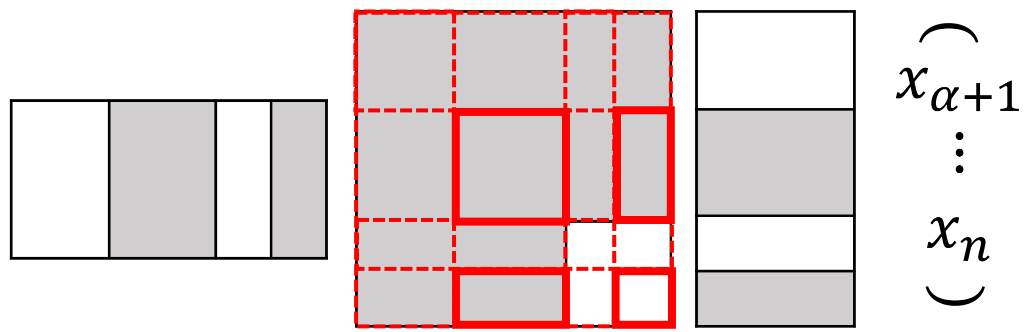
$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Substitute $(x_1, \dots, x_\alpha) = (0, \dots, 0)$

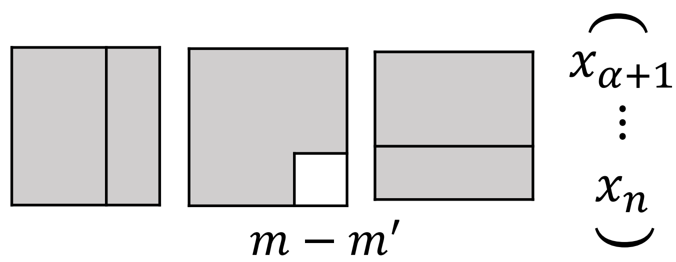
Step2: Reduction

$p_i(T'(0, \dots, 0, x_{\alpha+1}, \dots, x_n)^\top)$

$= (x_{\alpha+1} \cdots x_n)$



$= (x_{\alpha+1} \cdots x_n)$



Reduction to the UOV public key in $n - \alpha$ variables

($v - v'$: vinegar variables, $m - m'$: oil variables)

Our Results

Existing key recovery attacks can be performed with smaller complexity on the resulting system.

Simulations for some parameters (100-bit security)

- The proposed attack can reduce the given system into one with only 90-bit security with a probability of approximately 80 ~ 90%.
- The proposed attack works even when the number of faults is limited.

Outline

- Fault Attacks
- UOV
- Our Proposed Attack
- **Conclusion**

Conclusion

- We propose a new fault attack on UOV signature scheme.
- The proposed attack is the first attack on UOV utilizing faults caused on the secret key.
- A naive countermeasure against the proposed attack would be to check whether the secret key is faulty.