Cryptanalysis of Hash-based Tamed Transformation and Minus Signature Scheme

Xuyun Nie[1,2,3] Zhaohu Xu[1] Johannes Buchmann[2]

[1]University of Electronic Science and Technology of China

[2] TU Darmstadt, Germany

[3] Chinese Academy of Sciences

June 6, 2013

Outline

Introduction

General Form of MPKC (Multivariate Public Key Cryptosystem)

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^m,\ F : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

$$Y = (y_1, \cdots, y_m) = P(x_1, \cdots, x_n) = T \circ F \circ U(x_1, \cdots, x_n)$$

- Public key:
  $P(x_1, \ldots, x_n) = (P_1(x_1, \ldots, x_n), \ldots, P_m(x_1, \ldots, x_n))$.
- Private key: Two invertible affine maps T and U; the central map F.

Main attacks on MPKC

- Linearization Equations attack: MI, TTM, MFE etc.
- Differential attack: PMI, IPHFE, SFLASH, etc.
- Rank attack: Goubin and Courtois (2000); Kipnis and Shamir (1999) etc.
- Direct Inversion Attacks: XL, F_4, F_5 etc.

Security enhancement method

1. **Plus**: Add some random quadratic polynomials in central map.
2. **Minus:** Move some quadratic polynomials from public key.
3. **Vinegar:** Add several variables which may be quadratic in terms of themselves and cross quadratic with original variables.
4. **Internal perturbation:** Add several random quadratic terms in the expressions of central map, where the values of these quadratic terms is limited in a small space.
5. **Piece in Hand:** Some secret matrices did not used in generating public key but must be used in decryption.

Hash-based Tamed Transformation and Minus Signature Scheme

Main Idea

Wang H Z, Zhang H G, et al. Extended multivariate public key cryptosystems with secure encryption function. *Sci China Inf Sci*, June 2011 Vol. 54 No. 6: 1161-1171.

- In order to enhance the security of MPKC, they used a Hash-based Tame (HT) transformation to introduce some new variables in public key.
- Combined with minus method, they proposed HTTM (Hash-based tame and minus) signature scheme.

Symbol	Meaning
$\mathbb{F}_q$	a degree k extension of the field $\mathbb{F}_2$,where $q = 2^k$.
$\mathbb{F}_q^n$	n-dimensional vectorspace over $\mathbb{F}_q$.
$\mathbb{F}_{q^n}$	a degree n extension of the field $\mathbb{F}_q$.
$H(\cdot)$	a standard hash function such as SHA-1
$H_k(\cdot)$	an operation extracting the first k bits of $H(\cdot)$ and mapping the bitstring into an element in $\mathbb{F}_q$.
$a \parallel b$	concatenation of variables a and b.
δ	the number of extended input variables of public key.
μ	the number of deleted equations of the public key.

HT transformation (Hash-based tame transformation)

$L : F_q^{n+\delta} \rightarrow F_q^n$

$$\begin{cases} \begin{pmatrix} h_1 \\ \vdots \\ h_{n-\delta} \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n-\delta} \end{pmatrix} + \alpha_1 \\ \begin{pmatrix} h_{n-\delta+1} \\ \vdots \\ h_n \end{pmatrix} = \begin{pmatrix} x_{n-\delta+1} \\ \vdots \\ x_n \end{pmatrix} + D \cdot \begin{pmatrix} x_{n+1} \\ \vdots \\ x_{n+\delta} \end{pmatrix} + B \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n-\delta} \end{pmatrix} + \alpha_2 \end{cases}$$

where α_1, α_2 are $n-\delta$-dimension vector and δ-dimension vector respectively; $(n-\delta) \times (n-\delta)$ matrix A and full-rank $\delta \times \delta$ diagonal matrix D ; B is a $\delta \times (n-\delta)$ random matrix.

HT transformation (cont.)

- Definition of x_{n+i} $(1 \leq i \leq \delta)$:

$$x_{n+i} = H_k(x_1 \parallel x_2 \parallel \cdots \parallel x_{n-\delta+i-1})$$

-

$$(h_1, \ldots, h_n) = L(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+\delta})$$

- Public key:

$$\bar{P} = (\bar{P}_1, \ldots, \bar{P}_n) = P \circ L = T \circ F \circ U \circ L$$

- Removing the last μ eqution in $\bar{P}$, we get

$$\bar{P}^- = (\bar{P}_1, \ldots, \bar{P}_{n-\mu}) = T^- \circ F \circ U \circ L$$

HTTM

- *Private key* T, U, F and L
- *Public key*

$$\bar{P}^{-}(x_1, \ldots, x_{n+\delta}) = (\bar{P}_1, \ldots, \bar{P}_{n-\mu})$$

- *Signing* Given $y' = (y'_1, \cdots, y'_{n-\mu}) \in \mathbb{F}_q^{n-\mu}$. Appended it to $y' = (y'_1, \cdots, y'_n) \in \mathbb{F}_q^n$. Calculates

$$x = (x'_1, \ldots, x'_{n+\delta}) = L^{-1} \circ U^{-1} \circ F^{-1} \circ T^{-1}(y'_1, \cdots, y'_n).$$

- *Verification* Firstly, compute and check

$$x'_{n+i} = H_k(x'_1 \parallel x'_2 \parallel \cdots \parallel x'_{n-\delta+i-1}), 1 \leq i \leq \delta.$$

then check

$$\bar{P}^{-}(x'_1, \ldots, x'_{n+\delta}) = (y'_1, \cdots, y'_{n-\mu}).$$

Cryptanalysis of HTTM

Our Result

If there exists an algorithm $\mathcal{A}$ can forge a valid signature of the original MPKC-minus signature scheme, we could also forge a valid signature of HTTM.

Construct a New Public Key

Proposition 1: Let all terms which contained $x_{n+i}(1 \leq i \leq \delta)$ equal to zero in public key $\bar{P}^{-}$ of a HTTM scheme, we can get a new public key $\bar{P}^{-}_{L'}$, which is equivalent to the public key of the original MPKC-minus signature scheme, where L' is the special case of the function L with matrix $D = 0$.

Proof.

On one hand, set $D = 0$ in L

$$L = \begin{pmatrix} A & O & O \\ B & I & D \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_{n+\delta} \end{pmatrix} + \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$$

Let $L^{'} : F_q^{n+\delta} \rightarrow F_q^n$

$$L^{'} = \begin{cases} \begin{pmatrix} h_1 \\ \vdots \\ h_{n-\delta} \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n-\delta} \end{pmatrix} + \alpha_1 \\ \begin{pmatrix} h_{n-\delta+1} \\ \vdots \\ h_n \end{pmatrix} = \begin{pmatrix} x_{n-\delta+1} \\ \vdots \\ x_n \end{pmatrix} + B \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{n-\delta} \end{pmatrix} + \alpha_2 \end{cases}$$

The matrix form is

$$\begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} = \begin{pmatrix} A & O \\ B & I \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$$

Replaced L by L' in $\bar{P}^-$, we get

$$\bar{P}^-_{L'} = P \circ L'^- = T^- \circ F \circ U \circ L'$$

On the other hand, set $x_{n+i} = 0 (1 \leq i \leq \delta)$ in $\bar{P}^-$,then

$$\bar{P}^- \Rightarrow \bar{P}^-_{L'}.$$

Due to L' is an affine map, $\bar{P}^-_{L'}$ is equivalent to the original one. So, we can use the algorithm $\mathcal{A}$ to forge a signature of $\bar{P}^-_{L'}$.

Relationship between the Signatures under Two Public Keys

Proposition 2. Given a message $y' = (y'_1, \cdots, y'_{n-\mu}) \in \mathbb{F}_q^{n-\mu}$, consider the signatures under $\bar{P}^-$ and $\bar{P}^-_{L'}$, denote them $x' = (x'_1, \cdots, x'_{n+\delta})$ and $x'' = (x''_1, \cdots, x''_n)$, respectively. If we choose the same values of $y'_{n-\mu+1}, \cdots, y'_n$, then $x' = (x'_1, \cdots, x'_{n+\delta})$ and $x'' = (x''_1, \cdots, x''_n)$ satisfy:

(1) $x'_i = x''_i, \quad i = 1, \cdots, n-\delta;$

(2) $x'_{n-\delta+i} = x''_{n-\delta+i} - D[i][i]x'_{n+i}, \quad i = 1, \cdots, \delta$

where $D[i][i]$ denotes the i^{th} element in the diagonal of matrix D.

Key Point of Proof

- Given the same message, Observing the signature generation process, we found that the only difference in two functions is the difference between L' and L.
- - $x'_i = x''_i, \quad i = 1, \cdots, n-\delta;$
  - $$\begin{pmatrix} x'_{n-\delta+1} \\ \vdots \\ x'_n \end{pmatrix} + D \cdot \begin{pmatrix} x'_{n+1} \\ \vdots \\ x'_{n+\delta} \end{pmatrix} + B \cdot \begin{pmatrix} x'_1 \\ \vdots \\ x'_{n-\delta} \end{pmatrix} + \alpha_2 =$$
    $$\begin{pmatrix} x''_{n-\delta+1} \\ \vdots \\ x''_n \end{pmatrix} + B \cdot \begin{pmatrix} x''_1 \\ \vdots \\ x''_{n-\delta} \end{pmatrix} + \alpha_2$$

Getting the Value of Matrix D

Proposition 3. Given a public key of HTTM, $\bar{P}^- = T^- \circ F \circ U \circ L$, we can recover the value of matrix D from it.

let $x_1 = x_2 = \cdots = x_n = 0$ in L and $x_1 = x_2 = \cdots = x_{n-\delta} = 0$ in L', compare

$$\left\{ \begin{pmatrix} h_{n-\delta+1} \\ \vdots \\ h_n \end{pmatrix} = D \cdot \begin{pmatrix} x_{n+1} \\ \vdots \\ x_{n+\delta} \end{pmatrix} + \alpha_2 = \begin{pmatrix} D[1][1]x_{n+1} \\ \vdots \\ D[\delta][\delta]x_{n+\delta} \end{pmatrix} + \alpha_2 \right.$$

$$\left\{ \begin{pmatrix} h_{n-\delta+1} \\ \vdots \\ h_n \end{pmatrix} = \begin{pmatrix} x_{n-\delta+1} \\ \vdots \\ x_n \end{pmatrix} + \alpha_2 \right.$$

Steps of Recovering Matrix D

- Let $x_1 = x_2 = \cdots = x_n = 0$ and $x_{n+2} = x_{n+3} = \cdots = x_{n+\delta} = 0$ in $\bar{P}^-$, then we get

$$\bar{P}^-(x_{n+1}) = T^- \circ F \circ U \circ L(\overbrace{0, \cdots, 0}^{n}, x_{n+1}, \overbrace{0, \cdots, 0}^{\delta-1})^T.$$

  Taking x_{n+1} over the finite field $\mathbb{F}_q$ and storing all results of the function $\bar{P}^-(x_{n+1})$.

- Let $x_1 = x_2 = \cdots = x_{n-\delta} = 0$ and $x_{n-\delta+2} = x_{n-\delta+3} = \cdots = x_{n+\delta} = 0$ in $\bar{P}^-_{L'}$, then

$$\bar{P}^-_{L'}(x_{n-\delta+1}) = T^- \circ F \circ U \circ L'(\overbrace{0, \cdots 0}^{n-\delta}, x_{n-\delta+1}, \overbrace{0, \cdots, 0}^{\delta-1})^T.$$

Steps of Recovering Matrix D (cont.)

- Taking $x_{n-\delta+1}$ over the finite field $\mathbb{F}_q$ and comparing the results of $\bar{P}^-_{L'}(x_{n-\delta+1})$ to the results of the function $\bar{P}^-(x_{n+1})$, if there were x'_{n+1} and $x'_{n-\delta+1}$ satisfied $\bar{P}^-(x_{n+1}) = P^-_{L'}(x_{n-\delta+1})$, then we have $D[1][1]x'_{n+1} = x'_{n-\delta+1}$, namely, $D[1][1] = {x'_{n+1}}^{-1}x'_{n-\delta+1}$.
- Similarly, we can get the values of $D[2][2], \cdots, D[\delta][\delta]$.

Steps of the Whole Attack

- Firstly, we derived the function $\bar{P}^{-}_{L'} = T^{-} \circ F \circ U \circ L'$ by setting all terms which contained $x_{n+i}(1 \leq i \leq \delta)$ equal to zero in the public key $\bar{P}^{-}$.
- Recovering the value of matrix D following by the proposition 3.
- Given a message $y' = (y'_1, \cdots, y'_{n-\mu})$, forging a valid signature of $\bar{P}^{-}_{L'}$ using the algorithm $\mathcal{A}$.
- Deriving a valid signature corresponding to the message y' of HTTM according to the proposition 2.

Practical Cryptanalysis of HTTM^{V_1}

- The central map:

$$Y = \hat{F}(X) = X^{1+q^{\theta}}.$$

- Parameter: $q = 2$, $n = 31$, $k = 6$, $\delta = 10$, $\mu = 5$, $\theta = 11$.
- Hash function: SHA-1.
- Key point: MI^{-} can be forged a valid signature by differential method.

Conclusion

- The HT transformation can not enhanced the security of the original MPKC
- If there were an algorithm that can forge a valid signature for the original MPKC, there would be an algorithm working on the HTTM.
- Although the EMC method did not work, it is an interesting method which is worth further studying.

The End

Thanks! Questions?