A New Attack on the LUOV Schemes

Jintai Ding, Zheng Zhang, Joshua Deaton, Kurt Schmidt, Vishakha FNU

University of Cincinnati

jintai.ding@gmail.com

The 2nd NIST PQC workshop, Aug. 23, 2019

Overview

Multivariate Signature schemes

- **Public key**: $\mathcal{P}(x_1, \cdots, x_n) = (p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n))$. Here p_i are multivariate polynomials over a finite field.
- **Private key** A way to compute $\mathcal{P}^{-1}$.
- **Signing a hash of a document:** $(x_1, \cdots, x_n) \in \mathcal{P}^{-1}(y_1, \cdots, y_m)$.
- **Verifying:** $(y_1, \cdots, y_m) \stackrel{?}{=} \mathcal{P}(x_1, \cdots, x_n)$

Theoretical Foundation

- Direct attack is to solve the set of equations:

$$G(M) = G(x_1, ..., x_n) = (y'_1, ..., y'_m).$$

Theoretical Foundation

- Direct attack is to solve the set of equations:

$$G(M) = G(x_1, ..., x_n) = (y'_1, ..., y'_m).$$

- *- Solving a set of n randomly chosen equations (nonlinear) with n variables is NP-hard, though this does not necessarily ensure the security of the systems.*

Quadratic Constructions

- *1) Efficiency considerations lead to mainly quadratic constructions.*

$$G_l(x_1, ..x_n) = \sum_{i,j} \alpha_{lij} x_i x_j + \sum_i \beta_{li} x_i + \gamma_l.$$

- *2) Mathematical structure consideration: Any set of high degree polynomial equations can be reduced to a set of quadratic equations.*

$$x_1 x_2 x_3 = 5,$$

is equivalent to

$$\begin{aligned} x_1 x_2 - y &= 0 \\ y x_3 &= 5. \end{aligned}$$

The view from the history of Mathematics(Diffie in Paris)

- RSA – Number Theory – 18th century mathematics
- ECC – Theory of Elliptic Curves – 19th century mathematics
- Multivariate Public key cryptosystem – Algebraic Geometry – 20th century mathematics
  Algebraic Geometry – Theory of Polynomial Rings

Oil Vinegar Signature Scheme

- Introduced by J. Patarin, 1997
- Inspired by linearization attack to Matsumoto-Imai cryptosystem
- $\mathcal{P} = \mathcal{F} \circ \mathcal{T}$.
  $\mathcal{F}$: nonlinear, easy to compute $\mathcal{F}^{-1}$.
  $\mathcal{T}$: invertible linear, to **hide** the structure of $\mathcal{F}$.

Oil Vinegar Signature Scheme

- $\mathcal{F} = (f_1(x_1, \cdots, x_0, x'_1, \cdots, x'_v), \cdots, f_o(x_1, \cdots, x_0, x'_1, \cdots, x'_v))$.
- $f_k = \sum a_{i,j,k} x_i x'_j + \sum b_{i,j,k} x'_i x'_j + \sum c_{i,k} x_i + \sum d_{i,k} x'_i + e_k$
- Oil variables: $x_1, \cdots, x_o$

  Vinegar variables: $x'_1, \cdots, x'_v$.
- **Public Key:** $\mathcal{P} = \mathcal{F} \circ \mathcal{T}$.
  Private Key: $\mathcal{T}$.

How to find $\mathcal{F}^{-1}$

- Fix values for vinegar variables $x'_1, \cdots, x'_v$.
- $f_k = \sum a_{i,j,k} x_i x'_j + \sum b_{i,j,k} x'_i x'_j + \sum c_{i,k} x_i + \sum d_{i,k} x'_i + e_k$
- $\mathcal{F}$: Linear system in oil variables $x_1, \cdots, x_o$.

Broken Parameters

- $v = o$
  Defeated by Kipnis and Shamir using invariant subspace (1998).
- $v < o$
  by guessing some variables will be most likely turn into a OV system where $v = o$
- $v >> o$
  Finding a solution is generally easy

Usable Parameters

- $v = 2o, 3o$
  Direct attack does not work – the complexity is the same as if solving a random system!
- Beyond a direct attack, there is the reconciliation attack which uses the structure of OV systems. Looks for equivalent maps of a special form. Complexity becomes that of solving a system of o quadratic equations in v variables.
- Less efficient
  Signature is at least twice the size of the document

- Rainbow, J. Ding, D. Schmidt (2005)
  Multilayer version of UOV.
  Reduces number of variables in the public key
  smaller key sizes
  smaller signatures
- Rainbow is a NIST round 2 candidate.

LUOV

- Newly Designed by Ward Beullens, Bart Preneel, Alan Szepieniec, and Frederik Vercauteren from imec-COSIC KU Leuven in 2017.
- A modification of the original unbalanced oilvinegar scheme
- Coefficients of the public key are from $\mathbb{F}_2$
- Shorten the size of the public key.

LUOV

Let $\mathbb{F}_{2^r}$ be the extension of $\mathbb{F}_2$ of degree r, $v > o$ and $n = v + o$.

- Central map: $\mathcal{F} : \mathbb{F}_{2^r}^n \to \mathbb{F}_{2^r}^o$
- $f_k(\mathbf{x}) = \sum_{i=1}^{v} \sum_{j=i}^{n} \alpha_{i,j,k} x_i x_j + \sum_{i=1}^{n} \beta_{i,k} x_i + \gamma_k$.

  where $\alpha_{i,j,k}, \beta_{i,j,k}, \gamma_k$ are from $\mathbb{F}_2$.
- Choose $\mathcal{T}$:

$$\begin{bmatrix} \mathbf{1}_v & \mathbf{T} \\ \mathbf{0} & \mathbf{1}_o \end{bmatrix}$$

  where $\mathbf{T}$ is a $v \times o$ matrix whose entries are also from the small field $\mathbb{F}_2$

Representation of Finite Fields

- Base field: $\mathbb{F}_2$,
- Extension field: $\mathbb{F}_{2^r}$
- Small subfield: $\mathbb{F}_{2^d}$, where $d|r$.
- $\mathbb{F}_{2^r} \cong \mathbb{F}_{2^d}[t]/f(t)$, where $f(t)$ is an irreducible polynomial of degree r/d.
- Elements in $\mathbb{F}_{2^r}$ can be represented by $\sum_{i=0}^{r/d-1} a_i t^i$, where a_i are from $\mathbb{F}_{2^d}$.

The Differential

Differential:

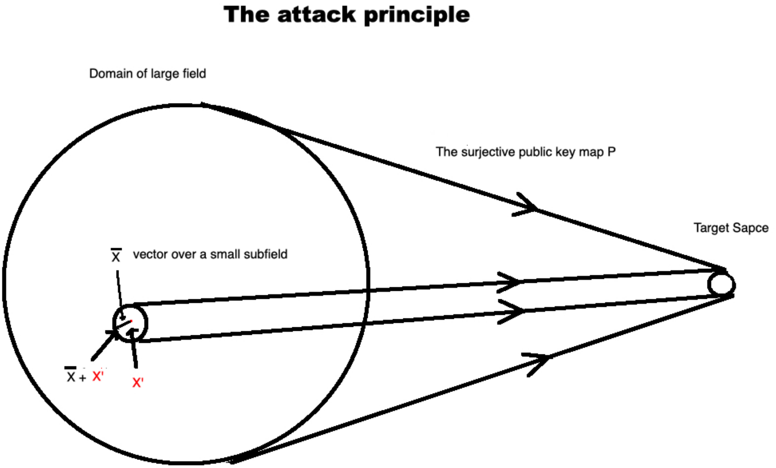
$$\mathbf{x}' + \bar{\mathbf{x}} \in \mathbb{F}_{2^r}^n$$

where we randomly fix $\mathbf{x}' \in \mathbb{F}_{2^r}^n$ and we let $\bar{\mathbf{x}} \in \mathbb{F}_{2^d}^n$ vary.

Probability of Successful Attack

Given: $\mathbf{y} = (y_1, \cdots, y_o) \in \mathbb{F}_{2^r}^o$ and choose an arbitrary $\mathbf{x}' \in \mathbb{F}_{2^r}^n$.
Question: Does there exist a reasonable small integer d such that there will also exist a $\bar{\mathbf{x}} \in \mathbb{F}_{2^d}^n \subset \mathbb{F}_{2^r}^n$ where $P(\mathbf{x}' + \bar{\mathbf{x}}) = \mathbf{y}$?

The attack principle



Probability of Successful Attack

- Given $\mathbf{y} \in \mathbb{F}_{2^r}^{o}$
- Choose $\mathbf{x'} \in \mathbb{F}_{2^d}^{n}$.
- $\mathcal{P}' : \mathbb{F}_{2^d}^{n} \to \mathbb{F}_{2^r}^{o}$ given by $\mathcal{P}'(\bar{\mathbf{x}}) = \mathcal{P}(\mathbf{x'} + \bar{\mathbf{x}})$
- Assume that $\mathcal{P}'$ acts as a random map from $\mathbb{F}_{2^d}^{n} \to \mathbb{F}_{2^r}^{o}$.

Probability of Successful Attack

- $|\mathbb{F}_{2^d}^n| = 2^{d \cdot n}$
- $|\mathbb{F}_{2^r}^o| = 2^{r \cdot o}$
- The probability that $\mathcal{P}'(\bar{\mathbf{x}}) \neq \mathbf{y}$ is $1 - \frac{1}{2^{r \cdot o}}$.

Probability of Successful Attack

- The outputs of $\mathcal{P}'$ are independent
- Exhausting every element of $\mathbb{F}_{2^d}^n$
- Estimated our desired probability as

$$\left(1-\frac{1}{2^{r\cdot o}}\right)^{2^{d\cdot n}} = \left(\left(1-\frac{1}{2^{r\cdot o}}\right)^{2^{r\cdot o}}\right)^{2^{(d\cdot n)-(r\cdot o)}} \approx e^{-2^{(d\cdot n)-(r\cdot o)}},$$

because $\lim_{n\to\infty}(1-\frac{1}{n})^n = e^{-1}$.

Estimated Probabilities for the LUOV Parameters Submitted

Security Level	r	o	v	n	d	Probability of Failure
II	8	58	237	295	2	$\exp(-2^{126})$
IV	8	82	323	405	2	$\exp(-2^{154})$
V	8	107	371	478	2	$\exp(-2^{100})$

Table: Estimated Probabilities of Failure for Parameters Designed to Minimize the Size of the Signature

Security Level	r	o	v	n	d	Probability of Failure
II	48	43	222	265	8	$\exp(-2^{56})$
IV	64	61	302	363	16	$\exp(-2^{1904})$
V	80	76	363	439	16	$\exp(-2^{944})$

Table: Estimated Probabilities of Failure for Parameters Designed to Minimize the Size of the Signature and Public Key

The Form of $P(x' + \bar{x})$ I

- kth component of $\mathcal{P}(\mathbf{x}' + \bar{\mathbf{x}})$

$$\tilde{f}_k(\mathbf{x}' + \bar{\mathbf{x}}) = \sum_{i=1}^{n} \sum_{j=i}^{n} \alpha_{i,j,k}(x'_i + \bar{x}_i)(x'_j + \bar{x}_j) + \sum_{i=1}^{n} \beta_{i,k}(x'_i + \bar{x}_i) + \gamma_k = y_k$$

Where $\alpha_{i,j,k}, \beta_{i,k}, \gamma_k \in \mathbb{F}_2$ and $x'_i \in \mathbb{F}_{2^r}$.

The Form of $P(x' + \bar{x})$ II

$$\tilde{f}_k(\mathbf{x}' + \bar{\mathbf{x}}) = \sum_{i=1}^{n}\sum_{j=i}^{n}\alpha_{i,j,k}(x_i'x_j' + x_i'\bar{x}_i + x_j'\bar{x}_j) + \sum_{i=1}^{n}\beta_{i,k}(x_i' + \bar{x}_i) + \gamma_k$$

$$+ \sum_{i=1}^{v}\sum_{j=i}^{n}\alpha_{i,j,k}\bar{x}_i\bar{x}_j$$

$$= y_k$$

The quadratic terms have coefficients $\alpha_{i,j,k}$, which can only be 0 or 1.

The Form of $P(x' + \bar{x})$ III

- We view these over $\mathbb{F}_{2^d}[t]/f(t)$
- So if $\frac{r}{d} = s$, $x'_i = a_{s-1}t^{s-1} + \cdots + a_0$.
- Regroup the above equations of $\tilde{f}_k = y_k$ in terms of the powers of t.
- This means that the coefficient of $t^i, i = 1 \cdots, s-1$ is a linear polynomial of the $\bar{x}_i$.

$P(x' + \bar{x})$

We have that

$$\tilde{f}_k(\mathbf{x}' + \bar{\mathbf{x}}) = \sum_{i=1}^{s-1} g_{i,k}(\bar{x}_1, \cdots, \bar{x}_n)t^i + Q_k(\bar{x}_1, \cdots, \bar{x}_n) = y_k = \sum_{i=0}^{s-1} w_{i,k}t^i.$$

for some $w_{i,k} \in \mathbb{F}_{2^d}$, some linear polynomials $g_{i,k}(\bar{x}_1, \cdots, \bar{x}_n) \in \mathbb{F}_{2^d}[\bar{x}_1, \cdots, \bar{x}_n]$, and some quadratic polynomial $Q_k(\bar{x}_1, \cdots, \bar{x}_n) \in \mathbb{F}_{2^d}[\bar{x}_1, \cdots, \bar{x}_n]$

How We Use This

- Each $\tilde{f}_k$ has $s-1$ linear equations $g_{i,k}(\bar{x}_1,\cdots,\bar{x}_n)=w_{i,k}$, one for each power of t.
- $(s-1)o$ linear equations with n variables.
- This can be represented by $\mathbf{Ax}=\mathbf{y}$.
- Our desired $\bar{\mathbf{x}}$ is in the solution space.

How we use this

- Each $\tilde{f}_k$ will have an additional quadratic polynomial equation Q_k which must also be satisfied.
  $Q_k(\bar{x}_1, \cdots, \bar{x}_n) = w_{0,k}$
- Each of these equations is over the small field $\mathbb{F}_{2^d}$.

Solution Space

- As the $(s-1)o$ linear equations to solve with n variables and these linear polynomials are essentially random and thus likely linearly independent, we have a solution space around the size of $n - \text{rank}(A) = n - (s-1)o$.
- We just need one an element from here that also satisfies the quadratic polynomials.

Algorithms

- If we have more variables than equations, we use the method of Thomae and Wolf: *"Solving underdetermined systems of multivariate quadratic equations revisited".*
- System of o equations, $n - (s-1)o$ variables reduced to System of m equations m variables
  $m = o - \left\lfloor \frac{n-(s-1)o}{o} \right\rfloor$.

Algorithms

- Guess for a certain number of the variables.
- Use algorithm XL with Wiedemann.

Degree of Regularity

- Use **Theorem 2** from *"Theoretical Analysis of XL over Small Fields"* by *Bo-yin Yang et al*.
- For a system of m equations with n variables over $\mathbb{F}_q$, the degree of regularity is
  $D_{reg} = \min\{D : [t^D]((1-t)^{-n-1}(1-t^q)^n(1-t^2)^m(1-t^{2q})^{-m})) \leq 0\}$
  $[u]p$ denotes the coefficient of term in the expansion of p.
  E.g. $[x^2](1+x)^4 = 6$.

Complexity

- Use **Proposition 3.4** from *"Analysis of QUAD"* Bo-yin Yang *et al*.
- Expected running time of XL is roughly: $C_{XL} \sim 3T^2\tau$
- $T = \binom{n+D_{reg}}{D_{reg}}$
- τ is number of terms in an equation.

Toy Example I

We will give a small toy example with the following parameters: $o = 2, v = 8, n = 10, r = 8, d = 2$.
Here we will represent $\mathbb{F}_{2^2}$ by the elements $\{0, 1, w_1, w_2\}$.
We note that

$$\mathbb{F}_{2^8} \cong \mathbb{F}_{2^2}[t]/f(t)$$

where $f(t) = t^4 + t^2 + w_1 t + 1$.

Toy Example II

Consider the LUOV public key $\mathcal{P} : \mathbb{F}_{2^8}^n \to \mathbb{F}_{2^8}^o$ which for simplicity sake will be homogeneous of degree two:

$$
\begin{aligned}
\tilde{f}_1(\mathbf{x}) =& x_1x_4 + x_1x_5 + x_1x_6 + x_1x_7 + x_1x_8 + x_1x_9 + x_2x_4 + x_2x_6 + x_2x_9 \\
&+ x_3^2 + x_3x_6 + x_3x_7 + x_3x_{10} + x_4^2 + x_4x_7 + x_4x_8 + x_4x_9 + x_4x_{10} \\
&+ x_5x_6 + x_6x_{10} + x_7^2 + x_7x_8 + x_7x_9 + x_8x_9 + x_8x_{10} + x_9^2 + x_9x_{10} \\
\tilde{f}_2(\mathbf{x}) =& x_1x_3 + x_1x_4 + x_1x_5 + x_1x_9 + x_2x_3 + x_2x_6 + x_2x_7 + x_2x_9 + x_3^2 + x_3x_4 \\
&+ x_3x_5 + x_3x_6 + x_3x_7 + x_3x_9 + x_4^2 + x_4x_5 + x_4x_6 + x_4x_7 + x_4x_{10} \\
&+ x_5^2 + x_5x_6 + x_5x_7 + x_5x_8 + x_5x_{10} + x_6x_7 + x_7x_9 + x_9x_{10} + x_{10}^2
\end{aligned}
$$

Toy Example III

We will attempt to find a signature for the message:

$$\mathbf{y} = \begin{bmatrix} w_1 t^3 + w_2 t^2 + w_2 t \\ w_2 t^3 + w_2 t^2 + t \end{bmatrix}$$

First we randomly select our $\mathbf{x}'$ as

$$\mathbf{x}' = \begin{bmatrix} t^3 + w_2 t \\ w_1 t^3 + w_2 t^2 + w_2 t \\ t^3 + t + 1 \\ w_2 t^2 + w_1 \\ t^3 + t^2 + 1 \\ w_2 t^3 + t^2 + w_2 t + w_2 \\ w_1 t^3 + w_2 t + w \\ w_1 t^2 + w_2 t + 1 \\ t^3 + w_2 t + w_1 \\ w_2 t + w_2 \end{bmatrix}$$

Toy Example IV

Next we compute $\mathcal{P}(\mathbf{x}' + \bar{\mathbf{x}}) =$

$$
\begin{aligned}
&[(\bar{x}_1 + w_1\bar{x}_2 + \bar{x}_3 + w_1\bar{x}_5 + w_2\bar{x}_6 + \bar{x}_7 + w_1\bar{x}_8 + \bar{x}_9 + w_2\bar{x}_{10})t^3 \\
&\;+ (\bar{x}_1 + w_1\bar{x}_2 + \bar{x}_3 + \bar{x}_4 + \bar{x}_5 + w_1\bar{x}_6 + \bar{x}_7 + w_2\bar{x}_8 + w_1\bar{x}_9)t^2 \\
&\;+ (w_2\bar{x}_3 + w_1\bar{x}_6 + w_1\bar{x}_7 + w_2\bar{x}_9 + w_1\bar{x}_{10})t \\
&\;+ Q_1(\bar{x}_1, \cdots, \bar{x}_n), \\
&(\bar{x}_1 + \bar{x}_2 + w_1\bar{x}_3 + \bar{x}_5 + \bar{x}_8)t^3 \\
&\;+ (w_1\bar{x}_1 + \bar{x}_2 + \bar{x}_6 + \bar{x}_8 + w_2\bar{x}_9 + w_1\bar{x}_{10})t^2 \\
&\;+ (w_1\bar{x}_1 + w_1\bar{x}_2 + w_2\bar{x}_3 + \bar{x}_4 + w_1\bar{x}_5 + \bar{x}_6 + w_1\bar{x}_7 + \bar{x}_9 + w_2\bar{x}_{10})t \\
&\;+ Q_2(\bar{x}_1, \cdots, \bar{x}_n)]
\end{aligned}
$$

Toy Example V

The linear part forms the matrix equation:

$$\begin{bmatrix} 1 & w_1 & 1 & 0 & w_1 & w_2 & 1 & w_1 & 1 & w_2 \\ 1 & w_1 & 1 & 1 & 1 & w_1 & 1 & w_2 & w_1 & 0 \\ 0 & 0 & w_2 & 0 & 0 & w_1 & w_1 & 0 & w_2 & w_1 \\ 1 & 1 & w_1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ w_1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & w_2 & w_1 \\ w_1 & w_1 & w_2 & 1 & w_1 & 1 & w_1 & 0 & 1 & w_2 \end{bmatrix} \begin{bmatrix} \bar{x}_1 \\ \bar{x}_2 \\ \bar{x}_3 \\ \bar{x}_4 \\ \bar{x}_5 \\ \bar{x}_6 \\ \bar{x}_7 \\ \bar{x}_8 \\ \bar{x}_9 \\ \bar{x}_{10} \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \\ w_2 \\ w_2 \\ w_2 \\ 1 \end{bmatrix}$$

Toy Example VI

Since the solution space is small (dim 4), by quick search we find signature

$$\sigma = \begin{bmatrix} t^3 + w_2 t + 1 \\ w_1 t^3 + w_2 t^2 + w_2 t + w_1 \\ t^3 + t + w_2 \\ w_2 t^2 \\ t^3 + t^2 + 1 \\ w_2 t^3 + t^2 + w_2 t + 1 \\ w_1 t^3 + w_2 t + w_1 \\ w_1 t^2 + w_2 t + 1 \\ t^3 + w_2 t + 1 \\ w_2 t \end{bmatrix}$$

Some Experimental Results

- In order to make sure that finding a signature like above was not a fluke, we ran an experiment of creating a public key with parameters $r = 8, o = 5, v = 20, n = 25, d = 2$. Generating 10,000 random documents, we were able to find using the method from the toy example a signature for every document.
- And in order to show that we achieve the expected $(s-1)o$ equations, we ran an experiment for the given parameters for level II security $r = 8, o = 58, v = 237, n = 295$. We were successful.

Computing Attack's Complexity

- In the following slides we will compute the complexity of SDA against the various parameters of LUOV.
- We will also give the NIST complexity requirement for classical attacks (not quantum).
- We will show the number of equation and variables before applying the method of Thomae and Wolf, and those after applying the method.
- Then the number of variables guessed in the XL algorithm as well as the degree of regularity.

Level II Parameter Choice

NIST Classical Security Complexity Requirement 2^{146}

- $r = 8, o = 58, v = 237, n = 295$
  Claimed Classical Security 2^{146}

Finite Field	Original eq $\times$ var	New eq $\times$ var	Variables Guessed	Degree of Regularity
$\mathbb{F}_{2^2}$	58×121	56×56	24	7

- Complexity of Attack: 2^{107}

- $r = 48, o = 43, v = 222, n = 265$
  Claimed Classical Security 2^{147}

Finite Field	Original eq $\times$ var	New eq $\times$ var	Variables Guessed	Degree of Regularity
$\mathbb{F}_{2^8}$	43×50	42×42	3	19

- Complexity of Attack: 2^{135}

Level IV Parameter Choice

NIST Classical Security Complexity Requirement 2^{210}

- $r = 8, o = 82, v = 323, n = 405$
  Claimed Classical Security 2^{212}

Finite Field	Original eq $\times$ var	New eq $\times$ var	Variables Guessed	Degree of Regularity
$\mathbb{F}_{2^2}$	82×159	81×81	37	8

- Complexity of Attack: $2^{144.5}$

- $r = 64, o = 61, v = 302, n = 363$
  Claimed Classical Security 2^{214}

Finite Field	Original eq $\times$ var	New eq $\times$ var	Variables Guessed	Degree of Regularity
$\mathbb{F}_{2^{16}}$	61×180	59×59	2	31

- Complexity of Attack: 2^{202}

Level V Parameter Choice

NIST Classical Security Complexity Requirement 2^{272}

- $r = 8, o = 107, v = 371, n = 478$
  Claimed Classical Security 2^{273}

Finite Field	Original eq $\times$ var	New eq $\times$ var	Variables Guessed	Degree of Regularity
$\mathbb{F}_{2^2}$	107×157	106×106	51	9

- Complexity of Attack: 2^{184}

- $r = 80, o = 76, v = 363, n = 439$
  Claimed Classical Security 2^{273}

Finite Field	Original eq $\times$ var	New eq $\times$ var	Variables Guessed	Degree of Regularity
$\mathbb{F}_{2^{16}}$	76×131	75×75	2	38

- Complexity of Attack: 2^{244}

Summarizing

- All LUOV schemes fail to meet the security level requirements.
- Level II schemes do not satisfy Level I requirement.
- The largest gap of security estimate is 89 bits.

Inapplicable on UOV

- UOV Public Key: $\mathcal{P} : \mathbb{F}_{2^r}^n \to \mathbb{F}_{2^r}^o$
- kth component of $\mathcal{P}$:
  $$\bar{f}_k(\mathbf{x}) = \sum_{i=1}^{v} \sum_{j=i}^{n} \alpha_{i,j,k} x_i x_j + \sum_{i=1}^{n} \beta_{i,k} x_i + \gamma_k.$$
- $\alpha_{i,j,k}, \beta_{i,k}$ and γ_k are randomly chosen from $\mathbb{F}_{2^r}$

Inapplicable on UOV

- Differential: $\mathbf{x}' + \bar{\mathbf{x}}$ with $\mathbf{x}' \in \mathbb{F}_{2^r}$ and $\bar{\mathbf{x}} \in \mathbb{F}_{2^d}$
- kth component of $\mathcal{P}$

$$\bar{f}_k(\mathbf{x}' + \bar{\mathbf{x}}) = \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{i,j,k}(x'_i + \bar{x}_i)(x'_j + \bar{x}_j) + \sum_{i=1}^{n} \beta_{i,k}(x'_i + + \bar{x}_i) + \gamma_k$$

$$= \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{i,j,k}(x'_i x'_j + x'_i \bar{x}_i + x'_j \bar{x}_j) + \sum_{i=1}^{n} \beta_{i,k}(x'_i + \bar{x}_i) + \gamma_k$$

$$+ \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{i,j,k}\bar{x}_i\bar{x}_j = y_k$$

Inapplicable on UOV

- $\alpha_{i,j,k}, \beta_{i,k}$ and γ_k can also be represented by a polynomial in $\mathbb{F}_{2^d}[t]/f(t)$
- multiplication from $\alpha_{i,j,k}, \beta_{i,k}$ and γ_k in $\bar{f}_k$ will mix the degrees of the polynomial expression of $\bar{x}_i$'s in $\mathbb{F}_{2^d}[t]/f(t)$
- Comparing the coefficients of all degrees of t is useless.

Conclusion

We have seen that though LUOV is an interesting development of UOV, its newness hides its flaws. In particular

- There is a near certainty that the differential attack can be successful with a small enough subfield $\mathbb{F}_{2^d}$
- That this gives us many linear equations over this small subfield which can be used to solve for a signature
- The complexity of doing such is lower (sometime MUCH LOWER) than the NIST security levels for each proposed category.
- We are developing new interesting and promising attacks using different subset.

Thanks and Any Questions?

-
Supported by Taft Fund, NIST and NSF
-