Cryptanalysis of multivariate signatures: Singula points of UOV and VOX

Pierre Pébereau
Sorbonne Université, LIP6, CNRS, Thales SIX

March, 2024
## NIST Post-quantum competition

- First NIST post-quantum standards: 2022
  - 2 lattice-based signatures (Dilithium, Falcon)
  - a hash-based signature (SPHINCS+)

Our approach

Study UOV to derive results on schemes related to UOV.
NIST Post-quantum competition

- First NIST post-quantum standards: 2022
  - 2 lattice-based signatures (Dilithium, Falcon)
  - A hash-based signature (SPHINCS+)
- Additional signature round targeting efficiency
  - 11 among 40 based on multivariate polynomial systems
  - 7 among 11 multivariate schemes are based on UOV
NIST Post-quantum competition

- First NIST post-quantum standards: 2022
  - 2 lattice-based signatures (Dilithium, Falcon)
  - a hash-based signature (SPHINCS+)
- Additional signature round targeting efficiency
  - 11 among 40 based on multivariate polynomial systems
  - 7 among 11 multivariate schemes are based on UOV

Our approach

Study UOV to derive results on schemes related to UOV.
### Multivariate Quadratic Problem - MQ($n, m, q$)

Find a solution (if any) $x \in \mathbb{F}_q^n$ to a system of $m$ quadratic equations in $n$ variables

$$\mathcal{P}(x) = 0 \in \mathbb{F}_q^m$$
Multivariate Quadratic Problem - MQ($n, m, q$)

Find a solution (if any) $x \in \mathbb{F}_q^n$ to a system of $m$ quadratic equations in $n$ variables

\[ P(x) = 0 \in \mathbb{F}_q^m \]

Multivariate Quadratic Cryptography

A multivariate signature scheme is defined by a key pair $(P, S)$:
Multivariate Quadratic Problem - MQ\((n, m, q)\)

Find a solution (if any) \(x \in \mathbb{F}_q^n\) to a system of \(m\) quadratic equations in \(n\) variables

\[
\mathcal{P}(x) = 0 \in \mathbb{F}_q^m
\]

Multivariate Quadratic Cryptography

A multivariate signature scheme is defined by a key pair \((\mathcal{P}, S)\):

- The public key \(\mathcal{P}\) is an instance of MQ\((n, m, q)\), \(n > m\).
Multivariate Quadratic Problem - MQ\((n, m, q)\)

Find a solution (if any) \(x \in \mathbb{F}_q^n\) to a system of \(m\) quadratic equations in \(n\) variables

\[
P(x) = 0 \in \mathbb{F}_q^m
\]

Multivariate Quadratic Cryptography

A multivariate signature scheme is defined by a key pair \((P, S)\):

- The public key \(P\) is an instance of MQ\((n, m, q)\), \(n > m\).
- The secret key \(S\) enables, for all \(t \in \mathbb{F}_q^m\), to efficiently find \(x \in \mathbb{F}_q^n\) s.t. \(P(x) = t\)
### Unbalanced Oil and Vinegar [Kipnis, Patarin, Goubin, 1999]

| Secret key: | - $m$ quadratic polynomials $x^T F_i x \in \mathbb{F}_q[x_1, \ldots, x_n]$  
|            | linear in $x_1, \ldots, x_m$.  
|            | - invertible change of variables $A$. |

---

**Figure 1:** UOV key pair in $\mathbb{F}_{257}$
# Unbalanced Oil and Vinegar [Kipnis, Patarin, Goubin, 1999]

**Secret key:** - $m$ quadratic polynomials $x^T F_i x \in \mathbb{F}_q[x_1, \ldots, x_n]$  
  - linear in $x_1, \ldots, x_m$.
  - invertible change of variables $A$.

**Public key:** $m$ quadratic polynomials $x^T P_i x$.  
\[ P = \mathcal{F} \circ A = (A^T F_1 A, \ldots, A^T F_m A) \]

---

**Figure 1:** UOV key pair in $\mathbb{F}_{257}$
**Unbalanced Oil and Vinegar [Kipnis, Patarin, Goubin, 1999]**

**Secret key:** - $m$ quadratic polynomials $\mathbf{x}^T F_i \mathbf{x} \in \mathbb{F}_q[x_1, \ldots, x_n]$  
  - linear in $x_1, \ldots, x_m$.
- invertible change of variables $A$.

**Public key:** $m$ quadratic polynomials $\mathbf{x}^T P_i \mathbf{x}$.

$$\mathcal{P} = \mathcal{F} \circ A = (A^T F_1 A, \ldots, A^T F_m A)$$

---

**Naming conventions and parameters**

With $I = \langle p_1(x), \ldots, p_m(x) \rangle$, define the UOV variety:

$$V(I) = \{ \mathbf{x} \in \mathbb{F}_q^m, \mathcal{P}(\mathbf{x}) = 0 \}$$
Unbalanced Oil and Vinegar [Kipnis, Patarin, Goubin, 1999]

Secret key: - $m$ quadratic polynomials $\mathbf{x}^T F_i \mathbf{x} \in \mathbb{F}_q[x_1, \ldots, x_n]$

  - linear in $x_1, \ldots, x_m$.

  - invertible change of variables $A$.

Public key: $m$ quadratic polynomials $\mathbf{x}^T P_i \mathbf{x}$.

$$\mathcal{P} = \mathcal{F} \circ A = (A^T F_1 A, \ldots, A^T F_m A)$$

Naming conventions and parameters

With $I = \langle p_1(x), \ldots, p_m(x) \rangle$, define the UOV variety:

$$V(I) = \{ \mathbf{x} \in \mathbb{F}^m_q, \mathcal{P}(\mathbf{x}) = 0 \}$$

$\mathbf{x} \in \mathbb{F}^n_q$ is a signature for message $t \in \mathbb{F}_q^m$ if $\mathcal{P}(\mathbf{x}) = t$. 
Characterisation of the secret key [Kipnis, Shamir 1998]

<table>
<thead>
<tr>
<th>Trapdoor: linear subspace ( \mathcal{O} \subset \mathbb{F}_q^n ) of dimension ( m ) such that</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{O} \subset V(I) )</td>
</tr>
</tbody>
</table>

Observation: The first \( m \) columns of the secret matrix \( A^{-1} \) form a basis of \( \mathcal{O} \).
Characterisation of the secret key  

[Kipnis, Shamir 1998]

Trapdoor: linear subspace $O \subset \mathbb{F}_q^n$ of dimension $m$ such that

$$O \subset V(I)$$

<table>
<thead>
<tr>
<th>Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The first $m$ columns of the secret matrix $A^{-1}$ form a basis of $O$.</td>
</tr>
</tbody>
</table>
Characterisation of the secret key [Kipnis, Shamir 1998]

Trapdoor: linear subspace $\mathcal{O} \subset \mathbb{F}_q^n$ of dimension $m$ such that

$$\mathcal{O} \subset V(I)$$

Observation

The first $m$ columns of the secret matrix $A^{-1}$ form a basis of $\mathcal{O}$.

Cryptanalysis: Key recovery

Find a basis of $\mathcal{O}$ with less than $2^\lambda$ logical gates.
Characterisation of the secret key \[ [\text{Kipnis, Shamir 1998}] \]

Trapdoor: linear subspace \( \mathcal{O} \subset \mathbb{F}^n_q \) of dimension \( m \) such that

\[
\mathcal{O} \subset V(I)
\]

Observation

The first \( m \) columns of the secret matrix \( A^{-1} \) form a basis of \( \mathcal{O} \).

Cryptanalysis: Key recovery

Find a basis of \( \mathcal{O} \) with less than \( 2^\lambda \) logical gates.

<table>
<thead>
<tr>
<th>Security level</th>
<th>I</th>
<th>III</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classical gates</td>
<td>( 2^{143} )</td>
<td>( 2^{207} )</td>
<td>( 2^{272} )</td>
</tr>
</tbody>
</table>
Contributions

One vector to full key recovery in polynomial time [P. 2023]

From one vector in \( \mathcal{O} \), return a basis of \( \mathcal{O} \) in polynomial time.
## Contributions

<table>
<thead>
<tr>
<th>One vector to full key recovery in polynomial time [P. 2023]</th>
</tr>
</thead>
<tbody>
<tr>
<td>From <strong>one vector</strong> in $\mathcal{O}$, return a basis of $\mathcal{O}$ in <strong>polynomial time</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Singular points of UOV and UOV$^\dagger$ [P. 2024]</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Existence and dimension</strong> of singular locus of $V(I)$.</td>
</tr>
</tbody>
</table>
## Contributions

<table>
<thead>
<tr>
<th>One vector to full key recovery in polynomial time [P. 2023]</th>
</tr>
</thead>
<tbody>
<tr>
<td>From <strong>one vector</strong> in $\mathcal{O}$, return a basis of $\mathcal{O}$ in <strong>polynomial time</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Singular points of UOV and UOV$^+$ [P. 2024]</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Existence and dimension</strong> of singular locus of $V(I)$.</td>
</tr>
<tr>
<td>• <strong>Faster</strong> computation of singular points of UOV$^+$.</td>
</tr>
</tbody>
</table>
### Contributions

#### One vector to full key recovery in polynomial time [P. 2023]

From one vector in $\mathcal{O}$, return a basis of $\mathcal{O}$ in polynomial time.

#### Singular points of UOV and UOV$^\hat{+}$ [P. 2024]

- Existence and dimension of singular locus of $V(I)$.
- Faster computation of singular points of UOV$^\hat{+}$.

#### Subfield attack on QR-UOV$^\hat{+}$ [P. 2024]

Identified a weakness in a structured variant of UOV$^\hat{+}$ submitted to the additional NIST call for signature schemes $^1$:

- Broken on a laptop in 0.3s, 1.35s, 0.56s (level I, III, V).

---

$^1$ [Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud, Patarin, 2023]
<table>
<thead>
<tr>
<th>Contributions</th>
</tr>
</thead>
</table>

Singular points of UOV and UOV\(^\dagger\) [P. 2024]

- **Existence** and **dimension** of singular locus of \(V(I)\).
- **Faster** computation of singular points of UOV\(^\dagger\).
Singular points

\[ y^2 = x^3 - 3x + 2 \text{ in } \mathbb{R}^2 \]

\[ x^2 - y^2z^2 + z^3 \text{ in } \mathbb{R}^3 \]

(from [Cox, Little, O’Shea])
Singular points

\[ y^2 = x^3 - 3x + 2 \text{ in } \mathbb{R}^2 \]

Singular point: (1,0)

\[ x^2 - y^2z^2 + z^3 \text{ in } \mathbb{R}^3 \]

(from [Cox, Little, O’Shea])
Singular points

\[ y^2 = x^3 - 3x + 2 \text{ in } \mathbb{R}^2 \]
Singular point: (1,0)

\[ x^2 - y^2z^2 + z^3 \text{ in } \mathbb{R}^3 \]
Singular points: line \((x=z=0)\)
(from [Cox, Little, O’Shea])
Singular points

\[ y^2 = x^3 - 3x + 2 \text{ in } \mathbb{R}^2 \]

Singular point: \((1,0)\)

\[ x^2 - y^2z^2 + z^3 \text{ in } \mathbb{R}^3 \]

Singular points: line \((x=z=0)\)

(from [Cox, Little, O’Shea])

**Definition**

Let \( I = \langle p_1, \ldots, p_m \rangle \) be an ideal of \( \mathbb{K}[x_1, \ldots, x_n] \).

\( x \in V(I) \setminus \{0\} \) is singular if \( \text{Jac}_P(x) \) has rank less than \( n - m \).
Singular points

\[ y^2 = x^3 - 3x + 2 \text{ in } \mathbb{R}^2 \]
Singular point: \((1,0)\)

\[ x^2 - y^2z^2 + z^3 \text{ in } \mathbb{R}^3 \]
Singular points: line \((x=z=0)\)
(from [Cox, Little, O’Shea])

**Definition**

Let \( I = \langle p_1, \ldots, p_m \rangle \) be an ideal of \( \mathbb{K}[x_1, \ldots, x_n] \).
\( x \in V(I) \setminus \{0\} \) is **singular** if \( \text{Jac}_P(x) \) has rank less than \( n - m \).

\[
\text{Jac}_P(x) = \left( \frac{\partial}{\partial x_j} p_i(x) \right) \in \mathbb{K}[x_1, \ldots, x_n]^{m \times n}
\]
Structured equations yield a structured Jacobian

Unbalanced Oil and Vinegar [Kipnis, Patarin, Goubin, 1999]

Secret key $F$: $m$ quadratic equations $x^T F_i x$ linear in $x_1, \ldots, x_m$. 
Structured equations yield a structured Jacobian

Unbalanced Oil and Vinegar [Kipnis, Patarin, Goubin, 1999]

Secret key $\mathcal{F}$: $m$ quadratic equations $x^T F_i x$ linear in $x_1, \ldots, x_m$.

Secret Jacobian

The Jacobian of $\mathcal{F}(x)$ has a special shape:

$$\text{Jac}_{\mathcal{F}}(x) = \begin{bmatrix} J_1 & J_2 \\ 1 \ldots m & m+1 \ldots n \end{bmatrix}$$
Structured equations yield a structured Jacobian

Unbalanced Oil and Vinegar [Kipnis, Patarin, Goubin, 1999]

Secret key $\mathcal{F}$: $m$ quadratic equations $x^T F_i x$ linear in $x_1, \ldots, x_m$.

Secret Jacobian

The Jacobian of $\mathcal{F}(x)$ has a special shape:

$$\text{Jac}_{\mathcal{F}}(x) = \begin{bmatrix} J_1 & J_2 \\ 1 \cdots m & m+1 \cdots n \end{bmatrix}$$

Where $J_1 \in \mathbb{F}_q[x_{m+1}, \ldots, x_n]^{m \times m}$ and $J_2 \in \mathbb{F}_q[x_1, \ldots, x_n]^{m \times n-m}$. 
Singular points leak the trapdoor

Singular points in $\mathcal{O}$

If $x \in \mathcal{O}$, then $x \in V(I)$

Determinantal ideal $\text{Sing}(V(I)) \cap \mathcal{O}$ is defined by a determinantal ideal noted $J_{m-1}$.

$J_{m-1} = \langle \text{MaxMinors}(J^2(x)) \rangle$

Dimension of the singular locus

Under a genericity assumption, $[FSS13]$ yields $\dim (\text{Sing}(V(I)) \cap \mathcal{O}) = 3m - n - 1 > 0$. 

1
Singular points leak the trapdoor

Singular points in \( \mathcal{O} \)

If \( x \in \mathcal{O} \), then \( x \in V(I) \) and

\[
\text{Jac}_F(x) = \begin{bmatrix} 0 & J_2(x) \\ 1 \ldots m & m + 1 \ldots n \end{bmatrix}
\]
Singular points leak the trapdoor

Singular points in $\mathcal{O}$

If $x \in \mathcal{O}$, then $x \in V(I)$ and

\[
\text{Jac}_{\mathcal{F}}(x) = \begin{bmatrix}
0 \\
1 \ldots \ldots \ m \ 
\end{bmatrix} \\
\begin{bmatrix}
m + 1 \ldots \ldots \ n \\
\end{bmatrix} \\
n_{2}(x)
\]

Determinantal ideal

Sing($V(I)$) $\cap \mathcal{O}$ is defined by a determinantal ideal noted $\mathcal{I}_{m-1}$.

$\mathcal{I}_{m-1} = \langle \text{MaxMinors}(J_2(x)) \rangle$
Singular points leak the trapdoor

Singular points in $\mathcal{O}$

If $x \in \mathcal{O}$, then $x \in V(I)$ and

$$\text{Jac}_\mathcal{F}(x) = \begin{bmatrix}
0 \\
1 \ldots \ldots m \\
m + 1 \ldots \ldots n
\end{bmatrix}$$

Determinantal ideal

$\text{Sing}(V(I)) \cap \mathcal{O}$ is defined by a determinantal ideal noted $\mathcal{I}_{m-1}$.

$$\mathcal{I}_{m-1} = \langle \text{MaxMinors}(J_2(x)) \rangle$$

Dimension of the singular locus

Under a genericity assumption, [FSS13]$^1$ yields

$$\dim (\text{Sing}(V(I)) \cap \mathcal{O}) = 3m - n - 1 > 0$$

$^1$Faugère, Safey El Din, Spaenlehauer, 2013, Theorem 10
\( \mathcal{P} \) is the UOV public key: \( m \) quadratic polynomials in \( n \) variables
Computing singular points

\( \mathcal{P} \) is the UOV public key: \( m \) quadratic polynomials in \( n \) variables

Modeling singular points

1. Minors modeling: \( \mathcal{M}(\mathcal{P}) : \)

\[
\begin{align*}
\mathbf{x} & \in \mathbb{F}_q^n \\
\mathcal{P}(\mathbf{x}) & = 0 \\
\text{MaxMinors}(\text{Jac}_{\mathcal{P}}(\mathbf{x})) & = 0
\end{align*}
\]
Computing singular points

\( \mathcal{P} \) is the UOV public key: \( m \) quadratic polynomials in \( n \) variables

### Modeling singular points

1. **Minors modeling**: \( \mathcal{M}(\mathcal{P}) : \quad \begin{cases} 
    x \in \mathbb{F}_q^n \\
    \mathcal{P}(x) = 0 \\
    \text{MaxMinors}(\text{Jac}_\mathcal{P}(x)) = 0
\end{cases} \)
Computing singular points

\( P \) is the UOV public key: \( m \) quadratic polynomials in \( n \) variables

### Modeling singular points

1. Minors modeling: \( \mathcal{M}(P) : \begin{cases} 
  x \in \mathbb{F}_q^n \\
  P(x) = 0 \\
  \text{MaxMinors}(\text{Jac}_P(x)) = 0
\end{cases} \)
Computing singular points

$\mathcal{P}$ is the UOV public key: $m$ quadratic polynomials in $n$ variables

Modeling singular points

1. Minors modeling: $\mathcal{M}(\mathcal{P})$:
   \[
   \begin{cases}
   x \in \mathbb{F}_q^n \\
   \mathcal{P}(x) = 0 \\
   \text{MaxMinors}(\text{Jac}_\mathcal{P}(x)) = 0
   \end{cases}
   \]

2. Bihomogeneous modeling: $\mathcal{B}(\mathcal{P})$:
   \[
   \begin{cases}
   x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\
   \mathcal{P}(x) = 0 \\
   y^T \text{Jac}_\mathcal{P}(x) = 0
   \end{cases}
   \]
Computing singular points

$\mathcal{P}$ is the UOV public key: $m$ quadratic polynomials in $n$ variables

### Modeling singular points

1. **Minors modeling:** $\mathcal{M}(\mathcal{P})$:
   \[
   \begin{cases}
   x \in \mathbb{F}_q^n \\
   \mathcal{P}(x) = 0 \\
   \text{MaxMinors(Jac}_{\mathcal{P}}(x)) = 0
   \end{cases}
   \]

2. **Bihomogeneous modeling:** $\mathcal{B}(\mathcal{P})$:
   \[
   \begin{cases}
   x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\
   \mathcal{P}(x) = 0 \\
   y^T \text{Jac}_{\mathcal{P}}(x) = 0
   \end{cases}
   \]

These systems may be solved with Gröbner bases computations.
Computing singular points

$P$ is the UOV public key: $m$ quadratic polynomials in $n$ variables

Modeling singular points

1. Minors modeling: $\mathcal{M}(P)$:
\[
\begin{align*}
\mathcal{M}(P) : & \quad \{ \mathbf{x} \in \mathbb{F}_q^n \} \\
& \quad \{ \mathcal{P}(\mathbf{x}) = 0 \} \\
& \quad \{ \text{MaxMinors}(\text{Jac}_P(\mathbf{x})) = 0 \}
\end{align*}
\]

2. Bihomogeneous modeling: $\mathcal{B}(P)$:
\[
\begin{align*}
\mathcal{B}(P) : & \quad \{ \mathbf{x} \in \mathbb{F}_q^n, \mathbf{y} \in \mathbb{F}_q^m \} \\
& \quad \{ \mathcal{P}(\mathbf{x}) = 0 \} \\
& \quad \{ \mathbf{y}^T \text{Jac}_P(\mathbf{x}) = 0 \}
\end{align*}
\]
Computing singular points

\( \mathcal{P} \) is the UOV public key: \( m \) quadratic polynomials in \( n \) variables

Modeling singular points

1. Minors modeling: \( \mathcal{M}(\mathcal{P}) : \)

\[
\begin{align*}
\mathcal{P}(\mathbf{x}) &= 0 \\
\text{MaxMinors}(\text{Jac}_\mathcal{P}(\mathbf{x})) &= 0
\end{align*}
\]

\[ \mathbf{x} \in \mathbb{F}_q^n \]

2. Bihomogeneous modeling: \( \mathcal{B}(\mathcal{P}) : \)

\[
\begin{align*}
\mathcal{P}(\mathbf{x}) &= 0 \\
\mathbf{y}^T \text{Jac}_\mathcal{P}(\mathbf{x}) &= 0
\end{align*}
\]

\[ \mathbf{x} \in \mathbb{F}_q^n, \mathbf{y} \in \mathbb{F}_q^m \]

These systems may be solved with Gröbner bases computations.
A good surprise in the grevlex Gröbner basis

**Gröbner basis**

The Gröbner bases we obtain are *special*: they contain linear polynomials.
A good surprise in the grevlex Gröbner basis

The Gröbner bases we obtain are special: they contain linear polynomials.

Figure 2: First 30 polynomials (out of 320) in a grevlex Gröbner basis for the system $B(\mathcal{P})$, $m = 7$, $n = 17$, $q = 251$ obtained with msolve.
A good surprise in the grevlex Gröbner basis

Gröbner basis

The Gröbner bases we obtain are special: they contain linear polynomials.

Figure 2: First 30 polynomials (out of 320) in a grevlex Gröbner basis for the system $B(P), m = 7, n = 17, q = 251$ obtained with msolve.
A good surprise in the grevlex Gröbner basis

The Gröbner bases we obtain are special: they contain linear polynomials.

**Figure 2:** First 30 polynomials (out of 320) in a grevlex Gröbner basis for the system $B(\mathcal{P})$, $m = 7$, $n = 17$, $q = 251$ obtained with **msolve**.
Self-diagnosis

If one or more of the below applies to you:

- I am terrified by polynomial systems!
- I have been traumatized by the $F4/F5$ algorithms!
- I really really love linear algebra!
- I want to break some crypto in the next 5 minutes!

Then the following may be of interest.
Are Gröbner bases overkill for this problem?

Self-diagnosis
If one or more of the below applies to you:

- I am terrified by polynomial systems!
- I have been traumatized by the $F4/F5$ algorithms!
- I really really love linear algebra!
- I want to break some crypto in the next 5 minutes!

Then the following may be of interest.

Motivation
Small field: Gröbner basis computation improved by enumeration.
An enumerative approach

Bihomogeneous modeling

\[ x \in \text{Sing}(V(I)) \iff \begin{cases} x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\ P(x) = 0 \\ y^T \text{Jac}_P(x) = 0 \end{cases} \]
An enumerative approach

Bihomogeneous modeling

\[ x \in \text{Sing}(V(I)) \iff \begin{cases} 
  x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\
  P(x) = 0 \\
  y^T \text{Jac}_P(x) = 0
\end{cases} \]

The [Kipnis, Shamir ’98] attack computes singular points

\[ x \in \text{Sing}(V(I)) \iff \begin{cases} 
  x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\
  P(x) = 0 \\
  x \in \ker \left( P^{-1}_m \sum_{i=1}^{m-1} y_i P_i - y_m I_n \right)
\end{cases} \]

\[ ^2 \text{[Luyten 2023], [Castryck, Beullens 2023]} \]
An enumerative approach

Bihomogeneous modeling

\[ x \in \text{Sing}(V(I)) \iff \begin{cases} x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\ \mathcal{P}(x) = 0 \\ y^T \text{Jac}_\mathcal{P}(x) = 0 \end{cases} \]

The [Kipnis, Shamir ’98] attack computes singular points

\[ x \in \text{Sing}(V(I)) \iff \begin{cases} x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\ \mathcal{P}(x) = 0 \\ x \in \ker \left( P_m^{-1} \sum_{i=1}^{m-1} y_i P_i - y_m I_n \right) \end{cases} \]

\[ ^2 \text{[Luyten 2023], [Castryck, Beullens 2023]} \]
An enumerative approach

Bihomogeneous modeling

\[ x \in \text{Sing}(V(I)) \iff \begin{cases} x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\ P(x) = 0 \\ y \in \ker \left( \text{Jac}_P(x)^T \right) \end{cases} \]

The [Kipnis, Shamir ’98] attack computes singular points

\[ x \in \text{Sing}(V(I)) \iff \begin{cases} x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\ P(x) = 0 \\ x \in \ker \left( P_m^{-1} \sum_{i=1}^{m-1} y_i P_i - y_m I_n \right) \end{cases} \]

\[2\] [Luyten 2023], [Castryck, Beullens 2023]
An enumerative approach

Bihomogeneous modeling

\[ x \in \text{Sing}(V(I)) \iff \begin{cases} 
  x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\
  P(x) = 0 \\
  y \in \ker \left( \text{Jac}_P(x)^T \right) 
\end{cases} \]

The [Kipnis, Shamir '98] attack computes singular points

\[ x \in \text{Sing}(V(I)) \iff \begin{cases} 
  x \in \mathbb{F}_q^n, y \in \mathbb{F}_q^m \\
  P(x) = 0 \\
  x \in \ker \left( P_m^{-1} \sum_{i=1}^{m-1} y_i P_i - y_m I_n \right) 
\end{cases} \]

\[ \implies x \text{ is an eigenvector of } P_m^{-1} \sum_{i=1}^{m-1} y_i P_i. \]

\[ ^2 \text{[Luyten 2023], [Castryck, Beullens 2023]} \]
### Kipnis-Shamir attack

[Kipnis, Patarin, Goubin 1999]

**x** is an eigenvector of \( P_m^{-1} \sum_{i=1}^{m-1} y_i P_i \) and \( x \in V(I) \).
Kipnis-Shamir revisited

Kipnis-Shamir attack [Kipnis, Patarin, Goubin 1999]

\[ x \text{ is an eigenvector of } P_m^{-1} \sum_{i=1}^{m-1} y_i P_i \text{ and } x \in V(I). \]

Expected cost [P. 2024]

If \( \dim \text{Sing}(V(I)) = d \), find \( \mathbb{F}_q \)-rational singular points by enumerating all \((y_1, \ldots, y_{m-1}) \in \mathbb{F}_q^{m-1} \) in time \( O(q^{m-1-d}mn^2) \).
### Kipnis-Shamir attack

Kipnis-Shamir attack \[\text{[Kipnis, Patarin, Goubin 1999]}\]

\[x\] is an eigenvector of \(P_m^{-1} \sum_{i=1}^{m-1} y_i P_i\) and \(x \in V(I)\).

### Expected cost

**Expected cost** \[\text{[P. 2024]}\]

If \(\dim \text{Sing}(V(I)) = d\), find \(\mathbb{F}_q\)-rational singular points by enumerating all \((y_1, \ldots, y_{m-1}) \in \mathbb{F}_q^{m-1}\) in time \(O(q^{m-1-d}mn^2)\).

### What did we bring to the table?

- Highlight heuristics and limits of Kipnis-Shamir.
### Kipnis-Shamir attack

[Kipnis, Patarin, Goubin 1999]

$x$ is an eigenvector of $P_m^{-1} \sum_{i=1}^{m-1} y_i P_i$ and $x \in V(I)$.  

### Expected cost

[P. 2024]

If $\dim \text{Sing}(V(I)) = d$, find $\mathbb{F}_q$-rational singular points by enumerating all $(y_1, \ldots, y_{m-1}) \in \mathbb{F}_q^{m-1}$ in time $O(q^{m-1-d} mn^2)$.

### What did we bring to the table?

- Highlight heuristics and limits of Kipnis-Shamir.
- Gröbner bases attack works if solutions are not $\mathbb{F}_q$-rational.
Kipnis-Shamir revisited

**Kipnis-Shamir attack**  
[Kipnis, Patarin, Goubin 1999]

\[ x \text{ is an eigenvector of } P_m^{-1} \sum_{i=1}^{m-1} y_i P_i \text{ and } x \in V(I). \]

**Expected cost**  
[P. 2024]

If \( \dim \text{Sing}(V(I)) = d \), find \( \mathbb{F}_q \)-rational singular points by enumerating all \( (y_1, \ldots, y_{m-1}) \in \mathbb{F}_q^{m-1} \) in time \( O(q^{m-1-d}mn^2) \)

**What did we bring to the table?**

- Highlight heuristics and limits of Kipnis-Shamir.
- Gröbner bases attack works if solutions are not \( \mathbb{F}_q \)-rational.
- Framework enables attacks on “perturbed” keys
  \[ \implies \text{we can attack other schemes.} \]
The $\hat{+}$ perturbation

$\text{UOV}^{\hat{+}}$ [Faugère, Macario-Rat, Patarin, Perret 2022]

Take a UOV secret key, replace $t$ equations by uniformly random equations, and mix the equations.
The $\hat{+}$ perturbation

[$\text{UOV}^{\hat{+}}$][Faugère, Macario-Rat, Patarin, Perret 2022]

Take a UOV secret key, replace $t$ equations by uniformly random equations, and mix the equations.

<table>
<thead>
<tr>
<th>UOV</th>
<th>$\text{UOV}^{\hat{+}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P = F \circ A$</td>
<td>$P = S \circ \hat{F} \circ A$</td>
</tr>
</tbody>
</table>
The \( \hat{+} \) perturbation

<table>
<thead>
<tr>
<th>UOV(^{\hat{+}})</th>
<th>[Faugère, Macario-Rat, Patarin, Perret 2022]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take a UOV secret key, replace ( t ) equations by uniformly random equations, and mix the equations.</td>
<td></td>
</tr>
</tbody>
</table>

\[
\begin{array}{c|c}
\text{UOV} & \text{UOV}^{\hat{+}} \\
\hline
\mathcal{P} = \mathcal{F} \circ A & \mathcal{P} = \mathcal{S} \circ \hat{\mathcal{F}} \circ A \\
\end{array}
\]

Methodology of the security analysis

Let \( \mathcal{P} \) be a UOV\(^{\hat{+}}\) public key defining an ideal \( I = \langle p_1, \ldots, p_m \rangle \). \( \emptyset \not\subset V(I) \), therefore key attacks on UOV\(^{\hat{+}}\) must invert \( \mathcal{S} \).
The $\hat{+}$ perturbation

**UOV$^\hat{+}$ [Faugère, Macario-Rat, Patarin, Perret 2022]**

Take a UOV secret key, replace $t$ equations by uniformly random equations, and mix the equations.

<table>
<thead>
<tr>
<th></th>
<th>UOV</th>
<th>UOV$^\hat{+}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{P} = \mathcal{F} \circ A$</td>
<td>$\mathcal{P} = S \circ \hat{\mathcal{F}} \circ A$</td>
<td></td>
</tr>
</tbody>
</table>

**Methodology of the security analysis**

Let $\mathcal{P}$ be a UOV$^\hat{+}$ public key defining an ideal $I = \langle p_1, \ldots, p_m \rangle$. $\emptyset \not\subset V(I)$, therefore key attacks on UOV$^\hat{+}$ must invert $S$.

**Motivation**

This methodology justifies an aggressive choice of parameters for improved efficiency compared with UOV.
New attack on VOX/UOV\(^\dagger\)

**Singular points attack and asymptotic result** [P. 2024]

Singular points of \(\hat{F} \circ A\) leak the trapdoor **without inverting** \(S\):

Our attack requires \(O(q^{2t} n^\omega)\) operations versus claimed \(q^{3t}\).

---

\(^3\) [Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud, Patarin, 2023]
New attack on VOX/UOV\textsuperscript{\dag}

**Singular points attack and asymptotic result** [P. 2024]

Singular points of $\hat{F} \circ A$ leak the trapdoor without inverting $S$:
Our attack requires $O(q^{2t} n^\omega)$ operations versus claimed $q^{3t}$.

For parameters submitted to NIST for VOX\textsuperscript{3}:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>I</th>
<th>III</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target (classical gates)</td>
<td>$2^{143}$</td>
<td>$2^{207}$</td>
<td>$2^{272}$</td>
</tr>
<tr>
<td>This work (classical gates)</td>
<td>$2^{121}$</td>
<td>$2^{167}$</td>
<td>$2^{221}$</td>
</tr>
</tbody>
</table>

\textsuperscript{3} [Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud, Patarin, 2023]
Thank you for your attention!

One vector to full key recovery in polynomial time \[ \text{[P. 2023]} \]
From **one vector** in \( \mathcal{O} \), return a basis of \( \mathcal{O} \) in **polynomial time**.

Singular points of UOV and UOV\(^{\land} \) \[ \text{[P. 2024]} \]
- \( V(I) \) has a **large** singular locus.
- Singular points of UOV\(^{\land} \) yield **faster** attacks.
- One vector to full key recovery on UOV\(^{\land} \) in \( O(q^t n^\omega) \).

Recap of the attack
- Find a weakness using **determinantal ideals**.
- Solve **bihomogeneous polynomial systems**.
Thank you for your attention!

**One vector to full key recovery in polynomial time** [P. 2023]

From *one vector* in $\mathcal{O}$, return a basis of $\mathcal{O}$ in *polynomial time*.

**Singular points of UOV and UOV$^{\dagger}$** [P. 2024]

- $V(I)$ has a *large* singular locus.
- Singular points of UOV$^{\dagger}$ yield *faster* attacks.
- One vector to full key recovery on UOV$^{\dagger}$ in $O(q^n \omega)$.

**Subfield attack on QR-UOV$^{\dagger}$** [P. 2024]

Weakness in a *structured variant* of UOV$^{\dagger}$ submitted to NIST:

- Broken on a laptop in *0.3s, 1.35s, 0.56s* (level I, III, V).
- *Attack new parameters* by *factoring* the degree of extension.
Bonus
A signature for the message $t \in \mathbb{F}_q^m$ is a vector $x \in \mathbb{F}_q^n$ such that

$$1 \leq i \leq m, G_i(x) = t_i$$
UOV: Signing process

**Signing**

A *signature* for the message $t \in \mathbb{F}_q^m$ is a vector $x \in \mathbb{F}_q^n$ such that $1 \leq i \leq m, G_i(x) = t_i$

- **Alice signs:** $y$ solution of $G(A^{-1}y) = t$ linear in $y_1, \ldots, y_m$.

---

**Diagram:**

1. **Alice** has **$(A, F)$**
2. **Alice** computes $x = Sign(G(t))$
3. **Bob** checks $G_i(x) = t_i$ for $1 \leq i \leq m$
Signatures

A signature for the message $t \in \mathbb{F}_q^m$ is a vector $x \in \mathbb{F}_q^n$ such that

$$1 \leq i \leq m, G_i(x) = t_i$$

- Alice signs: $y$ solution of $G(A^{-1}y) = t$ linear in $y_1, \ldots, y_m$. Sample $y_{m+1}, \ldots, y_n$ uniformly at random and solve a square linear system.

Alice returns $x = A^{-1}y$

Alice \hspace{1cm} Bob

$(A, F)$

$x = \text{Sign}(G(t))$

t $\in \mathbb{F}_q^m$

$x \in \mathbb{F}_q^n$

$G$
A **signature** for the message $t \in \mathbb{F}^m_q$ is a vector $x \in \mathbb{F}^n_q$ such that

$$1 \leq i \leq m, G_i(x) = t_i$$

- **Alice signs:** $y$ solution of $G(A^{-1}y) = t$ **linear** in $y_1, \ldots, y_m$.
  Sample $y_{m+1}, \ldots, y_n$ uniformly at random and solve a **square** linear system.
  Alice returns $x = A^{-1}y$
- **Bob verifies:** checks that for $1 \leq i \leq m, G_i(x) = t_i$. 

$$G(x) \rightleftharpoons t$$
Signing

A **signature** for the message $t \in \mathbb{F}_q^m$ is a vector $x \in \mathbb{F}_q^n$ such that

$$1 \leq i \leq m, G_i(x) = t_i$$

- **Alice signs**: $y$ solution of $G(A^{-1}y) = t$ **linear** in $y_1, \ldots, y_m$.
  Sample $y_{m+1}, \ldots, y_n$ uniformly at random and solve a **square linear system**.
  Alice returns $x = A^{-1}y$

- **Bob verifies**: checks that for $1 \leq i \leq m, G_i(x) = t_i$.

**Hash-and-sign**

In practice, $t = \mathcal{H}(M), M \in \{0, 1\}^*$
### UOV: Parameters

| NIST SL | $n$ | $m$ | $F_q$ | $|pk|$ (bytes) | $|sk|$ (bytes) | $|cpk|$ (bytes) | $|\text{sig+salt}|$ (bytes) |
|---------|-----|-----|-------|----------------|----------------|----------------|--------------------------|
| ov-Ip   | 1   | 112 | 44    | $F_{256}$      | 278 432        | 237 912        | 43 576                  | 128                      |
| ov-IIs  | 1   | 160 | 64    | $F_{16}$       | 412 160        | 348 720        | 66 576                  | 96                       |
| ov-III  | 3   | 184 | 72    | $F_{256}$      | 1 225 440      | 1 044 336      | 189 232                 | 200                      |
| ov-V    | 5   | 244 | 96    | $F_{256}$      | 2 869 440      | 2 436 720      | 446 992                 | 260                      |

**Figure 3:** Modern UOV [Beullens, Chen, Hung, Kannwischer, Peng, Shih, Yang 2023]
The UOV family

- "Multi-layer structure": Rainbow
- MAYO: key size/signature size trade-off.
- Structured keys: QR-UOV, VOX
- "Noisy" public key to increase security: UOV^+, VOX
- Formal security proof: T-UOV, PrUOV

UOV Family

PrUOV

T-UOV

SNOVA

DME-Sign

Biscuit
The UOV family

- “Multi-layer structure”: Rainbow
The UOV family

- "Multi-layer structure": Rainbow
- MAYO: key size/signature size trade-off.
The UOV family

- "Multi-layer structure": Rainbow
- MAYO: key size/signature size trade-off.
- Structured keys: QR-UOV, VOX, SNOVA
The UOV family

- "Multi-layer structure": Rainbow
- MAYO: key size/signature size trade-off.
- Structured keys: QR-UOV, VOX, SNOVA
- "Noisy" public key to increase security: UOV\(^\dagger\), VOX
The UOV family

- "Multi-layer structure": Rainbow
- MAYO: key size/signature size trade-off.
- Structured keys: QR-UOV, VOX, SNOVA
- "Noisy" public key to increase security: UOV, VOX
- Formal security proof: T-UOV, PrUOV