Cryptanalysis of multivariate signatures: Singular points of UOV and VOX

Pierre Pébereau
Sorbonne Université, LIP6, CNRS, Thales SIX

March, 2024

Context

NIST Post-quantum competition

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

Context

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

Context

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.

Building cryptography from (quantum-)hard problems

Multivariate Quadratic Problem - MQ(n, m, q)

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

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

Building cryptography from (quantum-)hard problems

Multivariate Quadratic Problem - MQ(n, m, q)

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

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

Multivariate Quadratic Cryptography

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

Building cryptography from (quantum-)hard problems

Multivariate Quadratic Problem - MQ(n, m, q)

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

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

Multivariate Quadratic Cryptography

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

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

Building cryptography from (quantum-)hard problems

Multivariate Quadratic Problem - MQ(n, m, q)

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

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

Multivariate Quadratic Cryptography

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

- The public key $\mathcal{P}$ is an instance of MQ(n, m, q), $n > m$.
- The secret key $\mathcal{S}$ enables, for all $\boldsymbol{t} \in \mathbb{F}_q^m$, to efficiently find $\boldsymbol{x} \in \mathbb{F}_q^n$ s.t. $\mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}$

UOV: Original formulation

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

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

Figure 1: UOV key pair in $\mathbb{F}_{257}$

UOV: Original formulation

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

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

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

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

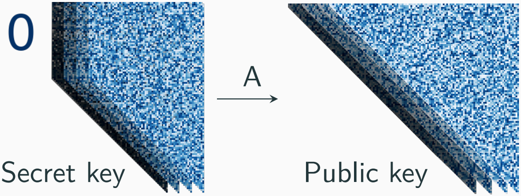


Figure 1: UOV key pair in $\mathbb{F}_{257}$

UOV: Original formulation

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

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

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

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

Naming conventions and parameters

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

$$V(I) = \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^m, \mathcal{P}(\boldsymbol{x}) = \boldsymbol{0}\}$$

UOV: Original formulation

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

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

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

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

Naming conventions and parameters

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

$$V(I) = \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^m, \mathcal{P}(\boldsymbol{x}) = \boldsymbol{0}\}$$

$\boldsymbol{x} \in \mathbb{F}_q^n$ is a signature for message $\boldsymbol{t} \in \mathbb{F}_q^m$ if $\mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}$.

UOV: Alternative formulation

Characterisation of the secret key **[Kipnis, Shamir 1998]**

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

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

UOV: Alternative formulation

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 $\mathcal{O}$.

UOV: Alternative formulation

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^λ logical gates.

UOV: Alternative formulation

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^λ logical gates.

Security level	I	III	V
Classical gates	2^{143}	2^{207}	2^{272}

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

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 $V(I)$.

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 $\text{UOV}^{\hat{+}}$ [P. 2024]

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

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$\hat{\dagger}$ [P. 2024]

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

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

Identified a weakness in a **structured variant** of UOV$\hat{\dagger}$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).

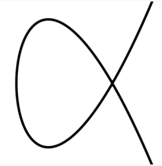
[1] [Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud, Patarin, 2023]

Contributions

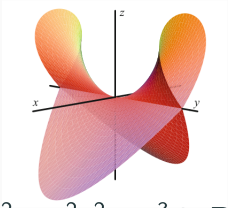
Singular points of UOV and $\text{UOV}^{\hat{+}}$ **[P. 2024]**

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

Singular points



$y^2 = x^3 - 3x + 2$ in $\mathbb{R}^2$

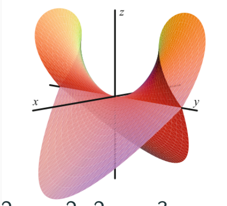


$x^2 - y^2z^2 + z^3$ in $\mathbb{R}^3$

(from [Cox, Little, O'Shea])

Singular points

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

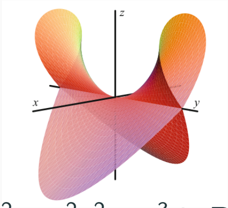


$x^2 - y^2 z^2 + z^3$ in $\mathbb{R}^3$

(from [Cox, Little, O'Shea])

Singular points

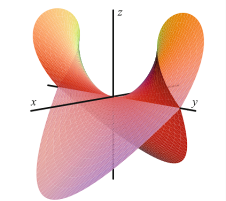
$y^2 = x^3 - 3x + 2$ in $\mathbb{R}^2$
Singular point: (1,0)



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

Singular points

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



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

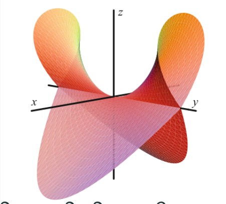
Definition

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

Singular points

$y^2 = x^3 - 3x + 2$ in $\mathbb{R}^2$

Singular point: (1,0)



$x^2 - y^2z^2 + z^3$ in $\mathbb{R}^3$

Singular points: line (x=z=0)

(from [Cox, Little, O'Shea])

Definition

Let $I = \langle p_1, \dots, p_m \rangle$ be an ideal of $\mathbb{K}[x_1, \dots, x_n]$.
$\boldsymbol{x} \in V(I) \setminus \{0\}$ is singular if $\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x})$ has rank less than $n - m$.

$$\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}) = \left(\frac{\partial}{\partial x_j} p_i(\boldsymbol{x}) \right) \in \mathbb{K}[x_1, \dots, x_n]^{m \times n}$$

Structured equations yield a structured Jacobian

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

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

Secret Jacobian

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \left[\begin{array}{c|c} \qquad J_1 \qquad & \qquad\qquad J_2 \qquad\qquad \end{array}\right] \\ 1 \cdots\cdots m \quad m+1 \cdots\cdots\cdots\cdots n \end{array}$$

Structured equations yield a structured Jacobian

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

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

Secret Jacobian

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \left[\begin{array}{c|c} \quad J_1 \quad & \qquad\quad J_2 \qquad\quad \end{array}\right] \\ 1 \cdots\cdots m \quad m+1 \cdots\cdots\cdots\cdots n \end{array}$$

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

1

Singular points in $\mathcal{O}$

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \begin{bmatrix} \quad 0 \quad & \quad J_2(\boldsymbol{x}) \quad \end{bmatrix} \\ 1 \cdots\cdots m \quad m+1 \cdots\cdots\cdots\cdots n \end{array}$$

1

Singular points leak the trapdoor

Singular points in $\mathcal{O}$

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \left[\begin{array}{c|c} \quad 0 \quad & \qquad J_2(\boldsymbol{x}) \qquad \end{array}\right] \\ \begin{array}{cc} 1 \cdots\cdots m & m+1 \cdots\cdots\cdots\cdots n \end{array} \end{array}$$

Determinantal ideal

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

$$\mathcal{J}_{m-1} = \langle \mathrm{MaxMinors}(\mathrm{J}_2(\mathrm{x})) \rangle$$

1

Singular points leak the trapdoor

Singular points in $\mathcal{O}$

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \left[\begin{array}{c|c} \quad 0 \quad & \qquad J_2(\boldsymbol{x}) \qquad \end{array}\right] \\ \begin{array}{cc} 1 \cdots\cdots m & m+1 \cdots\cdots\cdots\cdots n \end{array} \end{array}$$

Determinantal ideal

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

$$\mathcal{J}_{m-1} = \langle \mathrm{MaxMinors}(\mathrm{J}_2(\mathrm{x})) \rangle$$

Dimension of the singular locus

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

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

[1] Faugère, Safey El Din, Spaenlehauer, 2013, Theorem 10

Computing singular points

$\mathcal{P}$ 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

❶ Minors modeling: $\mathcal{M}(\mathcal{P}) : \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \mathrm{MaxMinors}(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x})) = 0 \end{cases}$

Computing singular points

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

Modeling singular points

❶ Minors modeling: $\mathcal{M}(\mathcal{P}) : \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \mathrm{MaxMinors}(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x})) = 0 \end{cases}$

Computing singular points

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

Modeling singular points

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

Computing singular points

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

Modeling singular points

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

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

Computing singular points

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

Modeling singular points

1. Minors modeling: $\mathcal{M}(\mathcal{P}) : \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \mathrm{MaxMinors}(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x})) = 0 \end{cases}$
2. Bihomogeneous modeling: $\mathcal{B}(\mathcal{P}) : \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n, \boldsymbol{y} \in \mathbb{F}_q^m \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \boldsymbol{y}^T \mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}) = 0 \end{cases}$

Computing singular points

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

Modeling singular points

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

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

Computing singular points

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

Modeling singular points

1. Minors modeling: $\mathcal{M}(\mathcal{P}) : \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \mathrm{MaxMinors}(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x})) = 0 \end{cases}$
2. Bihomogeneous modeling: $\mathcal{B}(\mathcal{P}) : \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n, \boldsymbol{y} \in \mathbb{F}_q^m \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \boldsymbol{y}^T \mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}) = 0 \end{cases}$

These systems may be solved with Gröbner bases computations.

A good surprise in the grevlex Gröbner basis

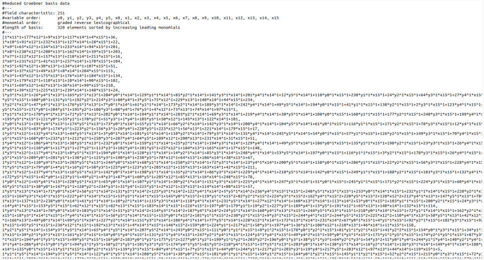
Gröbner basis

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

A good surprise in the grevlex Gröbner basis

Gröbner basis

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



```
#Reduced Groebner basis data
#---
#field characteristic: 251
#variable order:      y0, y1, y2, y3, y4, y5, x0, x1, x2, x3, x4, x5, x6, x7, x8, x9, x10, x11, x12, x13, x14, x15
#monomial order:      graded reverse lexicographical
#length of basis:     320 elements sorted by increasing leading monomials
#---
[1*x11^1+177*x12^1+9*x13^1+117*x14^1+4*x15^1+36,
1*x10^1+91*x12^1+232*x13^1+127*x14^1+28*x15^1+22,
1*x9^1+63*x12^1+134*x13^1+233*x14^1+94*x15^1+201,
1*x8^1+238*x12^1+200*x13^1+162*x14^1+39*x15^1+203,
1*x7^1+112*x12^1+157*x13^1+218*x14^1+211*x15^1+16,
1*x6^1+231*x12^1+41*x13^1+237*x14^1+170*x15^1+104,
1*x5^1+92*x12^1+30*x13^1+134*x14^1+107*x15^1+51,
1*x4^1+37*x12^1+49*x13^1+8*x14^1+204*x15^1+115,
1*x3^1+43*x12^1+175*x13^1+176*x14^1+184*x15^1+134,
1*x2^1+179*x12^1+110*x13^1+10*x14^1+90*x15^1+102,
1*x1^1+69*x12^1+62*x13^1+36*x14^1+99*x15^1+210,
1*x0^1+39*x12^1+225*x13^1+239*x14^1+148*x15^1+24,
```

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

A good surprise in the grevlex Gröbner basis

Gröbner basis

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

```
#Reduced Groebner basis data
#---
#field characteristic: 251
#variable order:       y0, y1, y2, y3, y4, y5, x0, x1, x2, x3, x4, x5, x6, x7, x8, x9, x10, x11, x12, x13, x14, x15
#monomial order:       graded reverse lexicographical
#length of basis:      320 elements sorted by increasing leading monomials
#---
[1*x11^1+177*x12^1+9*x13^1+117*x14^1+4*x15^1+36,
1*x10^1+91*x12^1+232*x13^1+127*x14^1+28*x15^1+22,
1*x9^1+63*x12^1+134*x13^1+233*x14^1+94*x15^1+201,
1*x8^1+238*x12^1+200*x13^1+162*x14^1+39*x15^1+203,
1*x7^1+112*x12^1+157*x13^1+218*x14^1+211*x15^1+16,
1*x6^1+231*x12^1+41*x13^1+237*x14^1+170*x15^1+104,
1*x5^1+92*x12^1+30*x13^1+134*x14^1+107*x15^1+51,
1*x4^1+37*x12^1+49*x13^1+8*x14^1+204*x15^1+115,
1*x3^1+43*x12^1+175*x13^1+176*x14^1+184*x15^1+134,
1*x2^1+179*x12^1+110*x13^1+10*x14^1+90*x15^1+102,
1*x1^1+69*x12^1+62*x13^1+36*x14^1+99*x15^1+210,
1*x0^1+39*x12^1+225*x13^1+239*x14^1+148*x15^1+24,
```

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

Gröbner basis

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

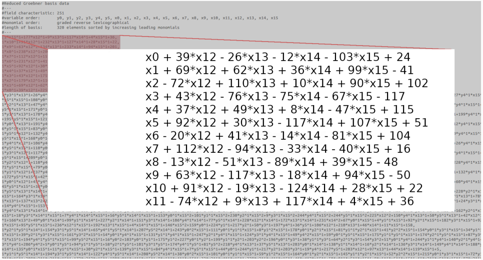


Figure 2: First 30 polynomials (out of 320) in a grevlex Gröbner basis for the system $\mathcal{B}(\mathcal{P}), m = 7, n = 17, q = 251$ obtained with **msolve**.

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.

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

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

An enumerative approach

Bihomogeneous modeling

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

The [Kipnis, Shamir '98] attack computes singular points [2]

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

[2] [Luyten 2023], [Castryck, Beullens 2023]

An enumerative approach

Bihomogeneous modeling

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

The [Kipnis, Shamir '98] attack computes singular points [2]

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

[2] [Luyten 2023], [Castryck, Beullens 2023]

An enumerative approach

Bihomogeneous modeling

$$x \in \mathrm{Sing}(V(I)) \iff \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n, \boldsymbol{y} \in \mathbb{F}_q^m \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \boldsymbol{y} \in \ker\left(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x})^T\right) \end{cases}$$

The [Kipnis, Shamir '98] attack computes singular points [2]

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

[2] [Luyten 2023], [Castryck, Beullens 2023]

An enumerative approach

Bihomogeneous modeling

$$\boldsymbol{x} \in \mathrm{Sing}(V(I)) \iff \begin{cases} \boldsymbol{x} \in \mathbb{F}_q^n, \boldsymbol{y} \in \mathbb{F}_q^m \\ \mathcal{P}(\boldsymbol{x}) = 0 \\ \boldsymbol{y} \in \ker\left(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x})^T\right) \end{cases}$$

The [Kipnis, Shamir '98] attack computes singular points [2]

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

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

[2] [Luyten 2023], [Castryck, Beullens 2023]

Kipnis-Shamir revisited

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

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

Kipnis-Shamir revisited

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

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

Expected cost **[P. 2024]**

If $\dim \operatorname{Sing}(V(I)) = d$, 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 revisited

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

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

Expected cost **[P. 2024]**

If $\dim \mathrm{Sing}(V(I)) = d$, 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 revisited

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

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

Expected cost [P. 2024]

If $\dim \mathrm{Sing}(V(I)) = d$, 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]**

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

Expected cost **[P. 2024]**

If $\dim \mathrm{Sing}(V(I)) = d$, 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

  $\Longrightarrow$ we can attack other schemes.

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.

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

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

UOV	UOV$^{\hat{+}}$
$\mathcal{P} = \mathcal{F} \circ A$	$\mathcal{P} = \mathcal{S} \circ \hat{\mathcal{F}} \circ A$

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.

UOV	UOV$^{\hat{+}}$
$\mathcal{P} = \mathcal{F} \circ A$	$\mathcal{P} = \mathcal{S} \circ \hat{\mathcal{F}} \circ A$

Methodology of the security analysis

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

UOV	UOV$^{\hat{+}}$
$\mathcal{P} = \mathcal{F} \circ A$	$\mathcal{P} = \mathcal{S} \circ \hat{\mathcal{F}} \circ A$

Methodology of the security analysis

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

Motivation

This methodology justifies an aggressive choice of parameters for improved efficiency compared with UOV.

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

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

[3] [Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud, Patarin, 2023]

New attack on VOX/UOV$\hat{+}$

Singular points attack and asymptotic result [P. 2024]

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

For parameters submitted to NIST for VOX[3]:

Parameters	I	III	V
Target (classical gates)	2^{143}	2^{207}	2^{272}
This work (classical gates)	$\mathbf{2^{121}}$	$\mathbf{2^{167}}$	$\mathbf{2^{221}}$

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 [P. 2023]

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

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

- $V(I)$ has a large singular locus.
- Singular points of $\text{UOV}^{\hat{+}}$ yield faster attacks.
- One vector to full key recovery on $\text{UOV}^{\hat{+}}$ 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$^{\hat{\dagger}}$ [P. 2024]

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

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

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

- Broken on a laptop in $\mathbf{0.3}s$, $\mathbf{1.35}s$, $\mathbf{0.56}s$ (level I, III, V).
- Attack new parameters by factoring the degree of extension.

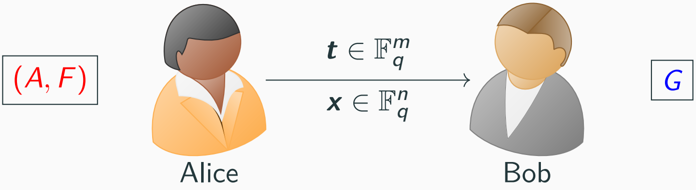
Bonus

UOV: Signing process

Signing

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

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



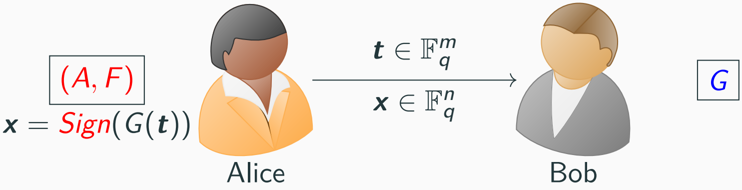
UOV: Signing process

Signing

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

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

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



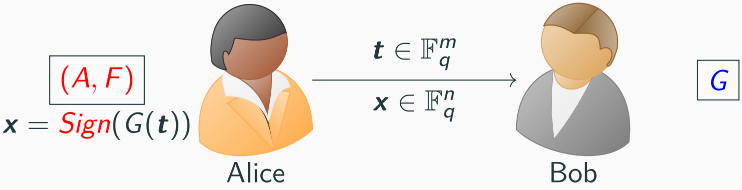
UOV: Signing process

Signing

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

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

- Alice *signs*: $\boldsymbol{y}$ 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 $\boldsymbol{x} = A^{-1}y$



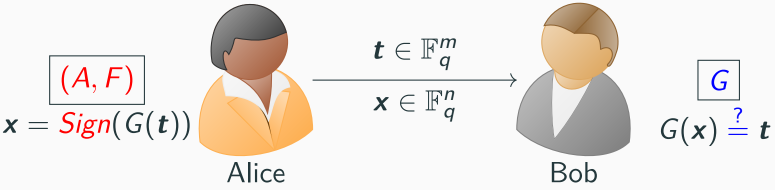
UOV: Signing process

Signing

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

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

- Alice *signs*: $\boldsymbol{y}$ 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 $\boldsymbol{x} = A^{-1}y$
- Bob verifies: checks that for $1 \leq i \leq m$, $G_i(\boldsymbol{x}) = t_i$.



UOV: Signing process

Signing

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

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

- Alice *signs*: $\boldsymbol{y}$ 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 $\boldsymbol{x} = A^{-1}y$
- Bob verifies: checks that for $1 \leq i \leq m$, $G_i(\boldsymbol{x}) = t_i$.

Hash-and-sign

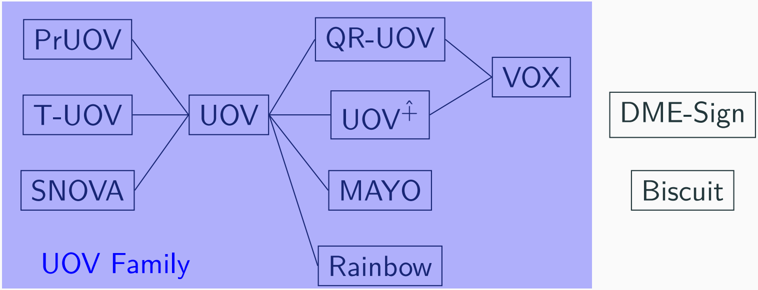
In practice, $\boldsymbol{t} = \mathcal{H}(M), M \in \{0,1\}^*$

UOV: Parameters

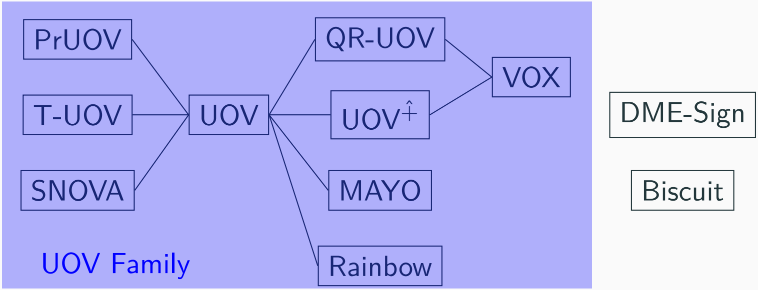
	NIST SL	n	m	$\mathbb{F}_q$	$\lvert$pk$\rvert$ (bytes)	$\lvert$sk$\rvert$ (bytes)	$\lvert$cpk$\rvert$ (bytes)	$\lvert$sig+salt$\rvert$ (bytes)
`ov-Ip`	1	112	44	$\mathbb{F}_{256}$	278 432	237 912	43 576	128
`ov-Is`	1	160	64	$\mathbb{F}_{16}$	412 160	348 720	66 576	96
`ov-III`	3	184	72	$\mathbb{F}_{256}$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

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

Multivariate Post-Quantum Zoo at NIST



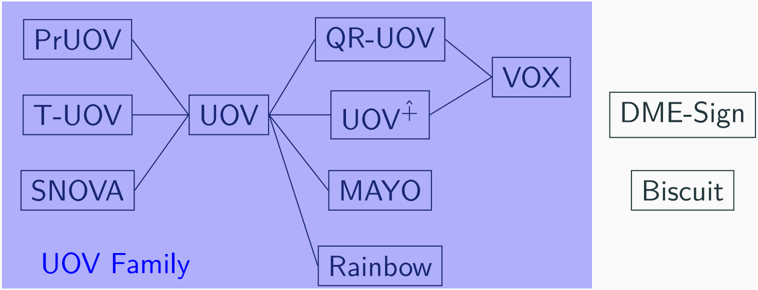
Multivariate Post-Quantum Zoo at NIST



The UOV family

- "Multi-layer structure": Rainbow

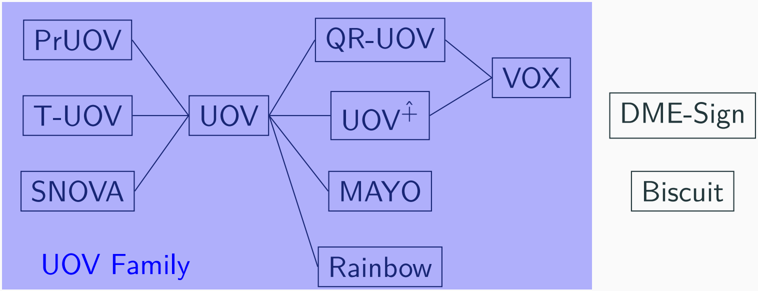
Multivariate Post-Quantum Zoo at NIST



The UOV family

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

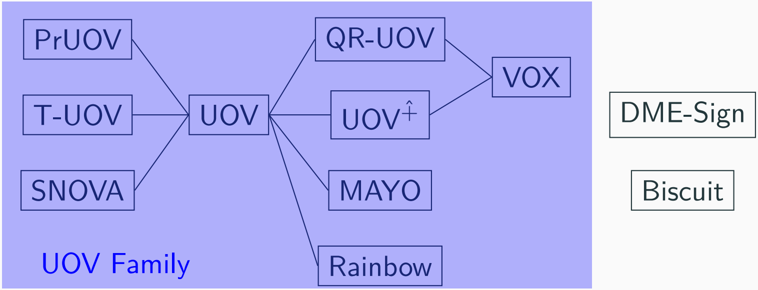
Multivariate Post-Quantum Zoo at NIST



The UOV family

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

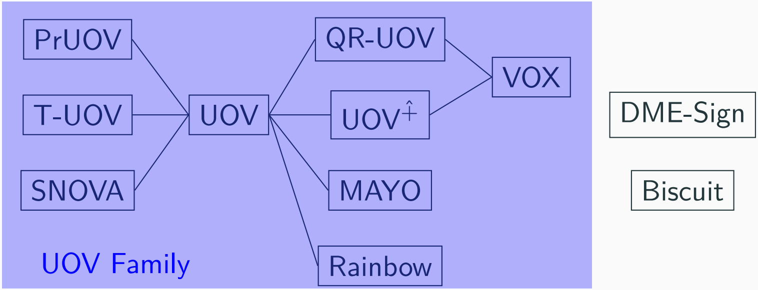
Multivariate Post-Quantum Zoo at NIST



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$^{\hat{+}}$, VOX

Multivariate Post-Quantum Zoo at NIST



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$^{\hat{+}}$, VOX
- Formal security proof: T-UOV, PrUOV