

# Cryptanalysis of multivariate signatures: Singular points of UOV and VOX

---

**Pierre Pébereau**

Sorbonne Université, LIP6, CNRS, Thales SIX



**SORBONNE  
UNIVERSITÉ**

**THALES**

March, 2024

## NIST Post-quantum competition

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

## 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.

# Building cryptography from (quantum-)hard problems

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

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

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

# Building cryptography from (quantum-)hard problems

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

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

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

## 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)  $\mathbf{x} \in \mathbb{F}_q^n$  to a system of  $m$  quadratic equations in  $n$  variables

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

## 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( $n, m, q$ ),  $n > m$ .

# Building cryptography from (quantum-)hard problems

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

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

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

## 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  $\mathbf{t} \in \mathbb{F}_q^m$ , to **efficiently** find  $\mathbf{x} \in \mathbb{F}_q^n$  s.t.  $\mathcal{P}(\mathbf{x}) = \mathbf{t}$



## UOV: Original formulation

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

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

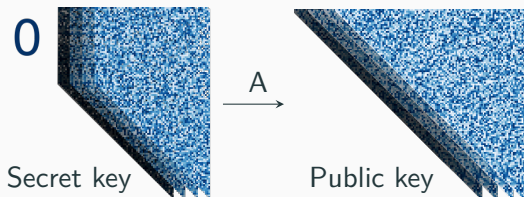
**Secret key:** -  $m$  quadratic polynomials  $\mathbf{x}^T F_i \mathbf{x} \in \mathbb{F}_q[x_1, \dots, x_n]$

linear in  $x_1, \dots, x_m$ .

- invertible change of variables  $A$ .

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

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



**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  $\mathbf{x}^T F_i \mathbf{x} \in \mathbb{F}_q[x_1, \dots, x_n]$

linear in  $x_1, \dots, x_m$ .

- invertible change of variables  $A$ .

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

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

### Naming conventions and parameters

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

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

# UOV: Original formulation

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

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

linear in  $x_1, \dots, x_m$ .

- invertible change of variables  $A$ .

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

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

## Naming conventions and parameters

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

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

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

## 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  $2^\lambda$  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  $2^\lambda$  logical gates.

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



**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**.

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

- **Existence** and **dimension** of singular locus of  $V(I)$ .

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

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

## 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  $\text{UOV}^{\hat{+}}$ .

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

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

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

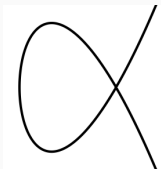
<sup>1</sup> [Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud, Patarin, 2023]

## Singular points of $\text{UOV}$ and $\text{UOV}^{\hat{+}}$

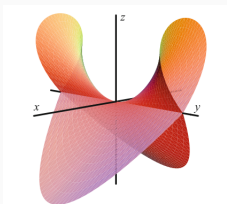
[P. 2024]

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

## Singular points



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



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

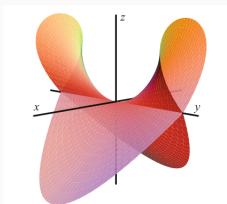
(from [Cox, Little, O'Shea])

## Singular points



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

Singular point:  $(1,0)$



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

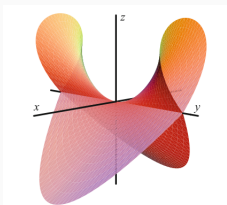
(from [Cox, Little, O'Shea])

## 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])

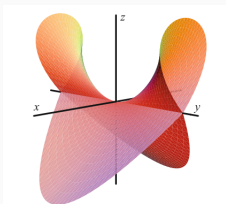


# Singular points



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

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  $I = \langle p_1, \dots, p_m \rangle$  be an ideal of  $\mathbb{K}[x_1, \dots, x_n]$ .

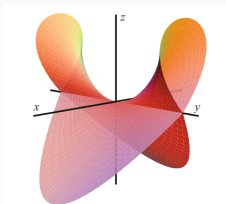
$\mathbf{x} \in V(I) \setminus \{0\}$  is **singular** if  $\text{Jac}_{\mathcal{P}}(\mathbf{x})$  has rank less than  $n - m$ .

## 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  $I = \langle p_1, \dots, p_m \rangle$  be an ideal of  $\mathbb{K}[x_1, \dots, x_n]$ .

$\mathbf{x} \in V(I) \setminus \{0\}$  is **singular** if  $\text{Jac}_p(\mathbf{x})$  has rank less than  $n - m$ .

$$\text{Jac}_p(\mathbf{x}) = \left( \frac{\partial}{\partial x_j} p_i(\mathbf{x}) \right) \in \mathbb{K}[x_1, \dots, x_n]^{m \times n}$$

## Structured equations yield a structured Jacobian

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

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

# Structured equations yield a structured Jacobian

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

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

## Secret Jacobian

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

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

# Structured equations yield a structured Jacobian

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

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

## Secret Jacobian

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

$$\text{Jac}_{\mathcal{F}}(\mathbf{x}) = \begin{bmatrix} J_1 & J_2 \end{bmatrix}$$

$1 \dots m \quad m+1 \dots n$

Where  $J_1 \in \mathbb{F}_q[x_{m+1}, \dots, x_n]^{m \times m}$  and  $J_2 \in \mathbb{F}_q[x_1, \dots, x_n]^{m \times n-m}$ .

# Singular points leak the trapdoor

## Singular points in $\mathcal{O}$

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

# Singular points leak the trapdoor

## Singular points in $\mathcal{O}$

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

$$\text{Jac}_{\mathcal{F}}(\mathbf{x}) = \begin{bmatrix} \mathbf{0} & J_2(\mathbf{x}) \end{bmatrix}$$

$1 \dots m \quad m+1 \dots n$

# Singular points leak the trapdoor

## Singular points in $\mathcal{O}$

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

$$\text{Jac}_{\mathcal{F}}(\mathbf{x}) = \begin{bmatrix} \mathbf{0} & J_2(\mathbf{x}) \end{bmatrix}$$

$1 \dots m \quad m+1 \dots n$

## Determinantal ideal

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

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



# Singular points leak the trapdoor

## Singular points in $\mathcal{O}$

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

$$\text{Jac}_{\mathcal{F}}(\mathbf{x}) = \begin{bmatrix} \mathbf{0} & J_2(\mathbf{x}) \end{bmatrix}$$

$1 \dots m \quad m+1 \dots n$

## Determinantal ideal

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

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

## Dimension of the singular locus

Under a **genericity** assumption, [FSS13]<sup>1</sup> yields

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

<sup>1</sup>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

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

# Computing singular points

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

## Modeling singular points

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

# Computing singular points

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

## Modeling singular points

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

# Computing singular points

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

## Modeling singular points

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

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

# Computing singular points

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

## Modeling singular points

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

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

# Computing singular points

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

## Modeling singular points

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

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



# Computing singular points

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

## Modeling singular points

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

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

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 Gröbner basis data
#
#File: character101: 33
#variable order:  m1, m2, m3, m4, m5, m6, m7, m8, m9, m10, m11, m12, m13, m14, m15, m16, m17, m18, m19, m20, m21, m22, m23, m24, m25, m26, m27, m28, m29, m30, m31, m32, m33, m34, m35, m36, m37, m38, m39, m40, m41, m42, m43, m44, m45, m46, m47, m48, m49, m50, m51, m52, m53, m54, m55, m56, m57, m58, m59, m60, m61, m62, m63, m64, m65, m66, m67, m68, m69, m70, m71, m72, m73, m74, m75, m76, m77, m78, m79, m80, m81, m82, m83, m84, m85, m86, m87, m88, m89, m90, m91, m92, m93, m94, m95, m96, m97, m98, m99, m100, m101, m102, m103, m104, m105, m106, m107, m108, m109, m110, m111, m112, m113, m114, m115, m116, m117, m118, m119, m120, m121, m122, m123, m124, m125, m126, m127, m128, m129, m130, m131, m132, m133, m134, m135, m136, m137, m138, m139, m140, m141, m142, m143, m144, m145, m146, m147, m148, m149, m150, m151, m152, m153, m154, m155, m156, m157, m158, m159, m160, m161, m162, m163, m164, m165, m166, m167, m168, m169, m170, m171, m172, m173, m174, m175, m176, m177, m178, m179, m180, m181, m182, m183, m184, m185, m186, m187, m188, m189, m190, m191, m192, m193, m194, m195, m196, m197, m198, m199, m200, m201, m202, m203, m204, m205, m206, m207, m208, m209, m210, m211, m212, m213, m214, m215, m216, m217, m218, m219, m220, m221, m222, m223, m224, m225, m226, m227, m228, m229, m230, m231, m232, m233, m234, m235, m236, m237, m238, m239, m240, m241, m242, m243, m244, m245, m246, m247, m248, m249, m250, m251
#monomial order:  graded reverse lexicographic
#strength of basis:  100 elements sorted by increasing leading monomials
#
#-----
#m1: x1^251
#m2: x1^250
#m3: x1^249
#m4: x1^248
#m5: x1^247
#m6: x1^246
#m7: x1^245
#m8: x1^244
#m9: x1^243
#m10: x1^242
#m11: x1^241
#m12: x1^240
#m13: x1^239
#m14: x1^238
#m15: x1^237
#m16: x1^236
#m17: x1^235
#m18: x1^234
#m19: x1^233
#m20: x1^232
#m21: x1^231
#m22: x1^230
#m23: x1^229
#m24: x1^228
#m25: x1^227
#m26: x1^226
#m27: x1^225
#m28: x1^224
#m29: x1^223
#m30: x1^222
#m31: x1^221
#m32: x1^220
#m33: x1^219
#m34: x1^218
#m35: x1^217
#m36: x1^216
#m37: x1^215
#m38: x1^214
#m39: x1^213
#m40: x1^212
#m41: x1^211
#m42: x1^210
#m43: x1^209
#m44: x1^208
#m45: x1^207
#m46: x1^206
#m47: x1^205
#m48: x1^204
#m49: x1^203
#m50: x1^202
#m51: x1^201
#m52: x1^200
#m53: x1^199
#m54: x1^198
#m55: x1^197
#m56: x1^196
#m57: x1^195
#m58: x1^194
#m59: x1^193
#m60: x1^192
#m61: x1^191
#m62: x1^190
#m63: x1^189
#m64: x1^188
#m65: x1^187
#m66: x1^186
#m67: x1^185
#m68: x1^184
#m69: x1^183
#m70: x1^182
#m71: x1^181
#m72: x1^180
#m73: x1^179
#m74: x1^178
#m75: x1^177
#m76: x1^176
#m77: x1^175
#m78: x1^174
#m79: x1^173
#m80: x1^172
#m81: x1^171
#m82: x1^170
#m83: x1^169
#m84: x1^168
#m85: x1^167
#m86: x1^166
#m87: x1^165
#m88: x1^164
#m89: x1^163
#m90: x1^162
#m91: x1^161
#m92: x1^160
#m93: x1^159
#m94: x1^158
#m95: x1^157
#m96: x1^156
#m97: x1^155
#m98: x1^154
#m99: x1^153
#m100: x1^152
#m101: x1^151
#m102: x1^150
#m103: x1^149
#m104: x1^148
#m105: x1^147
#m106: x1^146
#m107: x1^145
#m108: x1^144
#m109: x1^143
#m110: x1^142
#m111: x1^141
#m112: x1^140
#m113: x1^139
#m114: x1^138
#m115: x1^137
#m116: x1^136
#m117: x1^135
#m118: x1^134
#m119: x1^133
#m120: x1^132
#m121: x1^131
#m122: x1^130
#m123: x1^129
#m124: x1^128
#m125: x1^127
#m126: x1^126
#m127: x1^125
#m128: x1^124
#m129: x1^123
#m130: x1^122
#m131: x1^121
#m132: x1^120
#m133: x1^119
#m134: x1^118
#m135: x1^117
#m136: x1^116
#m137: x1^115
#m138: x1^114
#m139: x1^113
#m140: x1^112
#m141: x1^111
#m142: x1^110
#m143: x1^109
#m144: x1^108
#m145: x1^107
#m146: x1^106
#m147: x1^105
#m148: x1^104
#m149: x1^103
#m150: x1^102
#m151: x1^101
#m152: x1^100
#m153: x1^99
#m154: x1^98
#m155: x1^97
#m156: x1^96
#m157: x1^95
#m158: x1^94
#m159: x1^93
#m160: x1^92
#m161: x1^91
#m162: x1^90
#m163: x1^89
#m164: x1^88
#m165: x1^87
#m166: x1^86
#m167: x1^85
#m168: x1^84
#m169: x1^83
#m170: x1^82
#m171: x1^81
#m172: x1^80
#m173: x1^79
#m174: x1^78
#m175: x1^77
#m176: x1^76
#m177: x1^75
#m178: x1^74
#m179: x1^73
#m180: x1^72
#m181: x1^71
#m182: x1^70
#m183: x1^69
#m184: x1^68
#m185: x1^67
#m186: x1^66
#m187: x1^65
#m188: x1^64
#m189: x1^63
#m190: x1^62
#m191: x1^61
#m192: x1^60
#m193: x1^59
#m194: x1^58
#m195: x1^57
#m196: x1^56
#m197: x1^55
#m198: x1^54
#m199: x1^53
#m200: x1^52
#m201: x1^51
#m202: x1^50
#m203: x1^49
#m204: x1^48
#m205: x1^47
#m206: x1^46
#m207: x1^45
#m208: x1^44
#m209: x1^43
#m210: x1^42
#m211: x1^41
#m212: x1^40
#m213: x1^39
#m214: x1^38
#m215: x1^37
#m216: x1^36
#m217: x1^35
#m218: x1^34
#m219: x1^33
#m220: x1^32
#m221: x1^31
#m222: x1^30
#m223: x1^29
#m224: x1^28
#m225: x1^27
#m226: x1^26
#m227: x1^25
#m228: x1^24
#m229: x1^23
#m230: x1^22
#m231: x1^21
#m232: x1^20
#m233: x1^19
#m234: x1^18
#m235: x1^17
#m236: x1^16
#m237: x1^15
#m238: x1^14
#m239: x1^13
#m240: x1^12
#m241: x1^11
#m242: x1^10
#m243: x1^9
#m244: x1^8
#m245: x1^7
#m246: x1^6
#m247: x1^5
#m248: x1^4
#m249: x1^3
#m250: x1^2
#m251: x1
```

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**.



# 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**.

## Bihomogeneous modeling

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



## Bihomogeneous modeling

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

The [Kipnis, Shamir '98] attack computes singular points <sup>2</sup>

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

<sup>2</sup>[Luyten 2023], [Castricky, Beullens 2023]

## Bihomogeneous modeling

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

The [Kipnis, Shamir '98] attack computes singular points <sup>2</sup>

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

<sup>2</sup>[Luyten 2023], [Castricky, Beullens 2023]

## Bihomogeneous modeling

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

The [Kipnis, Shamir '98] attack computes singular points <sup>2</sup>

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

<sup>2</sup>[Luyten 2023], [Castricky, Beullens 2023]

# An enumerative approach

## Bihomogeneous modeling

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

The [Kipnis, Shamir '98] attack computes singular points <sup>2</sup>

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

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

<sup>2</sup>[Luyten 2023], [Castricky, 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 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  $(y_1, \dots, y_{m-1}) \in \mathbb{F}_q^{m-1}$  in time  $O(q^{m-1-d} mn^2)$

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  $(y_1, \dots, y_{m-1}) \in \mathbb{F}_q^{m-1}$  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  $(y_1, \dots, y_{m-1}) \in \mathbb{F}_q^{m-1}$  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 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  $(y_1, \dots, y_{m-1}) \in \mathbb{F}_q^{m-1}$  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  
 $\implies$  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.

# The $\hat{\dagger}$ perturbation

UOV $\hat{\dagger}$

[Faugère, Macario-Rat, Patarin, Perret 2022]

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

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

# The $\hat{\dagger}$ perturbation

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

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

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

## Methodology of the security analysis

Let  $\mathcal{P}$  be a UOV $\hat{\dagger}$  public key defining an ideal  $I = \langle p_1, \dots, p_m \rangle$ .  $\mathcal{O} \notin V(I)$ , therefore key attacks on UOV $\hat{\dagger}$  must invert  $\mathcal{S}$ .

# The $\hat{\dagger}$ perturbation

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

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

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

## Methodology of the security analysis

Let  $\mathcal{P}$  be a UOV $\hat{\dagger}$  public key defining an ideal  $I = \langle p_1, \dots, p_m \rangle$ .  $\mathcal{O} \notin V(I)$ , therefore key attacks on UOV $\hat{\dagger}$  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  $\mathcal{O}(q^{2t} n^\omega)$  operations versus claimed  $q^{3t}$ .

---

<sup>3</sup> [Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud, Patarin, 2023]

## 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  $\mathcal{O}(q^{2t} n^\omega)$  operations versus claimed  $q^{3t}$ .

For parameters submitted to NIST for VOX<sup>3</sup>:

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

<sup>3</sup> [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 $\text{UOV}^{\hat{\dagger}}$ [P. 2024]

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

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

Weakness in a **structured variant** of  $\text{UOV}^{\hat{+}}$  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.

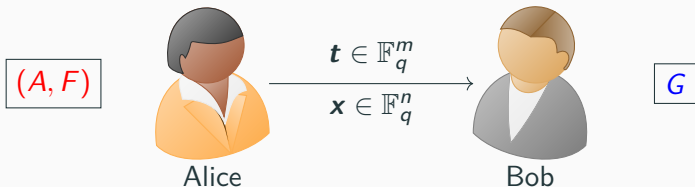
## Bonus

---

# UOV: Signing process

## Signing

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

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


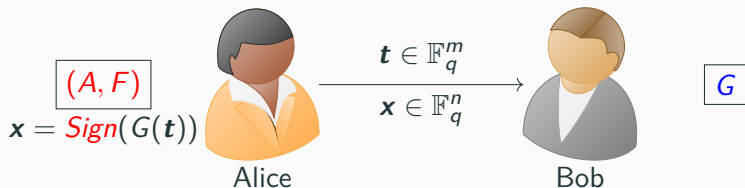
# UOV: Signing process

## Signing

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

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

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



# UOV: Signing process

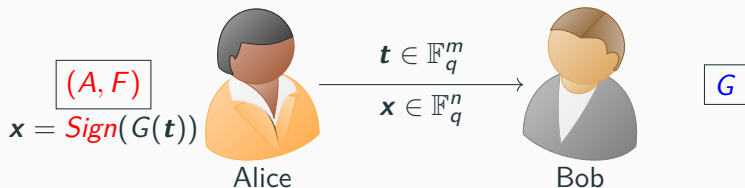
## Signing

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

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

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

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



# UOV: Signing process

## Signing

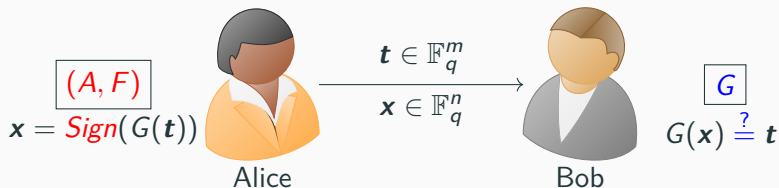
A **signature** for the message  $\mathbf{t} \in \mathbb{F}_q^m$  is a vector  $\mathbf{x} \in \mathbb{F}_q^n$  such that

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

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

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

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



# UOV: Signing process

## Signing

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

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

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

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

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

## Hash-and-sign

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

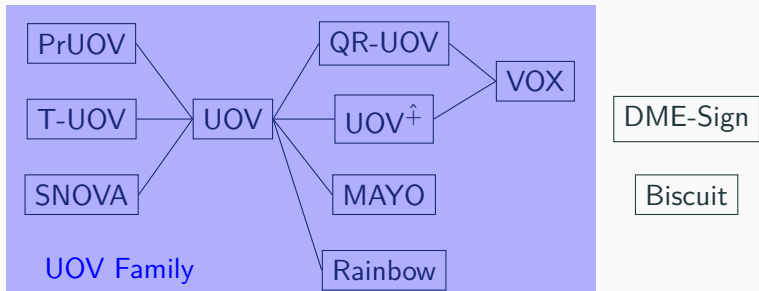
# UOV: Parameters

	NIST SL	$n$	$m$	$\mathbb{F}_q$	$ pk $ (bytes)	$ sk $ (bytes)	$ cpk $ (bytes)	$ sig+salt $ (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

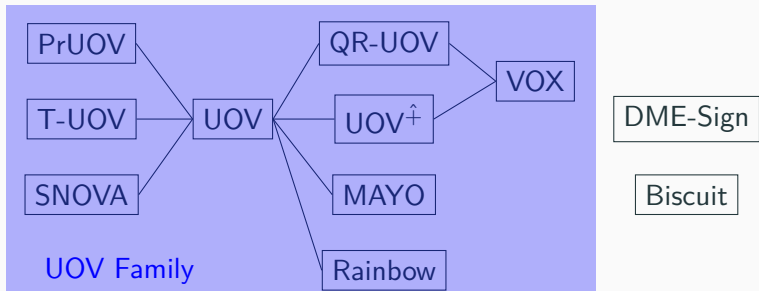
**Figure 3:** Modern UOV [Beullens, Chen, Hung, Kannwischer, Peng, Shih, Yang 2023]



# Multivariate Post-Quantum Zoo at NIST



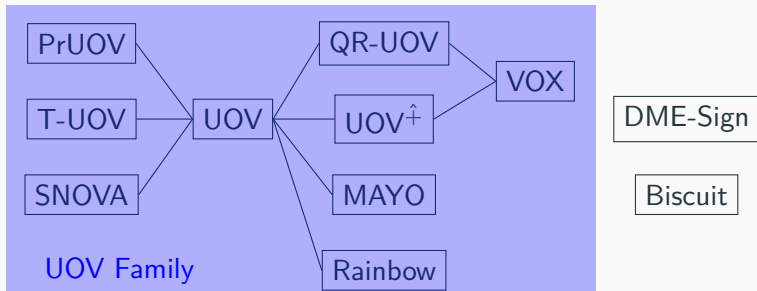
# Multivariate Post-Quantum Zoo at NIST



## The UOV family

- "Multi-layer structure": Rainbow

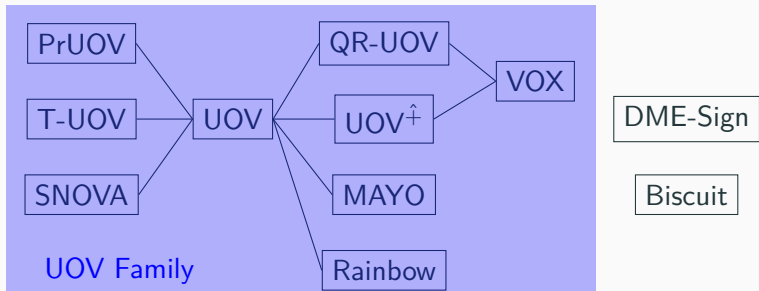
# Multivariate Post-Quantum Zoo at NIST



## The UOV family

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

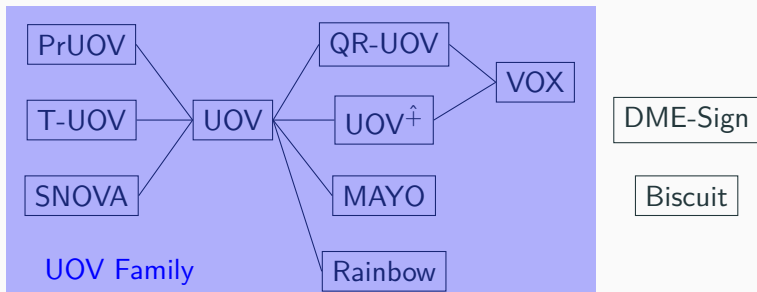
# Multivariate Post-Quantum Zoo at NIST



## The UOV family

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

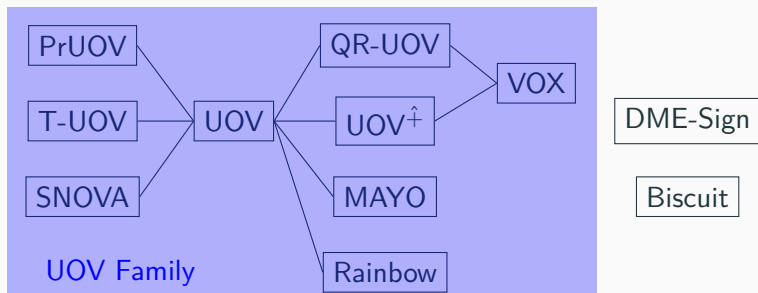
# Multivariate Post-Quantum Zoo at NIST



## 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