Cryptanalysis of multivariate signatures from a geometric point of view

Can you find a large linear subspace in an algebraic set?

Pierre Pébereau
Sorbonne Université, LIP6, CNRS, Thales SIX

April 25th, 2025

Motivation: Post Quantum Cryptography

Quantum Cryptanalysis

Since [Shor 1994], polynomial-time quantum algorithms for classical cryptographic problems.

Motivation: Post Quantum Cryptography

Quantum Cryptanalysis

Since [Shor 1994], polynomial-time quantum algorithms for classical cryptographic problems.

"Quantum-hard" problems for cryptography

- Finding short vectors in Euclidean lattices.
- Decoding error-correcting codes.
- Computing isogenies between elliptic curves.
- Solving systems of polynomial equations.

Motivation: Post Quantum Cryptography

Quantum Cryptanalysis

Since [Shor 1994], polynomial-time quantum algorithms for classical cryptographic problems.

"Quantum-hard" problems for cryptography

- Finding short vectors in Euclidean lattices.
- Decoding error-correcting codes.
- Computing isogenies between elliptic curves.
- Solving systems of polynomial equations.

NIST PQC Standardisation: Additional signatures

- Round 1: 11/40 schemes based on polynomial systems
- Round 2: 4/14 (UOV, MAYO, SNOVA, QR-UOV)

Main interest: **short** signatures and **fast** algorithms.

What is a signature scheme?

The signer picks λ and creates a pair public key $\mathcal{P}$, private key $\mathcal{S}$.

What is a signature scheme?

The signer picks λ and creates a pair public key $\mathcal{P}$, private key $\mathcal{S}$.

- Sign a message μ: $\textsf{sign}(\mathcal{S}, \mu) \to \sigma$.

What is a signature scheme?

The signer picks λ and creates a pair public key $\mathcal{P}$, private key $\mathcal{S}$.

- Sign a message μ: $\text{sign}(\mathcal{S}, \mu) \to \sigma$.
- Verify a signature: $\text{verify}(\mathcal{P}, \sigma, \mu) = \text{True/False}$.

What is a signature scheme?

The signer picks λ and creates a pair public key $\mathcal{P}$, private key $\mathcal{S}$.

- Sign a message μ: sign$(\mathcal{S}, \mu) \to \sigma$.
- Verify a signature: verify$(\mathcal{P}, \sigma, \mu) =$ True/False.
- Forge: signing without $\mathcal{S}$ requires $> 2^{\lambda}$ elementary operations.

Security level	I	III	V
λ	128	192	256

What is a signature scheme?

The signer picks λ and creates a pair public key $\mathcal{P}$, private key $\mathcal{S}$.

- Sign a message μ: sign$(\mathcal{S}, \mu) \to \sigma$.
- Verify a signature: verify$(\mathcal{P}, \sigma, \mu) =$ True/False.
- Forge: signing without $\mathcal{S}$ requires $> 2^\lambda$ elementary operations.

Security level	I	III	V
λ	128	192	256

Multivariate cryptography

- Public key: a polynomial map from $\mathbb{F}_q^n \mapsto \mathbb{F}_q^s$:
  $\boldsymbol{x} \mapsto \mathcal{P}(\boldsymbol{x}) = (p_1(\boldsymbol{x}), \ldots, p_s(\boldsymbol{x}))$

What is a signature scheme?

The signer picks λ and creates a pair public key $\mathcal{P}$, private key $\mathcal{S}$.

- Sign a message μ: sign$(\mathcal{S}, \mu) \to \sigma$.
- Verify a signature: verify$(\mathcal{P}, \sigma, \mu) =$ True/False.
- Forge: signing without $\mathcal{S}$ requires $> 2^\lambda$ elementary operations.

Security level	I	III	V
λ	128	192	256

Multivariate cryptography

- Public key: a polynomial map from $\mathbb{F}_q^n \mapsto \mathbb{F}_q^s$:
  $\boldsymbol{x} \mapsto \mathcal{P}(\boldsymbol{x}) = (p_1(\boldsymbol{x}), \ldots, p_s(\boldsymbol{x}))$
- Secret key: a way to find "preimages" $\boldsymbol{x} \in \mathbb{F}_q^n$ such that:
  $\mathcal{P}(\boldsymbol{x}) = \mathcal{H}(message)$

Crash course on polynomial systems

Algebra

The system $\mathcal{P}(\boldsymbol{x}) = 0$ generates an ideal $I = \langle p_1(\boldsymbol{x}), \ldots, p_s(\boldsymbol{x}) \rangle$

$$I := \{\sum_{i=1}^{s} a_i p_i(\boldsymbol{x}), (a_i) \in \mathbb{F}_q[\boldsymbol{x}]^s\}$$

$$I = \langle x^2 - y^2 z^2 + z^3 \rangle \in \mathbb{R}[x, y, z]$$

Crash course on polynomial systems

Algebra

The system $\mathcal{P}(\boldsymbol{x}) = 0$ generates an ideal $I = \langle p_1(\boldsymbol{x}), \ldots, p_s(\boldsymbol{x}) \rangle$

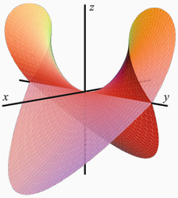
$$I := \{\textstyle\sum_{i=1}^{s} a_i p_i(\boldsymbol{x}), (a_i) \in \mathbb{F}_q[\boldsymbol{x}]^s\}$$

$$I = \langle x^2 - y^2 z^2 + z^3 \rangle \in \mathbb{R}[x, y, z]$$

Geometry

This ideal defines a variety

$$V(I) = \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^n, \forall p \in I, p(\boldsymbol{x}) = 0\}$$



$V(I)$ in $\mathbb{R}^3$
Image from [Cox, Little, O'Shea]

A key geometric property: dimension

Intuition of dimension from physics

$p_1(\boldsymbol{x}), \ldots, p_s(\boldsymbol{x})$: s "independant" constraints, n variables

$\implies n - s$ degrees of freedom in $V(I)$.

A key geometric property: dimension

Intuition of dimension from physics

$p_1(\boldsymbol{x}), \ldots, p_s(\boldsymbol{x})$: s "independant" constraints, n variables

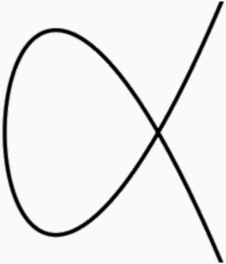
$\implies n - s$ degrees of freedom in $V(I)$.

This is correct if $p_1, \ldots, p_s$ is a regular sequence.

A key geometric property: dimension

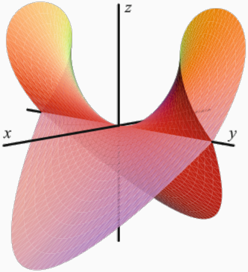
Intuition of dimension from physics

$p_1(\boldsymbol{x}), \ldots, p_s(\boldsymbol{x})$: s "independant" constraints, n variables
$\implies n - s$ degrees of freedom in $V(I)$.
This is correct if $p_1, \ldots, p_s$ is a regular sequence.



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

Figure 1: A curve has dimension 1



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

Figure 2: A hypersurface has dimension n-1

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

UOV Public key

Quadratic map $\mathcal{P}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^s$ generating $I = \langle p_1, \ldots, p_s \rangle$.

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

UOV Public key

Quadratic map $\mathcal{P}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^s$ generating $I = \langle p_1, \ldots, p_s \rangle$.

Private key (Algebraic point of view) [Patarin 1997]

- Quadratic map $\mathcal{F}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^s$ **linear** in $x_1, \ldots, x_s$.
- Linear change of variables A such that $\mathcal{P} = \mathcal{F} \circ A$.
- $x_1, \ldots, x_s$ are "oil variables", $x_{s+1}, \ldots, x_n$ "vinegar variables".

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

UOV Public key

Quadratic map $\mathcal{P}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^s$ generating $I = \langle p_1, \ldots, p_s \rangle$.

Private key (Algebraic point of view) [Patarin 1997]

- Quadratic map $\mathcal{F}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^s$ **linear** in $x_1, \ldots, x_s$.
- Linear change of variables A such that $\mathcal{P} = \mathcal{F} \circ A$.
- $x_1, \ldots, x_s$ are "oil variables", $x_{s+1}, \ldots, x_n$ "vinegar variables".

Private key (Geometric point of view) [Kipnis, Shamir 1998]

Linear subspace $\mathcal{S}$ of dimension s such that $\mathcal{S} \subset V(I)$

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

UOV Public key

Quadratic map $\mathcal{P}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^s$ generating $I = \langle p_1, \ldots, p_s \rangle$.

Private key (Algebraic point of view) [Patarin 1997]

- Quadratic map $\mathcal{F}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^s$ **linear** in $x_1, \ldots, x_s$.
- Linear change of variables A such that $\mathcal{P} = \mathcal{F} \circ A$.
- $x_1, \ldots, x_s$ are "oil variables", $x_{s+1}, \ldots, x_n$ "vinegar variables".

Private key (Geometric point of view) [Kipnis, Shamir 1998]

Linear subspace $\mathcal{S}$ of dimension s such that $\mathcal{S} \subset V(I)$

Observations

- First s columns of the secret matrix A^{-1} span $\mathcal{S}$.

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

UOV Public key

Quadratic map $\mathcal{P}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^s$ generating $I = \langle p_1, \ldots, p_s \rangle$.

Private key (Algebraic point of view) [Patarin 1997]

- Quadratic map $\mathcal{F}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^s$ **linear** in $x_1, \ldots, x_s$.
- Linear change of variables A such that $\mathcal{P} = \mathcal{F} \circ A$.
- $x_1, \ldots, x_s$ are "oil variables", $x_{s+1}, \ldots, x_n$ "vinegar variables".

Private key (Geometric point of view) [Kipnis, Shamir 1998]

Linear subspace $\mathcal{S}$ of dimension s such that $\mathcal{S} \subset V(I)$

Observations

- First s columns of the secret matrix A^{-1} span $\mathcal{S}$.
- $V(I)$ is a complete intersection if $n \geq 2s$.

Table of Contents

Objective: Find $\mathcal{S}$, the secret key.

Tangent space

Let $\mathrm{Jac}_{\mathcal{P}} := \begin{pmatrix} (\overrightarrow{\mathrm{grad}} p_1)^T \\ \vdots \\ (\overrightarrow{\mathrm{grad}} p_s)^T \end{pmatrix}$ and assume $I = \langle p_1, \ldots, p_s \rangle$ is radical.

Tangent space

$$\text{Let } \mathrm{Jac}_{\mathcal{P}} := \begin{pmatrix} (\overrightarrow{\mathrm{grad}} p_1)^T \\ \vdots \\ (\overrightarrow{\mathrm{grad}} p_s)^T \end{pmatrix} \text{ and assume } I = \langle p_1, \ldots, p_s \rangle \text{ is radical.}$$

Definition

$\boldsymbol{x} \in V(I)$ is regular if $\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x})$ is full rank.

Tangent space

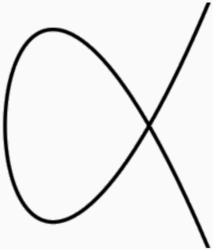
Let $\mathrm{Jac}_{\mathcal{P}} := \begin{pmatrix} (\overrightarrow{\mathrm{grad}} p_1)^T \\ \vdots \\ (\overrightarrow{\mathrm{grad}} p_s)^T \end{pmatrix}$ and assume $I = \langle p_1, \ldots, p_s \rangle$ is radical.

Definition

$\boldsymbol{x} \in V(I)$ is regular if $\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x})$ is full rank.

The tangent space of V at $\boldsymbol{x} \in V$ is

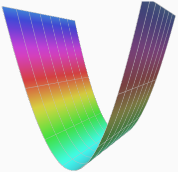
$$T_{\boldsymbol{x}} V := \ker_r(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}))$$



$y^2 - x^3 + 3x - 2 = 0$ in $\mathbb{R}^2$

Tangent spaces of the UOV variety

Goal: Distinguish points of $V(I) \setminus \mathcal{S}$ from points of $\mathcal{S}$.

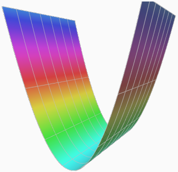


Geometric observation

A linear subspace is tangent to itself.

Tangent spaces of the UOV variety

Goal: Distinguish points of $V(I) \setminus \mathcal{S}$ from points of $\mathcal{S}$.



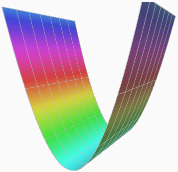
Geometric observation

A linear subspace is tangent to itself.

$$\forall \boldsymbol{x} \in \mathcal{S}, \mathcal{S} \subset T_{\boldsymbol{x}} V$$

Tangent spaces of the UOV variety

Goal: Distinguish points of $V(I) \setminus \mathcal{S}$ from points of $\mathcal{S}$.



Geometric observation

A linear subspace is tangent to itself.

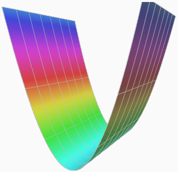
$$\forall \boldsymbol{x} \in \mathcal{S}, \mathcal{S} \subset T_{\boldsymbol{x}} V$$

Algorithm

Given $\boldsymbol{x} \in V$, compute $T_{\boldsymbol{x}} V$ and the matrices of $\mathcal{P}$ restricted to $T_{\boldsymbol{x}} V$. These matrices have low rank if $\boldsymbol{x} \in \mathcal{S}$.

Tangent spaces of the UOV variety

Goal: Distinguish points of $V(I) \setminus \mathcal{S}$ from points of $\mathcal{S}$.



Geometric observation

A linear subspace is tangent to itself.

$$\forall \boldsymbol{x} \in \mathcal{S}, \mathcal{S} \subset T_{\boldsymbol{x}} V$$

Algorithm

Given $\boldsymbol{x} \in V$, compute $T_{\boldsymbol{x}}V$ and the matrices of $\mathcal{P}$ restricted to $T_{\boldsymbol{x}}V$. These matrices have low rank if $\boldsymbol{x} \in \mathcal{S}$.

Computational approach

- With $B \in \mathbb{F}_q^{(n-s)\times n}$ a basis of $T_{\boldsymbol{x}}V$, restrict $\mathcal{P}$ to $T_{\boldsymbol{x}}V$:
  $\mathcal{P}_{|T_{\boldsymbol{x}}V}(\boldsymbol{y}) = (\boldsymbol{y}^T BP_1B^T \boldsymbol{y}, \ldots, \boldsymbol{y}^T BP_sB^T \boldsymbol{y})$

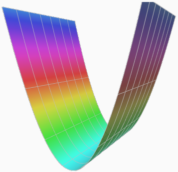
Tangent spaces of the UOV variety

Goal: Distinguish points of $V(I) \setminus \mathcal{S}$ from points of $\mathcal{S}$.

Geometric observation

A linear subspace is tangent to itself.

$$\forall \boldsymbol{x} \in \mathcal{S}, \mathcal{S} \subset T_{\boldsymbol{x}} V$$



Algorithm

Given $\boldsymbol{x} \in V$, compute $T_{\boldsymbol{x}} V$ and the matrices of $\mathcal{P}$ restricted to $T_{\boldsymbol{x}} V$. These matrices have low rank if $\boldsymbol{x} \in \mathcal{S}$.

Computational approach

- With $B \in \mathbb{F}_q^{(n-s)\times n}$ a basis of $T_{\boldsymbol{x}} V$, restrict $\mathcal{P}$ to $T_{\boldsymbol{x}} V$: $\mathcal{P}_{|T_{\boldsymbol{x}} V}(\boldsymbol{y}) = (\boldsymbol{y}^T B P_1 B^T \boldsymbol{y}, \ldots, \boldsymbol{y}^T B P_s B^T \boldsymbol{y})$
- Compute kernels of $B P_i B^T$, of large dimension if $\boldsymbol{x} \in \mathcal{S}$.

Consequence: One vector to rule them all

Main result: more than we bargained for **[P. 2024]**

Given **one vector** $x \in \mathcal{S}$ and $\mathcal{P}$, compute a basis of $\mathcal{S}$ in polynomial-time $O(sn^{\omega})$, $2 \leq \omega \leq 3$.

Consequence: One vector to rule them all

Main result: more than we bargained for [P. 2024]

Given **one vector** $x \in \mathcal{S}$ and $\mathcal{P}$, compute a basis of $\mathcal{S}$ in polynomial-time $O(sn^{\omega})$, $2 \leq \omega \leq 3$.

Security level n, s	I 112, 44	I 160, 64	III 184, 72	V 244, 96
Time	1.7s	4.4s	5.7s	13.3s

In practice with **SageMath** on my laptop (2.80GHz, 8GB RAM).

see also: [Aulbach, Campos, Krämer, Samardjiska, Stöttinger 2023]

Consequence: One vector to rule them all

Main result: more than we bargained for [P. 2024]

Given **one vector** $x \in \mathcal{S}$ and $\mathcal{P}$, compute a basis of $\mathcal{S}$ in polynomial-time $O(sn^{\omega})$, $2 \leq \omega \leq 3$.

Security level n, s	I 112, 44	I 160, 64	III 184, 72	V 244, 96
Time	1.7s	4.4s	5.7s	13.3s

In practice with **SageMath** on my laptop (2.80GHz, 8GB RAM).

Limit: locality of the UOV secret

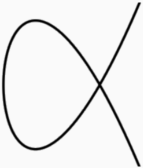
With this, the points of $V(I) \setminus \mathcal{S}$ give **no information** on $\mathcal{S}$.

see also: [Aulbach, Campos, Krämer, Samardjiska, Stöttinger 2023]

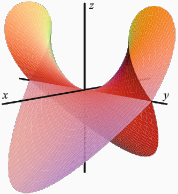
Table of Contents

Objective: Find $\mathcal{S}$, the secret key.

Singular points of $V(I)$ to find $\mathcal{S}$?

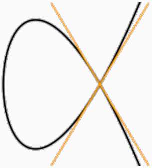


$y^2 = x^3 - 3x + 2$ in $\mathbb{R}^2$



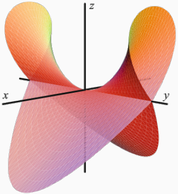
$x^2 - y^2z^2 + z^3$ in $\mathbb{R}^3$

Singular points of $V(I)$ to find $\mathcal{S}$?



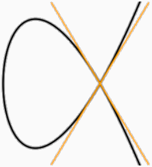
$y^2 = x^3 - 3x + 2$ in $\mathbb{R}^2$

Singular point: (1,0)

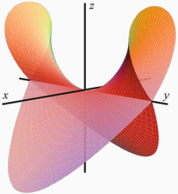


$x^2 - y^2z^2 + z^3$ in $\mathbb{R}^3$

Singular points of $V(I)$ to find $\mathcal{S}$?

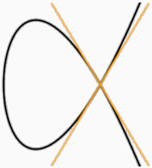


$y^2 = x^3 - 3x + 2$ in $\mathbb{R}^2$
Singular point: (1,0)

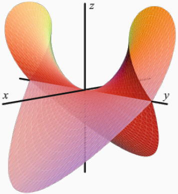


$x^2 - y^2z^2 + z^3$ in $\mathbb{R}^3$
Singular points: line (x=z=0)

Singular points of $V(I)$ to find $\mathcal{S}$?



$y^2 = x^3 - 3x + 2$ 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)

Definition

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

Structured equations yield a structured Jacobian

Algebraic private key **[Kipnis, Patarin, Goubin, 1999]**

Private key $\mathcal{F}$: s quadratic polynomials linear in $x_1, \ldots, x_s$.

Structured equations yield a structured Jacobian

Algebraic private key **[Kipnis, Patarin, Goubin, 1999]**

Private key $\mathcal{F}$: s quadratic polynomials linear in $x_1, \ldots, x_s$.

Secret Jacobian **[P. 2025]**

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

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

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

Structured equations yield a structured Jacobian

Algebraic private key **[Kipnis, Patarin, Goubin, 1999]**

Private key $\mathcal{F}$: s quadratic polynomials linear in $x_1, \ldots, x_s$.

Secret Jacobian **[P. 2025]**

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

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

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

Structured equations yield a structured Jacobian

Algebraic private key **[Kipnis, Patarin, Goubin, 1999]**

Private key $\mathcal{F}$: s quadratic polynomials linear in $x_1, \ldots, x_s$.

Secret Jacobian **[P. 2025]**

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

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

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

Dimension of the singular locus of V(I) **[P. 2025]**

$$\dim \mathrm{Sing}(V(I)) \geq 2\dim(\mathcal{S}) + s - n - 1$$

Locality of the UOV secret, bis

Secret Jacobian

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

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

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

Locality of the UOV secret, bis

Secret Jacobian

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

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

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

Intuition

Singular points $\iff$ Rank defects in the Jacobian.

- If J_2 is generic, rank defects should be caused **only** by J_1

Locality of the UOV secret, bis

Secret Jacobian

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

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

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

Intuition

Singular points $\iff$ Rank defects in the Jacobian.

- If J_2 is generic, rank defects should be caused **only** by J_1
- In other words, if $\mathcal{F}(\boldsymbol{x})$ is generic among UOV secret keys, singularities should be caused only by $\mathcal{S}$.

A genericity result on a non-generic object

Idea: compute $\mathcal{S} \subset V(I)$ by computing singularities of $V(I)$.

Problem: what if there are singularities that do not belong to $\mathcal{S}$?

1

A genericity result on a non-generic object

Idea: compute $\mathcal{S} \subset V(I)$ by computing singularities of $V(I)$.
Problem: what if there are singularities that do not belong to $\mathcal{S}$?

The right tool for the job

Generic varieties are smooth $\rightarrow$ generic points of $V(I)$ should be smooth for the same reason.

[1] This formulation is due to [Safey el Din, Schost 2016].

A genericity result on a non-generic object

Idea: compute $\mathcal{S} \subset V(I)$ by computing singularities of $V(I)$.

Problem: what if there are singularities that do not belong to $\mathcal{S}$?

The right tool for the job

Generic varieties are smooth $\rightarrow$ generic points of $V(I)$ should be smooth for the same reason.

Thom's weak transversality theorem (in characteristic 0)[1]

Consider $\Phi : \begin{cases} \mathbb{F}^n \times \mathbb{F}^d \rightarrow \mathbb{F}^s \\ \boldsymbol{x}, \mathcal{P} \mapsto \mathcal{P}(\boldsymbol{x}) \end{cases}$ and $\mathcal{O} \neq \emptyset$ a Zariski open set.

If Φ is **non-singular** on $\mathcal{O} \times \mathbb{F}^d$,

[1] This formulation is due to [Safey el Din, Schost 2016].

A genericity result on a non-generic object

Idea: compute $\mathcal{S} \subset V(I)$ by computing singularities of $V(I)$.
Problem: what if there are singularities that do not belong to $\mathcal{S}$?

The right tool for the job

Generic varieties are smooth $\rightarrow$ generic points of $V(I)$ should be smooth for the same reason.

Thom's weak transversality theorem (in characteristic 0)[1]

Consider $\Phi : \begin{cases} \mathbb{F}^n \times \mathbb{F}^d \rightarrow \mathbb{F}^s \\ \boldsymbol{x}, \mathcal{P} \mapsto \mathcal{P}(\boldsymbol{x}) \end{cases}$ and $\mathcal{O} \neq \emptyset$ a Zariski open set.

If Φ is **non-singular** on $\mathcal{O} \times \mathbb{F}^d$, then $\exists \mathcal{U} \neq \emptyset$ a Zariski open set

[1] This formulation is due to [Safey el Din, Schost 2016].

A genericity result on a non-generic object

Idea: compute $\mathcal{S} \subset V(I)$ by computing singularities of $V(I)$.

Problem: what if there are singularities that do not belong to $\mathcal{S}$?

The right tool for the job

Generic varieties are smooth $\to$ generic points of $V(I)$ should be smooth for the same reason.

Thom's weak transversality theorem (in characteristic 0)[1]

Consider $\Phi : \begin{cases} \mathbb{F}^n \times \mathbb{F}^d \to \mathbb{F}^s \\ \boldsymbol{x}, \mathcal{P} \mapsto \mathcal{P}(\boldsymbol{x}) \end{cases}$ and $\mathcal{O} \neq \emptyset$ a Zariski open set.

If Φ is **non-singular** on $\mathcal{O} \times \mathbb{F}^d$, then $\exists \mathcal{U} \neq \emptyset$ a Zariski open set such that for all $\mathcal{P} \in \mathcal{U}$, $\boldsymbol{x} \mapsto \mathcal{P}(\boldsymbol{x})$ is **non-singular** on $\mathcal{O}$.

[1] This formulation is due to [Safey el Din, Schost 2016].

Application to UOV

Thom's theorem

- Field of characteristic 0.

Our setting

- $\mathbb{F} = \mathbb{Q}$.

Application to UOV

Thom's theorem

- Field of characteristic 0.
- Φ smooth on an open $\mathcal{O}$.

Our setting

- $\mathbb{F} = \mathbb{Q}$.
- $\mathcal{O} = \mathcal{S}^c$.

Application to UOV

Thom's theorem

- Field of characteristic 0.
- Φ smooth on an open $\mathcal{O}$.

$\implies \mathcal{U} \subset \mathbb{Q}^d$, an open s.t.
$\forall \theta \in \mathcal{U}, \Phi_\theta$ smooth on $\mathcal{O}$.

Our setting

- $\mathbb{F} = \mathbb{Q}$.
- $\mathcal{O} = \mathcal{S}^c$.

$\implies \mathcal{U} \subset \mathbb{Q}^d$, an open s.t.
$\forall \theta \in \mathcal{U},\ V(I_\theta)$ smooth on $\mathcal{O}$.

Application to UOV

Thom's theorem

- Field of characteristic 0.
- Φ smooth on an open $\mathcal{O}$.

$\implies \mathcal{U} \subset \mathbb{Q}^d$, an open s.t. $\forall \theta \in \mathcal{U}, \Phi_\theta$ smooth on $\mathcal{O}$.

Our setting

- $\mathbb{F} = \mathbb{Q}$.
- $\mathcal{O} = \mathcal{S}^c$.

$\implies \mathcal{U} \subset \mathbb{Q}^d$, an open s.t. $\forall \theta \in \mathcal{U},\ V(I_\theta)$ smooth on $\mathcal{O}$.

Difficulty: lifting to positive characteristic.

Application to UOV

Thom's theorem

- Field of characteristic 0.
- Φ smooth on an open $\mathcal{O}$.

$\implies \mathcal{U} \subset \mathbb{Q}^d$, an open s.t. $\forall \theta \in \mathcal{U}, \Phi_\theta$ smooth on $\mathcal{O}$.

Our setting

- $\mathbb{F} = \mathbb{Q}$.
- $\mathcal{O} = \mathcal{S}^c$.

$\implies \mathcal{U} \subset \mathbb{Q}^d$, an open s.t. $\forall \theta \in \mathcal{U},\ V(I_\theta)$ smooth on $\mathcal{O}$.

Difficulty: lifting to positive characteristic.

Generic smoothness of a singular variety **[P. 2025]**

For a generic UOV variety, $\mathrm{Sing}(V(I)) \subset \mathcal{S}$ (in $\mathbb{Q}$ and $\mathbb{F}_p$, $p \gg 1$).

A good surprise in $\mathrm{Sing}(V(I))$

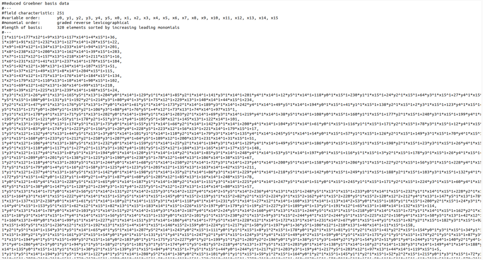
Gröbner basis of $\mathrm{Sing}\, V(I)$

The Gröbner bases we obtain are special: they contain linear polynomials defining $\mathcal{S}$.

A good surprise in $\mathrm{Sing}(V(I))$

Gröbner basis of $\mathrm{Sing}\,V(I)$

The Gröbner bases we obtain are special: they contain linear polynomials defining $\mathcal{S}$.



```
#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,
```

A good surprise in $\mathrm{Sing}(V(I))$

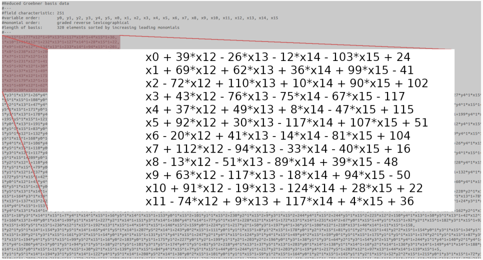
Gröbner basis of $\mathrm{Sing}\, V(I)$

The Gröbner bases we obtain are special: they contain linear polynomials defining $\mathcal{S}$.

```
#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,
```

Gröbner basis of Sing $V(I)$

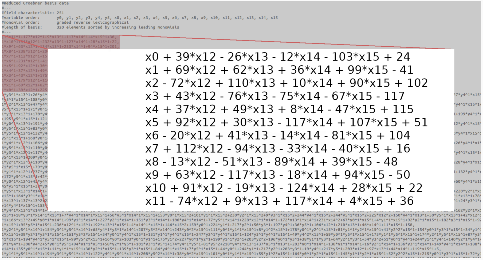
The Gröbner bases we obtain are special: they contain linear polynomials defining $\mathcal{S}$.



A good surprise in $\mathrm{Sing}(V(I))$

Gröbner basis of $\mathrm{Sing}\, V(I)$

The Gröbner bases we obtain are special: they contain linear polynomials defining $\mathcal{S}$.



Geometric interpretation

Even in small characteristic, $\mathrm{Sing}(V(I)) \cap \mathcal{S}$ is the component of highest dimension of $\mathrm{Sing}(V(I))$.

$\mathrm{Sing}(V(I))$ leaks the secret key

Key recovery attack targeting singular points

Previous Gröbner basis attack does not threaten current UOV parameters, due to the small field sizes.

$\mathrm{Sing}(V(I))$ leaks the secret key

Key recovery attack targeting singular points

Previous Gröbner basis attack does not threaten current UOV parameters, due to the small field sizes.

A history of targeting special points in $\mathcal{S}$

- **Oil and Vinegar**: invariant subspaces of the public key are always in $\mathcal{S}$ [Kipnis, Shamir 1998]

$\mathrm{Sing}(V(I))$ leaks the secret key

Key recovery attack targeting singular points

Previous Gröbner basis attack does not threaten current UOV parameters, due to the small field sizes.

A history of targeting special points in $\mathcal{S}$

- **Oil and Vinegar**: invariant subspaces of the public key are always in $\mathcal{S}$ [Kipnis, Shamir 1998]
- **Unbalanced Oil and Vinegar**: invariant subspaces of the public key are more likely in $\mathcal{S}$ [Kipnis, Patarin, Goubin 1999]

$\mathrm{Sing}(V(I))$ leaks the secret key

Key recovery attack targeting singular points

Previous Gröbner basis attack does not threaten current UOV parameters, due to the small field sizes.

A history of targeting special points in $\mathcal{S}$

- **Oil and Vinegar**: invariant subspaces of the public key are always in $\mathcal{S}$ [Kipnis, Shamir 1998]
- **Unbalanced Oil and Vinegar**: invariant subspaces of the public key are more likely in $\mathcal{S}$ [Kipnis, Patarin, Goubin 1999]

Geometric interpretation of an old attack **[P. 2025]**

[Kipnis-Shamir 1998] is a (hybrid) singular point computation.
Support heuristic analysis by relying on Thom's theorem and by estimating $|\mathrm{Sing}(V(I))|_{\mathbb{F}_q}$ with the Lang-Weil bound.

Table of Contents

Objective: Find $\mathcal{S}$, the secret key.

Hide $\mathcal{S}$ with the $\hat{+}$ perturbation

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

Start with a UOV secret key, replace $t \leq \mathbf{8}$ polynomials by random polynomials, and mix. $\mathcal{P} = \mathcal{R} \circ \mathcal{F} \circ A$

Idea: Tradeoff between signing time and key size.

Hide $\mathcal{S}$ with the $\hat{+}$ perturbation

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

Start with a UOV secret key, replace $t \leq \mathbf{8}$ polynomials by random polynomials, and mix. $\mathcal{P} = \mathcal{R} \circ \mathcal{F} \circ A$

Idea: Tradeoff between signing time and key size.

When t increases, signing time increases. $t = 0$ is UOV.

Hide $\mathcal{S}$ with the $\hat{+}$ perturbation

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

Start with a UOV secret key, replace $t \leq \mathbf{8}$ polynomials by random polynomials, and mix. $\mathcal{P} = \mathcal{R} \circ \mathcal{F} \circ A$

Idea: Tradeoff between signing time and key size.

When t increases, signing time increases. $t = 0$ is UOV.

Security assumption

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

Geometric interpretation of the $\hat{+}$ perturbation

$$\mathcal{P} = \mathcal{R} \circ \mathcal{F} \circ A$$

$$\mathcal{F} = (\underbrace{f_1, \ldots, f_t}_{\text{Random}}, \underbrace{f_{t+1}, \ldots, f_s}_{\text{UOV}})$$

Geometric interpretation of the $\hat{+}$ perturbation

$\mathcal{P} = \mathcal{R} \circ \mathcal{F} \circ A$

$$\mathcal{F} = (\underbrace{f_1, \dots, f_t}_{\text{Random}}, \underbrace{f_{t+1}, \dots, f_s}_{\text{UOV}})$$

Geometric interpretation

$V(I)$ is the intersection of a UOV variety with t generic quadrics.

$$J = \langle f_1, \dots, f_t \rangle$$

$$V(I) = \underbrace{V(J)}_{\text{Generic quadrics}} \cap \underbrace{V(\hat{\imath})}_{\text{UOV variety}}$$

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

Jacobian of $\mathcal{F}$ when $\boldsymbol{x} \in \mathcal{S}$:

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{cc} \left[\begin{array}{c|c} \multicolumn{2}{c}{J_1} \\ \hline 0 & J_2 \end{array}\right] & \begin{array}{c} t+1 \\ \vdots \\ s \end{array} \\ \begin{array}{cc} 1 \cdots\cdots s & s+1 \cdots\cdots\cdots\cdots n \end{array} & \end{array}$$

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

Jacobian of $\mathcal{F}$ when $\boldsymbol{x} \in \mathcal{S}$:

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{cc} \left[\begin{array}{c|c} \multicolumn{2}{c}{J_1} \\ \hline 0 & J_2 \end{array}\right] & \begin{array}{l} t+1 \\ \vdots \\ s \end{array} \\ 1 \cdots\cdots s \quad s+1 \cdots\cdots\cdots\cdots n & \end{array}$$

Observation

The singular locus of $V(I)$ contains $(\operatorname{Sing} V(\hat{\imath})) \cap V(J)$.

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

Jacobian of $\mathcal{F}$ when $\boldsymbol{x} \in \mathcal{S}$:

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{cc} \left[\begin{array}{c|c} \multicolumn{2}{c}{J_1} \\ \hline 0 & J_2 \end{array}\right] & \begin{array}{c} \\ t+1 \\ \vdots \\ s \end{array} \\ \begin{array}{cc} 1 \cdots\cdots s & s+1 \cdots\cdots\cdots\cdots n \end{array} & \end{array}$$

Observation

The singular locus of $V(I)$ contains $(\operatorname{Sing} V(\hat{\mathrm{i}})) \cap V(J)$.

Dimension computation [P. 2025]

$\hat{+}$ reduces the dimension of the singular locus by at most $\mathbf{2t}$.

From singular points to a key recovery attack

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(I)) \subset \mathrm{Sing}(V(\hat{\imath})) \subset \mathcal{S}$$

From singular points to a key recovery attack

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(I)) \subset \mathrm{Sing}(V(\hat{\imath})) \subset \mathcal{S}$$

Singular points of $V(I)$

$\approx q^{3s-2t-n-1}$ singular points of $V(I)$, and $\mathcal{P}(\boldsymbol{x}) = 0$.

From singular points to a key recovery attack

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(I)) \subset \mathrm{Sing}(V(\hat{\imath})) \subset \mathcal{S}$$

Singular points of $V(I)$

$\approx q^{3s-2t-n-1}$ singular points of $V(I)$, and $\mathcal{P}(\boldsymbol{x}) = 0$.

Expected cost: $O(q^{n-2s+2t} n^{\omega}) \rightarrow$ This is Kipnis-Shamir [KPG'99]

From singular points to a key recovery attack

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(I)) \subset \mathrm{Sing}(V(\hat{\imath})) \subset \mathcal{S}$$

Singular points of $V(I)$

$\approx q^{3s-2t-n-1}$ singular points of $V(I)$, and $\mathcal{P}(\boldsymbol{x}) = 0$.

Expected cost: $O(q^{n-2s+2t}n^{\omega}) \rightarrow$ This is Kipnis-Shamir [KPG'99]

Singular points of $V(\hat{\imath})$

$\approx q^{3s-\boldsymbol{t}-n-1}$ singular points of $V(\hat{\imath})$.

From singular points to a key recovery attack

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(I)) \subset \mathrm{Sing}(V(\hat{\imath})) \subset \mathcal{S}$$

Singular points of $V(I)$

$\approx q^{3s-2t-n-1}$ singular points of $V(I)$, and $\mathcal{P}(\boldsymbol{x}) = 0$.

Expected cost: $O(q^{n-2s+2t} n^{\omega}) \rightarrow$ This is Kipnis-Shamir [KPG'99]

Singular points of $V(\hat{\imath})$

$\approx q^{3s-\boldsymbol{t}-n-1}$ singular points of $V(\hat{\imath})$.

Expected number of trials: $O(q^{n-2s+\boldsymbol{t}})$ but $\mathcal{P}(\boldsymbol{x}) \neq 0$

From singular points to a key recovery attack

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(I)) \subset \mathrm{Sing}(V(\hat{\imath})) \subset \mathcal{S}$$

Singular points of $V(I)$

$\approx q^{3s-2t-n-1}$ singular points of $V(I)$, and $\mathcal{P}(\boldsymbol{x}) = 0$.

Expected cost: $O(q^{n-2s+2t} n^{\omega})$ $\rightarrow$ This is Kipnis-Shamir [KPG'99]

Singular points of $V(\hat{\imath})$

$\approx q^{3s-\boldsymbol{t}-n-1}$ singular points of $V(\hat{\imath})$.

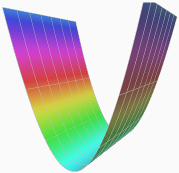
Expected number of trials: $O(q^{n-2s+\boldsymbol{t}})$ but $\mathcal{P}(\boldsymbol{x}) \neq 0$

$\rightarrow$ Can we decide $\boldsymbol{x} \in \mathcal{S}$ faster than $O(q^{t} n^{\omega})$?

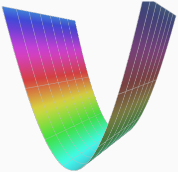
Adapting "$\boldsymbol{x} \in \mathcal{S}$?" to UOV$\hat{+}$ efficiently

Tangent spaces again

$\boldsymbol{x} \in \mathcal{S} \implies \mathcal{S} \cap T_{\boldsymbol{x}} V$ large dimension



Adapting “$\boldsymbol{x} \in \mathcal{S}$?” to UOV$\hat{+}$ efficiently



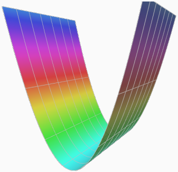
Tangent spaces again

$\boldsymbol{x} \in \mathcal{S} \implies \mathcal{S} \cap T_{\boldsymbol{x}} V$ large dimension

Restricting to an easier UOV$\hat{+}$ instance

$\mathcal{P}_{|T_x V}(\boldsymbol{x})$ is a UOV$\hat{+}$ instance with s **equations** but $n - s + 1$ **variables** and an $s - t$ dimensional UOV trapdoor.

Adapting “$\boldsymbol{x} \in \mathcal{S}$?” to UOV$\hat{+}$ efficiently



Tangent spaces again

$\boldsymbol{x} \in \mathcal{S} \implies \mathcal{S} \cap T_{\boldsymbol{x}} V$ large dimension

Restricting to an easier UOV$\hat{+}$ instance

$\mathcal{P}_{|T_x V}(\boldsymbol{x})$ is a UOV$\hat{+}$ instance with s **equations** but $n - s + 1$ **variables** and an $s - t$ dimensional UOV trapdoor.

Distinguisher

$\boldsymbol{x} \in \mathcal{S} \implies V(\mathcal{P}_{|T_x V}(\boldsymbol{x}))$ has constant codimension.

Solved in polynomial time.

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

$\boldsymbol{x} \in \mathcal{S}$? in polynomial time **[P. 2025]**

Decide $\boldsymbol{x} \in \mathcal{S}$? in $O(\binom{n-2s+2t-3}{4}^2\binom{n-2s+2t+1}{2})$.

2

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

$\boldsymbol{x} \in \mathcal{S}$? in polynomial time **[P. 2025]**

Decide $\boldsymbol{x} \in \mathcal{S}$? in $O(\binom{n-2s+2t-3}{4}^2\binom{n-2s+2t+1}{2})$.

Singular points attack and asymptotic result **[P. 2025]**

Singular points of $V(\hat{\imath})$ leak the trapdoor without inverting $\mathcal{R}$:

$$O(\underbrace{q^{n-2s+t}}_{\#\text{ trials}} \cdot \underbrace{\binom{n-2s+2t-3}{4}^2\binom{n-2s+2t+1}{2}}_{\text{Cost of each trial from } \boldsymbol{x}\in\mathcal{S}?})$$

2

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

$\boldsymbol{x} \in \mathcal{S}$? in polynomial time [P. 2025]

Decide $\boldsymbol{x} \in \mathcal{S}$? in $O(\binom{n-2s+2t-3}{4}^2\binom{n-2s+2t+1}{2})$.

Singular points attack and asymptotic result [P. 2025]

Singular points of $V(\hat{\imath})$ leak the trapdoor without inverting $\mathcal{R}$:

$$O(\underbrace{q^{n-2s+t}}_{\#\text{ trials}} \cdot \underbrace{\binom{n-2s+2t-3}{4}^2\binom{n-2s+2t+1}{2}}_{\text{Cost of each trial from } \boldsymbol{x}\in\mathcal{S}?})$$

Previous result [VOX][2]

This attack improves the Kipnis-Shamir attack which required:

$$O(q^{n-2s+\mathbf{2t}}n^{\omega})$$

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

Practical results and bit complexity

Parameters	I	III	V
$\log_2$ gates	39	41	43
Timing on my laptop	1.8s	5.5s	15.4s

Figure 3: $\boldsymbol{x} \in \mathcal{S}$? with msolve on $\mathrm{UOV}\hat{+}$.

Practical results and bit complexity

Parameters	I	III	V
$\log_2$ gates	39	41	43
Timing on my laptop	1.8s	5.5s	15.4s

Figure 3: $\boldsymbol{x} \in \mathcal{S}$? with msolve on UOV$\hat{+}$.

We add $\log_2(q) \times (n - 2s + t)$ to obtain the full cost:

Parameters	I	III	V
Security level ($\log_2$ gates)	143	207	272
Kipnis-Shamir ($\log_2$ gates)	166	233	313
This work ($\log_2$ gates)	**140**	**188**	**243**

Figure 4: Full attack on UOV$\hat{+}$.

Table of Contents

Objective: Find $\mathcal{S}$, the secret key.

How many equations characterize the secret?

Let $\delta(n, s, r) = (r+1)(n-r) - s\binom{r+2}{2}$

The Debarre and Manivel Bound[3] **[Debarre, Manivel 1998]**

Let X be a generic complete intersection of s quadrics of rank n.

[3] The original statement is for arbitrary degrees.

How many equations characterize the secret?

$$\text{Let } \delta(n, s, r) = (r+1)(n-r) - s\binom{r+2}{2}$$

The Debarre and Manivel Bound[3] [Debarre, Manivel 1998]

Let X be a generic complete intersection of s quadrics of rank n.

- If $\delta(n, s, r) < 0$, then X contains no (proj.) r-dimensional subspaces

[3] The original statement is for arbitrary degrees.

How many equations characterize the secret?

$$\text{Let } \delta(n,s,r) = (r+1)(n-r) - s\binom{r+2}{2}$$

The Debarre and Manivel Bound[3] **[Debarre, Manivel 1998]**

Let X be a generic complete intersection of s quadrics of rank n.

- If $\delta(n,s,r) < 0$, then X contains no (proj.) r-dimensional subspaces
- Otherwise, $\delta(n,s,r)$ is the dimension of the variety of linear spaces included in X.

[3] The original statement is for arbitrary degrees.

How many equations characterize the secret?

$$\text{Let } \delta(n,s,r) = (r+1)(n-r) - s\binom{r+2}{2}$$

The Debarre and Manivel Bound[3] [Debarre, Manivel 1998]

Let X be a generic complete intersection of s quadrics of rank n.

- If $\delta(n,s,r) < 0$, then X contains no (proj.) r-dimensional subspaces
- Otherwise, $\delta(n,s,r)$ is the dimension of the variety of linear spaces included in X.

Application to UOV

If $\alpha = \frac{n}{s}$ is a constant, then a UOV secret is characterized by a constant number of polynomials from the public key.

For practical parameters, 3 or 4 polynomials are enough.

[3] The original statement is for arbitrary degrees.

Applications to cryptanalysis

Two possible directions:

Solving underdetermined polynomial systems

Computing the largest subspace in generic complete intersections.

$\rightarrow$ improves forgery attacks against UOV.

Original key recovery attacks against UOV

Computing the smallest non-generic subspace in a UOV variety.

Generic application: How to solve underdetermined systems?

Task: Find one solution of $\mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q[x_1, \ldots, x_n]$

Generic application: How to solve underdetermined systems?

Task: Find one solution of $\mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q[x_1, \ldots, x_n]$

ⓐ Compute a subspace S of dimension $s - k$ such that $p_{1|S}, \ldots, p_{k|S} = 0$.

Generic application: How to solve underdetermined systems?

Task: Find one solution of $\mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q[x_1, \ldots, x_n]$

- (a) Compute a subspace S of dimension $s - k$ such that $p_{1|S}, \ldots, p_{k|S} = 0$.
- (b) Solve $\mathcal{P}_{|S}(\boldsymbol{x}) = 0$, a system of $s - k$ equations and variables.

Generic application: How to solve underdetermined systems?

Task: Find one solution of $\mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q[x_1, \ldots, x_n]$

- **a** Compute a subspace S of dimension $s - k$ such that $p_{1|S}, \ldots, p_{k|S} = 0$.
- **b** Solve $\mathcal{P}_{|S}(\boldsymbol{x}) = 0$, a system of $s - k$ equations and variables.

Algorithms using this approach for systems $\frac{n}{s} = \frac{5}{2}$

- [Thomae, Wolf 2012] step **a** in polynomial time for $k = 1$.
- (WIP) [Reid 72]: step **a** in prob. polynomial time for $k = 2$.

Generic application: How to solve underdetermined systems?

Task: Find one solution of $\mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q[x_1, \ldots, x_n]$

ⓐ Compute a subspace S of dimension $s - k$ such that $p_{1|S}, \ldots, p_{k|S} = 0$.

ⓑ Solve $\mathcal{P}_{|S}(\boldsymbol{x}) = 0$, a system of $s - k$ equations and variables.

Algorithms using this approach for systems $\frac{n}{s} = \frac{5}{2}$

- [Thomae, Wolf 2012] step **a** in polynomial time for $k = 1$.
- (WIP) [Reid 72]: step **a** in prob. polynomial time for $k = 2$.

Maximal precomputation

Debarre and Manivel: maximal possible value for k generically.

$$\frac{n}{s} = \frac{5}{2} \to k = 3.$$

Generic application: How to solve underdetermined systems?

Task: Find one solution of $\mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q[x_1, \ldots, x_n]$

- ⓐ Compute a subspace S of dimension $s - k$ such that $p_{1|S}, \ldots, p_{k|S} = 0$.
- ⓑ Solve $\mathcal{P}_{|S}(\boldsymbol{x}) = 0$, a system of $s - k$ equations and variables.

Algorithms using this approach for systems $\frac{n}{s} = \frac{5}{2}$

- [Thomae, Wolf 2012] step **a** in polynomial time for $k = 1$.
- (WIP) [Reid 72]: step **a** in prob. polynomial time for $k = 2$.

Maximal precomputation

Debarre and Manivel: maximal possible value for k generically.

$$\frac{n}{s} = \frac{5}{2} \rightarrow k = 3.$$

- Efficient algorithm for $k = 3$?

Generic application: How to solve underdetermined systems?

Task: Find one solution of $\mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q[x_1, \ldots, x_n]$

a. Compute a subspace S of dimension $s - k$ such that $p_{1|S}, \ldots, p_{k|S} = 0$.
b. Solve $\mathcal{P}_{|S}(\boldsymbol{x}) = 0$, a system of $s - k$ equations and variables.

Algorithms using this approach for systems $\frac{n}{s} = \frac{5}{2}$

- [Thomae, Wolf 2012] step **a** in polynomial time for $k = 1$.
- (WIP) [Reid 72]: step **a** in prob. polynomial time for $k = 2$.

Maximal precomputation

Debarre and Manivel: maximal possible value for k generically.

$$\frac{n}{s} = \frac{5}{2} \rightarrow k = 3.$$

- Efficient algorithm for $k = 3$?
- Does step **a** become more expensive than step **b**?

Analyzing our previous work through [DM98]

- Tangent spaces reveal information only if $\boldsymbol{x} \in \mathcal{S}$.

Analyzing our previous work through [DM98]

- Tangent spaces reveal information only if $\boldsymbol{x} \in \mathcal{S}$.
- Singular points are expensive to compute.

Analyzing our previous work through [DM98]

- Tangent spaces reveal information only if $\boldsymbol{x} \in \mathcal{S}$.
- Singular points are expensive to compute.
- Singular points require $\frac{m}{2} + 1$ polynomials: does not achieve the bound.

UOV application: Can we find a large linear subspace in a large variety? with S. Abelard and M. Safey el Din

$I = \langle p_1, p_2, p_3 \rangle$ and $\mathcal{S} \subset V(I)$, $\dim \mathcal{S} = s$, $\delta(n-1, s-1, 3) < 0$

UOV application: Can we find a large linear subspace in a large variety? with S. Abelard and M. Safey el Din

$I = \langle p_1, p_2, p_3 \rangle$ and $\mathcal{S} \subset V(I)$, $\dim \mathcal{S} = s$, $\delta(n-1, s-1, 3) < 0$

Polar varieties

Critical locus of the projection of $V(I)$ on well-chosen space Π.

UOV application: Can we find a large linear subspace in a large variety? with S. Abelard and M. Safey el Din

$I = \langle p_1, p_2, p_3 \rangle$ and $\mathcal{S} \subset V(I)$, $\dim \mathcal{S} = s$, $\delta(n-1, s-1, 3) < 0$

Polar varieties

Critical locus of the projection of $V(I)$ on well-chosen space Π.

Motivation: the degree of these varieties is controlled, which yields efficient algorithms.

UOV application: Can we find a large linear subspace in a large variety? with S. Abelard and M. Safey el Din

$I = \langle p_1, p_2, p_3 \rangle$ and $\mathcal{S} \subset V(I)$, $\dim \mathcal{S} = s$, $\delta(n-1, s-1, 3) < 0$

Polar varieties

Critical locus of the projection of $V(I)$ on well-chosen space Π.

Motivation: the degree of these varieties is controlled, which yields efficient algorithms.

Challenge

How to choose Π so that it is easy to compute the polar variety when $\mathcal{S}$ is unknown?

$\rightarrow$ Easy to distinguish UOV from generic systems with polar varieties... when $\mathcal{S}$ is known.

Thank you for your attention!

One vector to full key recovery in polynomial time PQC '24

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

Singular points of UOV and UOV$\hat{+}$ Eurocrypt '25

- $V(I)$ has a large singular locus.
- Singular points of UOV$\hat{+}$ yield faster attacks.
- Key recovery from one vector for UOV$\hat{+}$ in polynomial time.

Future/On-going work

Find efficient algorithms to achieve the Debarre and Manivel bound.

- In the generic case, as a precomputation for solving systems.
- In the UOV case, as key recovery attacks.

Proposed UOV$\hat{+}$ parameters

Level	q, o, v, t	epk gain vs UOV
I	251, 48, 55, 6	36%
III	1021, 70, 79, 7	44%
V	4093, 96, 107, 8	27%

Table of Contents

Quotient Ring UOV [Furue, Ikematsu, Kiyomura, Takagi '21]

The Quotient Ring transform

- Generate a UOV(q^ℓ, m, n) key with ℓs equations.

Quotient Ring UOV [Furue, Ikematsu, Kiyomura, Takagi '21]

The Quotient Ring transform

- Generate a UOV(q^ℓ, m, n) key with ℓs equations.
- Represent it in $\mathbb{F}_q$ via a quotient $\mathbb{F}_{q^\ell} \cong \mathbb{F}_q[x]/\langle f \rangle$.

Quotient Ring UOV [Furue, Ikematsu, Kiyomura, Takagi '21]

The Quotient Ring transform

- Generate a UOV(q^ℓ, m, n) key with ℓs equations.
- Represent it in $\mathbb{F}_q$ via a quotient $\mathbb{F}_{q^\ell} \cong \mathbb{F}_q[x]/\langle f \rangle$.
- This is a (non-generic) UOV instance for parameters $q, \ell m, \ell n$.

Quotient Ring UOV [Furue, Ikematsu, Kiyomura, Takagi '21]

The Quotient Ring transform

- Generate a $\mathrm{UOV}(q^\ell, m, n)$ key with ℓs equations.
- Represent it in $\mathbb{F}_q$ via a quotient $\mathbb{F}_{q^\ell} \cong \mathbb{F}_q[x]/\langle f \rangle$.
- This is a (non-generic) UOV instance for parameters $q, \ell m, \ell n$.
- Secure only if $\mathrm{UOV}(q^\ell, m, n, \ell m)$ **and** $\mathrm{UOV}(q, \ell m, \ell n)$ are.

Quotient Ring UOV [Furue, Ikematsu, Kiyomura, Takagi '21]

The Quotient Ring transform

- Generate a $\mathrm{UOV}(q^\ell, m, n)$ key with ℓs equations.
- Represent it in $\mathbb{F}_q$ via a quotient $\mathbb{F}_{q^\ell} \cong \mathbb{F}_q[x]/\langle f \rangle$.
- This is a (non-generic) UOV instance for parameters $q, \ell m, \ell n$.
- Secure only if $\mathrm{UOV}(q^\ell, m, n, \ell m)$ **and** $\mathrm{UOV}(q, \ell m, \ell n)$ are.

VOX: QR-UOV$\hat{+}$

$$\mathrm{UOV}\hat{+}(q^\ell, m/\ell, n/\ell, m, t) \xrightarrow[\mathrm{QR}]{} \mathrm{UOV}\hat{+}(q, m, n, t).$$

Quotient Ring UOV [Furue, Ikematsu, Kiyomura, Takagi '21]

The Quotient Ring transform

- Generate a UOV(q^ℓ, m, n) key with ℓs equations.
- Represent it in $\mathbb{F}_q$ via a quotient $\mathbb{F}_{q^\ell} \cong \mathbb{F}_q[x]/\langle f \rangle$.
- This is a (non-generic) UOV instance for parameters $q, \ell m, \ell n$.
- Secure only if UOV($q^\ell, m, n, \ell m$) **and** UOV($q, \ell m, \ell n$) are.

VOX: QR-UOV$\hat{+}$

$$\mathrm{UOV}\hat{+}(q^\ell, m/\ell, n/\ell, m, t) \xrightarrow[\mathrm{QR}]{} \mathrm{UOV}\hat{+}(q, m, n, t).$$

MinRank attacks on the big field instance of VOX

- Initial parameters are not secure [Furue, Ikematsu 2023]
- Practical attack on all new parameters [Guo, Ding 2024]

Practical attack on VOX

Dimension computation

$\mathrm{UOV}\hat{+}(q^\ell, m/\ell, n/\ell, m, t)$ defines a **variety that contains** $\mathcal{S}_t$ but it should be the empty variety for a generic system.

Practical attack on VOX

Dimension computation

$\mathrm{UOV}\hat{+}(q^\ell, m/\ell, n/\ell, m, t)$ defines a **variety that contains** $\mathcal{S}_t$ but it should be the empty variety for a generic system.

Subfield attack [P. 2024b]

Practical key recovery attack on the big field instance and use of subfields $\mathbb{F}_{q^{\ell'}} \subset \mathbb{F}_{q^\ell}$ to attack a subset of new parameters.

Practical attack on VOX

Dimension computation

UOV$\hat{+}(q^\ell, m/\ell, n/\ell, m, t)$ defines a **variety that contains** $\mathcal{S}_t$ but it should be the empty variety for a generic system.

Subfield attack [P. 2024b]

Practical key recovery attack on the big field instance and use of subfields $\mathbb{F}_{q^{\ell'}} \subset \mathbb{F}_{q^\ell}$ to attack a subset of new parameters.

Parameters	I	Ic	III	IIIa	V	Vb
ℓ	6	9	7	15	8	14
ℓ'	6	3	7	5	8	7
time	0.29s	2^{67}gates[4]	1.35s	56.7s	0.56s	6.11s

Figure 5: Timing for the subfield attack on QR-UOV$\hat{+}$ on my laptop.

[4] 400 CPU-hours on a server in practice.