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

Séminaire Cryptographie de l'ANSSI
May 28th, 2025

Context: Post Quantum Cryptography

“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.

Context: Post Quantum Cryptography

"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 features: **short** signatures and **fast** algorithms.

What is a signature scheme?

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

Crash course on cryptography

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: $\text{sign}(\mathcal{S}, \mu) \to \sigma$.

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

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

Security level [1]	I	III	V
λ	143	207	272

[1] also referred to/defined with $\ell \in \{128, 192, 256\}$: "at least as hard to break as AES-ℓ".

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 [1]	I	III	V
λ	143	207	272

Applications

SSH, TLS, Software signing, ...

[1] also referred to/defined with $\ell \in \{128, 192, 256\}$: "at least as hard to break as AES-ℓ".

Polynomial systems in cryptology

Multivariate cryptography

Using multivariate polynomial systems to build cryptography.

Polynomial systems in cryptology

Multivariate cryptography

Using multivariate polynomial systems to build cryptography.

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

Polynomial systems in cryptology

Multivariate cryptography

Using multivariate polynomial systems to build cryptography.

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

Polynomial systems in cryptology

Multivariate cryptography

Using multivariate polynomial systems to build cryptography.

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

Algebraic cryptanalysis

Solving polynomial systems to attack cryptography.

Polynomial systems in cryptology

Multivariate cryptography

Using multivariate polynomial systems to build cryptography.

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

Algebraic cryptanalysis

Solving polynomial systems to attack cryptography.

- Using algorithms such as F4, F5, XL, SAT solvers, ...

Polynomial systems in cryptology

Multivariate cryptography

Using multivariate polynomial systems to build cryptography.

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

Algebraic cryptanalysis

Solving polynomial systems to attack cryptography.

- Using algorithms such as F4, F5, XL, SAT solvers, ...
- Targeting many families: symmetric, lattices, codes, multivariate, ...

Crash course on polynomial systems

Algebra

The system $\mathcal{P}(\boldsymbol{x}) = 0$ generates an ideal

$I = \langle p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x}) \rangle$

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

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

Algebra

The system $\mathcal{P}(\boldsymbol{x}) = 0$ generates an ideal

$I = \langle p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x}) \rangle$

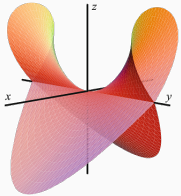
$$I := \{\sum_{i=1}^{s} a_i p_i(\boldsymbol{x}), (a_i) \in \mathbb{F}_q[\boldsymbol{x}]^s\}$$

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

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[2] of dimension from physics

$p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x})$: m “independent” constraints, n variables
$\implies n - m$ degrees of freedom in $V(I)$.

[2] This is correct if $p_1, \ldots, p_m$ is a regular sequence.

A key geometric property: dimension

Intuition[2] of dimension from physics

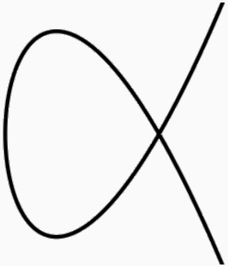
$p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x})$: m "independent" constraints, n variables
$\implies n - m$ degrees of freedom in $V(I)$.

[2] This is correct if $p_1, \ldots, p_m$ is a regular sequence.

A key geometric property: dimension

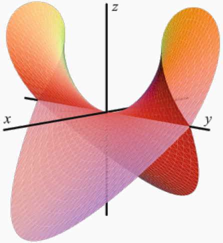
Intuition[2] of dimension from physics

$p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x})$: m "independent" constraints, n variables
$\Longrightarrow n - m$ degrees of freedom in $V(I)$.



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

Figure 1: A curve has dimension 1



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

Figure 2: A hypersurface has dimension n-1

[2]This is correct if $p_1, \ldots, p_m$ is a regular sequence.

UOV Public key

Quadratic map $\mathcal{P}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ generating $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$, with $n > 2m$.

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

UOV Public key

Quadratic map $\mathcal{P}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ generating $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$, with $n > 2m$.

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

- Quadratic map $\mathcal{F}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ **linear** in $x_1, \ldots, x_o$ (*oil variables*).
- Linear change of variables $A \in GL_n(\mathbb{F}_q)$ such that $\mathcal{P} = \mathcal{F} \circ A$.

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

UOV Public key

Quadratic map $\mathcal{P}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ generating $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$, with $n > 2m$.

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

- Quadratic map $\mathcal{F}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ **linear** in $x_1, \ldots, x_o$ (*oil variables*).
- Linear change of variables $A \in GL_n(\mathbb{F}_q)$ such that $\mathcal{P} = \mathcal{F} \circ A$.

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

Linear subspace $\mathcal{O}$ of dimension o such that $\mathcal{O} \subset V(\mathcal{I})$.

UOV Public key

Quadratic map $\mathcal{P}(\mathbf{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ generating $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$, with $n > 2m$.

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

- Quadratic map $\mathcal{F}(\mathbf{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ **linear** in $x_1, \ldots, x_o$ (*oil variables*).
- Linear change of variables $A \in GL_n(\mathbb{F}_q)$ such that $\mathcal{P} = \mathcal{F} \circ A$.

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

Linear subspace $\mathcal{O}$ of dimension o such that $\mathcal{O} \subset V(\mathcal{I})$.

Observations

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

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

UOV Public key

Quadratic map $\mathcal{P}(\mathbf{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ generating $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$, with $n > 2m$.

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

- Quadratic map $\mathcal{F}(\mathbf{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ **linear** in $x_1, \ldots, x_o$ (*oil variables*).
- Linear change of variables $A \in GL_n(\mathbb{F}_q)$ such that $\mathcal{P} = \mathcal{F} \circ A$.

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

Linear subspace $\mathcal{O}$ of dimension o such that $\mathcal{O} \subset V(\mathcal{I})$.

Observations

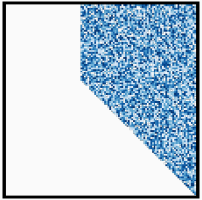
- First o columns of the secret matrix A^{-1} span $\mathcal{O}$.
- In UOV, $o = m$, but not always the case in variants.

Representing UOV keys

UOV keys are quadratic forms

$$\mathcal{F}(\boldsymbol{x}) = \boldsymbol{x}^T F_1 \boldsymbol{x}, \ldots, \boldsymbol{x}^T F_m \boldsymbol{x} \qquad \mathcal{P}(\boldsymbol{x}) = \boldsymbol{x}^T P_1 \boldsymbol{x}, \ldots, \boldsymbol{x}^T P_m \boldsymbol{x}$$

$$\forall 1 \leq i \leq m, P_i = A^T F_i A$$



$F_1 \in (\mathbb{F}_{257})^{n \times n}$

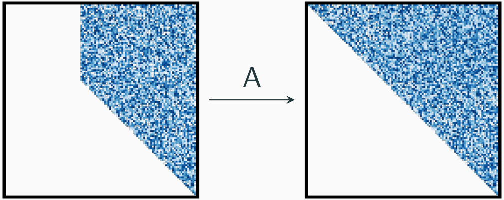
Figure 3: UOV polynomial pair in $\mathbb{F}_{257}$

Representing UOV keys

UOV keys are quadratic forms

$$\mathcal{F}(\boldsymbol{x}) = \boldsymbol{x}^T F_1 \boldsymbol{x}, \dots, \boldsymbol{x}^T F_m \boldsymbol{x} \qquad \mathcal{P}(\boldsymbol{x}) = \boldsymbol{x}^T P_1 \boldsymbol{x}, \dots, \boldsymbol{x}^T P_m \boldsymbol{x}$$

$$\forall 1 \leq i \leq m, P_i = A^T F_i A$$



$F_1 \in (\mathbb{F}_{257})^{n \times n}$ $\qquad$ $P_1 \in (\mathbb{F}_{257})^{n \times n}$

Figure 3: UOV polynomial pair in $\mathbb{F}_{257}$

Signing

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

$\mathcal{P}(A^{-1}\boldsymbol{x})$ is linear in the oil variables and quadratic in the vinegar variables.

Signing

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

$\mathcal{P}(A^{-1}\boldsymbol{x})$ is linear in the oil variables and quadratic in the vinegar variables.

Signing with the secret key

Forging without the secret key

Signing

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

$\mathcal{P}(A^{-1}\boldsymbol{x})$ is linear in the oil variables and quadratic in the vinegar variables.

Signing with the secret key

- Draw $x_{o+1}, \ldots, x_n \leftarrow_\$ \mathbb{F}_q$.

Forging without the secret key

- Draw $y_{m+1}, \ldots, y_n \leftarrow_\$ \mathbb{F}_q$.

Signing

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

$\mathcal{P}(A^{-1}\boldsymbol{x})$ is linear in the oil variables and quadratic in the vinegar variables.

Signing with the secret key

- Draw $x_{o+1}, \dots, x_n \leftarrow_{\$} \mathbb{F}_q$.
- Solve a linear system $\mathcal{P}(A^{-1}\boldsymbol{x}) = \boldsymbol{t}$.

Forging without the secret key

- Draw $y_{m+1}, \dots, y_n \leftarrow_{\$} \mathbb{F}_q$.
- Solve a quadratic system $\mathcal{P}(\boldsymbol{y}) = \boldsymbol{t}$.

Signing

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

$\mathcal{P}(A^{-1}\boldsymbol{x})$ is linear in the oil variables and quadratic in the vinegar variables.

Signing with the secret key

- Draw $x_{o+1}, \ldots, x_n \leftarrow_\$ \mathbb{F}_q$.
- Solve a linear system $\mathcal{P}(A^{-1}\boldsymbol{x}) = \boldsymbol{t}$.
- Return $\boldsymbol{y} = A^{-1}\boldsymbol{x}$.

Forging without the secret key

- Draw $y_{m+1}, \ldots, y_n \leftarrow_\$ \mathbb{F}_q$.
- Solve a quadratic system $\mathcal{P}(\boldsymbol{y}) = \boldsymbol{t}$.
- Return $\boldsymbol{y}$.

Signing

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

$\mathcal{P}(A^{-1}\boldsymbol{x})$ is linear in the oil variables and quadratic in the vinegar variables.

Signing with the secret key

- Draw $x_{o+1}, \ldots, x_n \leftarrow_\$ \mathbb{F}_q$.
- Solve a linear system $\mathcal{P}(A^{-1}\boldsymbol{x}) = \boldsymbol{t}$.
- Return $\boldsymbol{y} = A^{-1}\boldsymbol{x}$.

$$O(n^\omega), \quad 2 \leq \omega < 3$$

Forging without the secret key

- Draw $y_{m+1}, \ldots, y_n \leftarrow_\$ \mathbb{F}_q$.
- Solve a quadratic system $\mathcal{P}(\boldsymbol{y}) = \boldsymbol{t}$.
- Return $\boldsymbol{y}$.

$$O(q^m)$$

Table of Contents

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

Tangent space

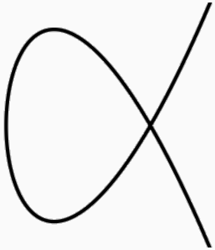
Let $\mathrm{Jac}_{\mathcal{P}} := \begin{pmatrix} (\overrightarrow{\mathrm{grad}} p_1)^T \\ \vdots \\ (\overrightarrow{\mathrm{grad}} p_m)^T \end{pmatrix}$ and assume $I = \langle p_1, \ldots, p_m \rangle$ is radical.

Tangent space

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

Definition

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



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

Tangent space

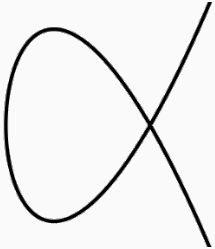
$$\text{Let } \mathrm{Jac}_{\mathcal{P}} := \begin{pmatrix} (\overrightarrow{\mathrm{grad}} p_1)^T \\ \vdots \\ (\overrightarrow{\mathrm{grad}} p_m)^T \end{pmatrix} \text{ and assume } I = \langle p_1, \ldots, p_m \rangle \text{ is radical.}$$

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

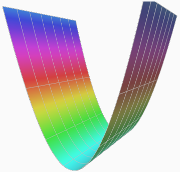
$$T_{\boldsymbol{x}} V := \ker_r(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}))$$



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

Tangent spaces of the UOV variety

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

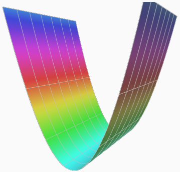


Geometric observation

A linear subspace is tangent to itself.

Tangent spaces of the UOV variety

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



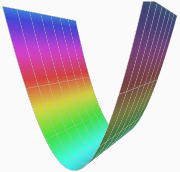
Geometric observation

A linear subspace is tangent to itself.

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

Tangent spaces of the UOV variety

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



Geometric observation

A linear subspace is tangent to itself.

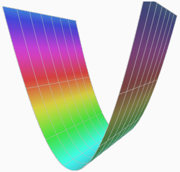
$$\forall \boldsymbol{x} \in \mathcal{O}, \mathcal{O} \subset T_{\boldsymbol{x}} V$$

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 $\boldsymbol{x} \in \mathcal{O}$.

Tangent spaces of the UOV variety

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



Geometric observation

A linear subspace is tangent to itself.

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

Algorithm

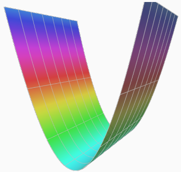
Given $\boldsymbol{x} \in V$, compute $T_{\boldsymbol{x}} V$ and the matrices of $\mathcal{P}$ restricted to $T_{\boldsymbol{x}} V$. These matrices have low rank if $\boldsymbol{x} \in \mathcal{O}$.

Computational approach

- With $B \in \mathbb{F}_q^{(n-s)\times n}$ a basis of $T_{\boldsymbol{x}} V$, restrict $\mathcal{P}$ to $T_{\boldsymbol{x}} V$:
  $\mathcal{P}_{|T_{\boldsymbol{x}} V}(\boldsymbol{y}) = (\boldsymbol{y}^T B P_1 B^T \boldsymbol{y}, \ldots, \boldsymbol{y}^T B P_m B^T \boldsymbol{y})$

Tangent spaces of the UOV variety

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



Geometric observation

A linear subspace is tangent to itself.

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

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 $\boldsymbol{x} \in \mathcal{O}$.

Computational approach

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

Consequence: One vector to rule them all

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

Given **one vector** $x \in \mathcal{O}$ and $\mathcal{P}$, compute a basis of $\mathcal{O}$ in polynomial-time $O(mn^{\omega})$, where $2 \leq \omega \leq 3$ is the exponent of matrix multiplication.

Consequence: One vector to rule them all

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

Given **one vector** $x \in \mathcal{O}$ and $\mathcal{P}$, compute a basis of $\mathcal{O}$ in polynomial-time $O(mn^{\omega})$, where $2 \leq \omega \leq 3$ is the exponent of matrix multiplication.

Security level n, m	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** $x \in \mathcal{O}$ and $\mathcal{P}$, compute a basis of $\mathcal{O}$ in polynomial-time $O(mn^{\omega})$, where $2 \leq \omega \leq 3$ is the exponent of matrix multiplication.

Security level n, m	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 $V(I) \setminus \mathcal{O}$ give **no information** on $\mathcal{O}$.

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

Table of Contents

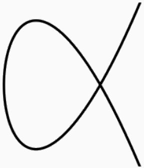
Objective: Find $\mathcal{O}$, the secret key.

Singular points

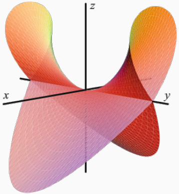
Let $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ be a radical ideal of codimension m.

Definition (Tangent space at a regular point)

The tangent space of V at $\boldsymbol{x} \in V$ is $T_{\boldsymbol{x}} V := \ker_r(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}))$



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



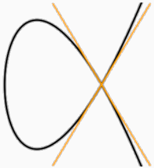
$x^2 - y^2 z^2 + z^3 = 0$ in $\mathbb{R}^3$

Singular points

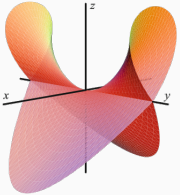
Let $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ be a radical ideal of codimension m.

Definition (Tangent space at a regular point)

The tangent space of V at $\boldsymbol{x} \in V$ is $T_{\boldsymbol{x}} V := \ker_r(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}))$



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



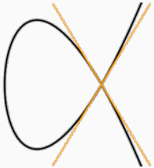
$x^2 - y^2 z^2 + z^3 = 0$ in $\mathbb{R}^3$

Singular points

Let $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ be a radical ideal of codimension m.

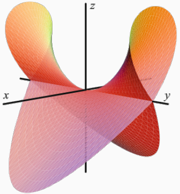
Definition (Tangent space at a regular point)

The tangent space of V at $\boldsymbol{x} \in V$ is $T_{\boldsymbol{x}} V := \ker_r(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}))$



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

Singular point: (1,0)



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

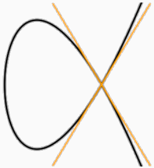
Singular points: line (x=z=0)

Singular points

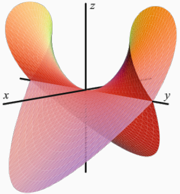
Let $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ be a radical ideal of codimension m.

Definition (Tangent space at a regular point)

The tangent space of V at $\boldsymbol{x} \in V$ is $T_{\boldsymbol{x}} V := \ker_r(\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}))$



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



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

Definition (Singular points)

$\boldsymbol{x} \in V(\mathcal{I}) \setminus \{0\}$ is singular if $\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x})$ has rank less than m.

Structured equations yield a structured Jacobian

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

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

Structured equations yield a structured Jacobian

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

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

Secret Jacobian [P. 2025]

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \left[\begin{array}{c|c} J_1 & J_2 \end{array}\right]$$

$$1 \cdots\cdots o \quad o+1 \cdots\cdots\cdots\cdots n$$

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

Structured equations yield a structured Jacobian

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

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

Secret Jacobian [P. 2025]

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

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

$$1 \cdots\cdots o \quad o+1 \cdots\cdots\cdots n$$

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

Structured equations yield a structured Jacobian

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

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

Secret Jacobian [P. 2025]

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

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

$$1 \cdots\cdots o \quad o+1 \cdots\cdots\cdots\cdots n$$

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

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

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

An algebraic attack targeting singular points

Generic smoothness of a singular variety [P. 2025]

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

In other words, the singular points we have counted are expected to be the only ones.

An algebraic attack targeting singular points

Generic smoothness of a singular variety [P. 2025]

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

In other words, the singular points we have counted are expected to be the only ones.

Polynomial system solving

Compute singular points by solving a polynomial system using a Gröbner basis: an equivalent polynomial system that is easy to solve, but hard to find.

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 $\mathcal{O}$.

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

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


```
#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 $\mathrm{Sing}\,V(I)$

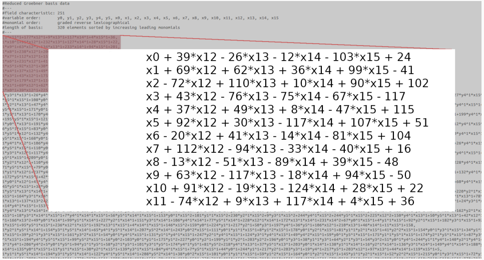
The Gröbner bases we obtain are special: they contain linear polynomials defining $\mathcal{O}$.

```
#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 $\mathrm{Sing}\,V(I)$

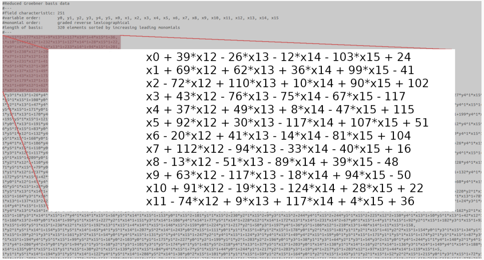
The Gröbner bases we obtain are special: they contain linear polynomials defining $\mathcal{O}$.



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 $\mathcal{O}$.



Geometric interpretation when p is too small for genericity

$\mathrm{Sing}(V(I)) \cap \mathcal{O}$ is the component of highest dimension of $\mathrm{Sing}(V(I))$.

Spoiler: this algorithm is too expensive to threaten UOV.

The Kipnis-Shamir attack against (U)OV

From quadratic forms to linear algebra **[Kipnis-Shamir 1998]**

If $n = 2m$, then $\mathcal{O}$ is an invariant subspace of $P_i^{-1}P_j$. Poly-time cryptanalysis.

The Kipnis-Shamir attack against (U)OV

From quadratic forms to linear algebra **[Kipnis-Shamir 1998]**

If $n = 2m$, then $\mathcal{O}$ is an invariant subspace of $P_i^{-1}P_j$. Poly-time cryptanalysis.

Generalisation to UOV **[Kipnis, Patarin, Goubin 1999]**

$\boldsymbol{x} \in \mathcal{O}$ is an eigenvector of $P_m^{-1} \sum_{i=1}^{m-1} y_i P_i$ with probability $\approx q^{2m-n}$. Exp-time.

The Kipnis-Shamir attack against (U)OV

From quadratic forms to linear algebra [Kipnis-Shamir 1998]

If $n = 2m$, then $\mathcal{O}$ is an invariant subspace of $P_i^{-1}P_j$. Poly-time cryptanalysis.

Generalisation to UOV [Kipnis, Patarin, Goubin 1999]

$\boldsymbol{x} \in \mathcal{O}$ is an eigenvector of $P_m^{-1}\sum_{i=1}^{m-1} y_i P_i$ with probability $\approx q^{2m-n}$. Exp-time.

Previous work

[KS'98] computes singular points of the intersection of two quadrics. [Luyten '23]

[KPG'99] computes singular points of $V(\mathcal{I})$. Beullens, Castryck '23

The Kipnis-Shamir attack against (U)OV

From quadratic forms to linear algebra [Kipnis-Shamir 1998]

If $n = 2m$, then $\mathcal{O}$ is an invariant subspace of $P_i^{-1}P_j$. Poly-time cryptanalysis.

Generalisation to UOV [Kipnis, Patarin, Goubin 1999]

$\boldsymbol{x} \in \mathcal{O}$ is an eigenvector of $P_m^{-1} \sum_{i=1}^{m-1} y_i P_i$ with probability $\approx q^{2m-n}$. Exp-time.

Previous work

[KS'98] computes singular points of the intersection of two quadrics. [Luyten '23]

[KPG'99] computes singular points of $V(\mathcal{I})$. Beullens, Castryck '23

Geometric interpretation of an old attack [P. 2025]

[KS'98/KPG'99] are (hybrid) singular point computations. Weaken hypotheses and support heuristic analysis by estimating $|\mathrm{Sing}(V(I))|_{\mathbb{F}_q}$ with the Lang-Weil bound.

Table of Contents

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

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

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

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

Idea: Tradeoff between signing time and key size.

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

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

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

Idea: Tradeoff between signing time and key size.

Analysis: $\mathcal{O} \not\subset V(\mathcal{I}) \implies$ key attacks on UOV$\hat{+}$ must invert $\mathcal{S}$.

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

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

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

Idea: Tradeoff between signing time and key size.

Analysis: $\mathcal{O} \not\subset V(\mathcal{I}) \implies$ key attacks on UOV$\hat{+}$ must invert $\mathcal{S}$.

Geometric interpretation [P. 2025]

Let $\mathcal{I} = \langle \mathcal{P}(\boldsymbol{x}) \rangle$. $V(\mathcal{I})$ is the intersection of a UOV variety with t generic quadrics.

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

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{bmatrix} \multicolumn{2}{c}{J_1} \\ 0 & J_2 \end{bmatrix} \begin{matrix} t+1 \\ \vdots \\ o \end{matrix}$$

$$\quad 1 \cdots\cdots o \quad o+1 \cdots\cdots\cdots n$$

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{bmatrix} \multicolumn{2}{c}{J_1} \\ 0 & J_2 \end{bmatrix} \begin{matrix} t+1 \\ \vdots \\ o \end{matrix}$$

$$1 \cdots\cdots o \quad o+1 \cdots\cdots\cdots n$$

Observation

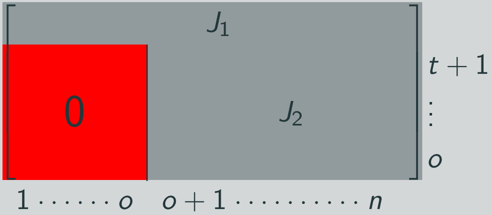
The singular locus of $V(\mathcal{I})$ contains $(\mathrm{Sing}\, V(\mathcal{J})) \cap V(\mathcal{G})$.

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

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

$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) =$



Observation

The singular locus of $V(\mathcal{I})$ contains $(\mathrm{Sing}\, V(\mathcal{J})) \cap V(\mathcal{G})$.

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

$V(\mathcal{I})$ is the public key variety, $V(\mathcal{J})$ is the underlying UOV variety.

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(\mathcal{I})) \subset \mathrm{Sing}(V(\mathcal{J})) \subset \mathcal{O}$$

From singular points to a key recovery attack

$V(\mathcal{I})$ is the public key variety, $V(\mathcal{J})$ is the underlying UOV variety.

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(\mathcal{I})) \subset \mathrm{Sing}(V(\mathcal{J})) \subset \mathcal{O}$$

Singular points of $V(\mathcal{I})$

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

From singular points to a key recovery attack

$V(\mathcal{I})$ is the public key variety, $V(\mathcal{J})$ is the underlying UOV variety.

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(\mathcal{I})) \subset \mathrm{Sing}(V(\mathcal{J})) \subset \mathcal{O}$$

Singular points of $V(\mathcal{I})$

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

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

From singular points to a key recovery attack

$V(\mathcal{I})$ is the public key variety, $V(\mathcal{J})$ is the underlying UOV variety.

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(\mathcal{I})) \subset \mathrm{Sing}(V(\mathcal{J})) \subset \mathcal{O}$$

Singular points of $V(\mathcal{I})$

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

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

Singular points of $V(\mathcal{J})$

$\approx q^{3o-\boldsymbol{t}-n-1}$ singular points of $V(\mathcal{J})$, with q^{o-1} candidates.

From singular points to a key recovery attack

$V(\mathcal{I})$ is the public key variety, $V(\mathcal{J})$ is the underlying UOV variety.

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(\mathcal{I})) \subset \mathrm{Sing}(V(\mathcal{J})) \subset \mathcal{O}$$

Singular points of $V(\mathcal{I})$

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

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

Singular points of $V(\mathcal{J})$

$\approx q^{3o-\boldsymbol{t}-n-1}$ singular points of $V(\mathcal{J})$, with q^{o-1} candidates.

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

From singular points to a key recovery attack

$V(\mathcal{I})$ is the public key variety, $V(\mathcal{J})$ is the underlying UOV variety.

Singular points (still) leak the trapdoor

$$\mathrm{Sing}(V(\mathcal{I})) \subset \mathrm{Sing}(V(\mathcal{J})) \subset \mathcal{O}$$

Singular points of $V(\mathcal{I})$

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

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

Singular points of $V(\mathcal{J})$

$\approx q^{3o-\boldsymbol{t}-n-1}$ singular points of $V(\mathcal{J})$, with q^{o-1} candidates.

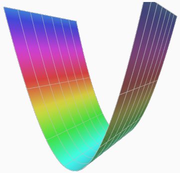
Expected number of trials: $O(q^{n-2o+\boldsymbol{t}})$ but $\mathcal{P}(\boldsymbol{x}) \neq 0$.

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

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

Previous result for UOV **[P. 2024]**

Decide $\boldsymbol{x} \in \mathcal{O}$? in polynomial time: $\boldsymbol{x} \in \mathcal{O} \implies \mathcal{O} \subset T_x V$.



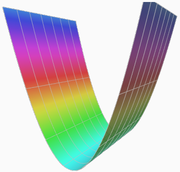
Adapting "$\boldsymbol{x} \in \mathcal{O}$?" to UOV$\hat{+}$ efficiently

Previous result for UOV **[P. 2024]**

Decide $\boldsymbol{x} \in \mathcal{O}$? in polynomial time: $\boldsymbol{x} \in \mathcal{O} \implies \mathcal{O} \subset T_x V$.

Tangent spaces again

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



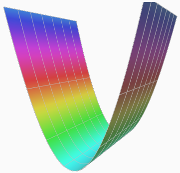
Adapting “$x \in \mathcal{O}$?” to UOV$\hat{+}$ efficiently

Previous result for UOV [P. 2024]

Decide $\boldsymbol{x} \in \mathcal{O}$? in polynomial time: $\boldsymbol{x} \in \mathcal{O} \implies \mathcal{O} \subset T_x V$.

Tangent spaces again

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



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

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

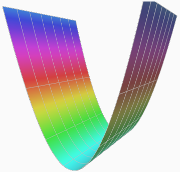
Adapting "$\boldsymbol{x} \in \mathcal{O}$?" to UOV$\hat{+}$ efficiently

Previous result for UOV [P. 2024]

Decide $\boldsymbol{x} \in \mathcal{O}$? in polynomial time: $\boldsymbol{x} \in \mathcal{O} \implies \mathcal{O} \subset T_x V$.

Tangent spaces again

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



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

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

Distinguisher [P. 2025]

$\boldsymbol{x} \in \mathcal{O} \implies V(\mathcal{P}_{|T_x V}(\boldsymbol{x}))$ has constant codimension. **Solved in polynomial time.**

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

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

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

3

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

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

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

Singular points attack and asymptotic result [P. 2025]

Singular points of $V(\mathcal{J})$ leak the trapdoor without inverting $\mathcal{S}$:

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

3

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

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

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

Singular points attack and asymptotic result [P. 2025]

Singular points of $V(\mathcal{J})$ leak the trapdoor without inverting $\mathcal{S}$:

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

Previous result [VOX][3]

This attack improves the Kipnis-Shamir attack which required:

$$O(q^{n-2o+\boldsymbol{2t}}n^{\omega})$$

[3] [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 4: $\boldsymbol{x} \in \mathcal{O}$? with msolve on 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 4: $\boldsymbol{x} \in \mathcal{O}$? with msolve on UOV$\hat{+}$.

We add $\log_2(q) \times (n - 2o + t)$ 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 5: Full attack on UOV$\hat{+}$.

Table of Contents

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

1. What is special about $\mathcal{O}$, compared to the rest of $V(I)$?
2. What is special about $V(I)$, compared to other varieties ?
3. Can $\mathcal{O}$ be hidden with a perturbation or random equations?
4. Can you compress by embedding your key in a field extension?

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

The Quotient Ring transform

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

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

The Quotient Ring transform

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

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

The Quotient Ring transform

- Generate a $\mathrm{UOV}(q^\ell, m, n)$ key with ℓm 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$\hat{+}$

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

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

The Quotient Ring transform

- Generate a UOV(q^ℓ, m, n) key with ℓm 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]

Geometric interpretation of the big field scheme

The dimension of the public key variety in $\mathbb{F}_{q^\ell}$

ℓm generic quadratic polynomials in n variables define a variety of dimension $n - \ell m$.

In (QR-)UOV, $\mathcal{O} \subset V(\mathcal{I}) \implies \dim(V(\mathcal{I})) \geq \dim \mathcal{O} \geq m$

Geometric interpretation of the big field scheme

The dimension of the public key variety in $\mathbb{F}_{q^\ell}$...

ℓm generic quadratic polynomials in n variables define a variety of dimension $n - \ell m$.

In (QR-)UOV, $\mathcal{O} \subset V(\mathcal{I}) \implies \dim(V(\mathcal{I})) \geq \dim \mathcal{O} \geq m$

... leaks the secret key

If $m \geq n - \ell m$ then the big-field polynomial system is easier to solve than a generic system, and the solutions are points of $\mathcal{O}$.

Geometric interpretation of the big field scheme

The dimension of the public key variety in $\mathbb{F}_{q^\ell}$...

ℓm generic quadratic polynomials in n variables define a variety of dimension $n - \ell m$.

In (QR-)UOV, $\mathcal{O} \subset V(\mathcal{I}) \implies \dim(V(\mathcal{I})) \geq \dim \mathcal{O} \geq m$

... leaks the secret key

If $m \geq n - \ell m$ then the big-field polynomial system is easier to solve than a generic system, and the solutions are points of $\mathcal{O}$.

This attack is taken into account in [QRUOV] but not in [VOX].

Practical attack on VOX [VOX@NIST 2023], [VOX minus, Varjabedian 2025]

Dimension computation

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

Practical attack on VOX [VOX@NIST 2023], [VOX minus, Varjabedian 2025]

Dimension computation

UOV$\hat{+}(q^\ell, m/\ell, n/\ell, m, t)$ defines a **variety that contains** $\mathcal{O} \cap V(\mathcal{G})$ 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 [VOX@NIST 2023], [VOX minus, Varjabedian 2025]

Dimension computation

$\mathrm{UOV}\hat{+}(q^\ell, m/\ell, n/\ell, m, t)$ defines a **variety that contains** $\mathcal{O} \cap V(\mathcal{G})$ 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 6: Timing for the subfield attack on VOX (2023) on my laptop.

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

Thank you for your attention!

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

From **one vector** in $\mathcal{O}$, return a basis of $\mathcal{O}$ 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 $\widehat{\text{UOV}}$ 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

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[5] **[Debarre, Manivel 1998]**

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

[5] 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[5] **[Debarre, Manivel 1998]**

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

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

[5] 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[5] **[Debarre, Manivel 1998]**

Let X be a generic complete intersection of m 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.

[5] 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[5] **[Debarre, Manivel 1998]**

Let X be a generic complete intersection of m 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.

[5] 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 $\mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q[x_1, \ldots, x_n]$

- (a) 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 $\mathcal{P}(\boldsymbol{x}) = 0 \in \mathbb{F}_q[x_1, \ldots, x_n]$

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

Generic application: How to solve underdetermined systems?

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

- (a) Compute a subspace S of dimension $s - k$ such that $p_{1|S}, \dots, p_{k|S} = 0$.
- (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. $\frac{n}{s} = \frac{5}{2} \to k = 3$.

- 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 $\boldsymbol{x} \in \mathcal{O}$.

Analyzing our previous work through [DM98]

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

Analyzing our previous work through [DM98]

- Tangent spaces reveal information only if $\boldsymbol{x} \in \mathcal{O}$.
- 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 $\mathcal{O} \subset V(I)$, $\dim \mathcal{O} = s$, $\delta(n-1, s-1, 3) < 0$

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 $\mathcal{O} \subset V(I)$, $\dim \mathcal{O} = s$, $\delta(n-1, s-1, 3) < 0$

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 $\mathcal{O} \subset V(I)$, $\dim \mathcal{O} = s$, $\delta(n-1, s-1, 3) < 0$

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 $\mathcal{O} \subset V(I)$, $\dim \mathcal{O} = s$, $\delta(n-1, s-1, 3) < 0$

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 $\mathcal{O}$ is unknown?

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