Singular points of UOV and VOX

Pierre Pébereau
Sorbonne Université, LIP6, CNRS, Thales SIX

May 2025

Context: Post Quantum Cryptography

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.

Context: Post Quantum Cryptography

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.

Multivariate cryptography

Public key: a polynomial map from $\mathbb{F}_q^n \mapsto \mathbb{F}_q^m$:

$$\boldsymbol{x} \mapsto \mathcal{P}(\boldsymbol{x}) = (p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x}))$$

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.

Multivariate 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:

$$\mathcal{P}(\boldsymbol{x}) = \mathcal{H}(message)$$

Crash course on polynomial systems

Algebra

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

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

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

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

Crash course on polynomial systems

Algebra

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

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

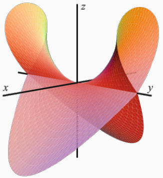
$$\mathcal{I} := \{\textstyle\sum_{i=1}^{m} a_i p_i(\boldsymbol{x}), (a_i) \in \mathbb{F}_q[\boldsymbol{x}]^m\}$$

Geometry

This ideal defines a variety

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

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



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

Crash course on polynomial systems

Algebra

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

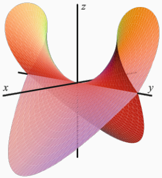
$$\mathcal{I} := \{\textstyle\sum_{i=1}^m a_i p_i(\boldsymbol{x}), (a_i) \in \mathbb{F}_q[\boldsymbol{x}]^m\}$$

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

Geometry

This ideal defines a variety

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



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

Dimension of a variety

Let $(H_i)_{i \in \mathbb{N}}$ be generic hyperplanes and V a variety. $\dim V = 0$ if V is finite, and $\dim V = d$ if $V \cap H_1 \cap \ldots \cap H_d$ has dimension 0.

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 $n > 2m$.

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

UOV Public key

Quadratic map $\mathcal{P}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ generating $\mathcal{I} = \langle p_1, \dots, p_m \rangle$, 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 $x_1, \dots, x_o$ (*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 $\mathcal{P}(\boldsymbol{x}) : \mathbb{F}_q^n \mapsto \mathbb{F}_q^m$ 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 $\mathcal{O} \subset V(\mathcal{I})$.

Observations

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

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.

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.
- $V(\mathcal{I})$ is a complete intersection if $n \geq 2m$: $\dim V(\mathcal{I}) = n - m$.

The Kipnis-Shamir attack against (U)OV

$$\mathcal{P}(\boldsymbol{x}) = (\boldsymbol{x}^T P_1 \boldsymbol{x}, \ldots, \boldsymbol{x}^T P_m \boldsymbol{x}), \quad \dim \mathcal{O} = m$$

The Kipnis-Shamir attack against (U)OV

$$\mathcal{P}(\boldsymbol{x}) = (\boldsymbol{x}^T P_1 \boldsymbol{x}, \ldots, \boldsymbol{x}^T P_m \boldsymbol{x}), \quad \dim \mathcal{O} = m$$

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

$$\mathcal{P}(\boldsymbol{x}) = (\boldsymbol{x}^T P_1 \boldsymbol{x}, \ldots, \boldsymbol{x}^T P_m \boldsymbol{x}), \quad \dim \mathcal{O} = m$$

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

$$\mathcal{P}(\boldsymbol{x}) = (\boldsymbol{x}^T P_1 \boldsymbol{x}, \ldots, \boldsymbol{x}^T P_m \boldsymbol{x}), \quad \dim \mathcal{O} = m$$

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

Contributions

Objective: characterize the singular locus of $V(\mathcal{I})$ and propose new algebraic attacks.

$$\mathcal{I} = \langle p_1, \ldots, p_m \rangle \subset \mathbb{F}_q[\boldsymbol{x}], \quad \dim(\mathcal{O}) = o.$$

Contributions

Objective: characterize the singular locus of $V(\mathcal{I})$ and propose new algebraic attacks.

$$\mathcal{I} = \langle p_1, \ldots, p_m \rangle \subset \mathbb{F}_q[\boldsymbol{x}], \quad \dim(\mathcal{O}) = o.$$

Dimension of the singular locus of $V(\mathcal{I})$ (Th. 3.1)

Suppose $\mathcal{I}$ is radical of codimension m, and $n > m + o$. Then

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

Contributions

Objective: characterize the singular locus of $V(\mathcal{I})$ and propose new algebraic attacks.

$$\mathcal{I} = \langle p_1, \dots, p_m \rangle \subset \mathbb{F}_q[\boldsymbol{x}], \quad \dim(\mathcal{O}) = o.$$

Dimension of the singular locus of $V(\mathcal{I})$ (Th. 3.1)

Suppose $\mathcal{I}$ is radical of codimension m, and $n > m + o$. Then

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

Generic smoothness of a singular variety (Th. 3.2)

Let $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p, p \gg 1$.

For a UOV variety generic in the Zariski sense, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

Contributions

Objective: characterize the singular locus of $V(\mathcal{I})$ and propose new algebraic attacks.

$$\mathcal{I} = \langle p_1, \ldots, p_m \rangle \subset \mathbb{F}_q[\boldsymbol{x}], \quad \dim(\mathcal{O}) = o.$$

Dimension of the singular locus of $V(\mathcal{I})$ (Th. 3.1)

Suppose $\mathcal{I}$ is radical of codimension m, and $n > m + o$. Then

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

Generic smoothness of a singular variety (Th. 3.2)

Let $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p, p \gg 1$.

For a UOV variety generic in the Zariski sense, $\operatorname{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

Application: Singular point attack on UOV$\hat{+}$

The security of UOV$\hat{+}$ was overestimated by a factor q^t.

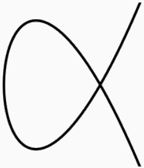
This improves the cryptanalysis by factors $2^2, 2^{18}, 2^{37}$ (I, III, V).

Singular points

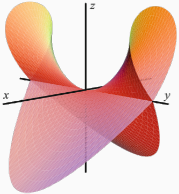
Let $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ be a radical ideal of codimension m.

Definition (Tangent space at a non-singular 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 $\mathbb{R}^2$



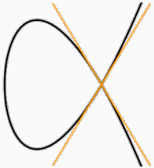
$x^2 - y^2 z^2 + z^3 = 0$ in $\mathbb{R}^3$

Singular points

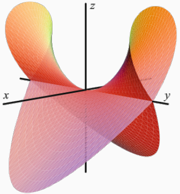
Let $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ be a radical ideal of codimension m.

Definition (Tangent space at a non-singular 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)

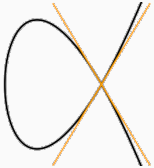


$x^2 - y^2 z^2 + z^3 = 0$ in $\mathbb{R}^3$

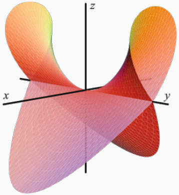
Let $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ be a radical ideal of codimension m.

Definition (Tangent space at a non-singular 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)



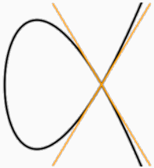
$x^2 - y^2z^2 + z^3 = 0$ in $\mathbb{R}^3$
Singular points: line (x=z=0)

Singular points

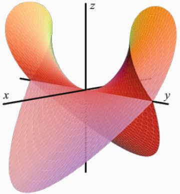
Let $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ be a radical ideal of codimension m.

Definition (Tangent space at a non-singular 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 :

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

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

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

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

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

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

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 $V(\mathcal{I})$ **[P. 2025]**

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

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

Generic smoothness: Thom's weak transversality theorem

In characteristic 0, generic complete intersections are smooth.

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

Generic smoothness: Thom's weak transversality theorem

In characteristic 0, generic complete intersections are smooth.

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

Let $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p$, $p \gg 1$.

For a UOV variety generic in the Zariski sense, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

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

Generic smoothness: Thom's weak transversality theorem

In characteristic 0, generic complete intersections are smooth.

Generic smoothness of a singular variety [P. 2025]

Let $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p$, $p \gg 1$.

For a UOV variety generic in the Zariski sense, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

Geometric interpretation of Kipnis-Shamir [P. 2025]

Kipnis-Shamir [KPG'99] is a (hybrid) singular point computation. Support previous analyses by weakening hypotheses and by estimating $|\mathrm{Sing}(V(\mathcal{I}))|_{\mathbb{F}_q}$ with the Lang-Weil bound.

Application: Study of UOV$\hat{+}$/VOX

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.

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

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.

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

Dimension computation **[P. 2025]**

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

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.

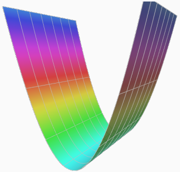
Expected number of trials: $O(q^{n-2o+\boldsymbol{t}})$ but $\mathcal{P}(\boldsymbol{x}) \neq 0$.

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]**

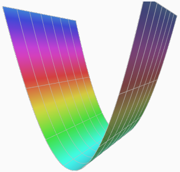
Decide $\boldsymbol{x} \in \mathcal{O}$? in polynomial time: $\boldsymbol{x} \in \mathcal{O} \implies \mathcal{O} \subset T_x V$.



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.

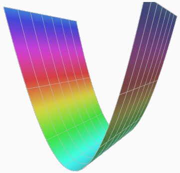
Adapting “$x \in \mathcal{O}$?” to UOV$\hat{+}$ efficiently

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.

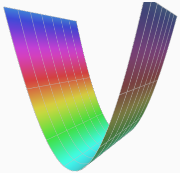
Adapting “$x \in \mathcal{O}$?” to UOV$\hat{+}$ efficiently

Previous result for UOV [P. 2024]

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

Tangent spaces again

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



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

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

Distinguisher [P. 2025]

$x \in \mathcal{O} \implies V(\mathcal{P}_{|T_x V}(x))$ 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 $O(\binom{n-2o+2t-3}{4}^2\binom{n-2o+2t+1}{2})$ with tangent spaces.

1

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

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

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

Singular points attack and asymptotic result [P. 2025]

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

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

1

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

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

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

Singular points attack and asymptotic result [P. 2025]

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

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

Previous result [VOX][1]

This attack improves the Kipnis-Shamir attack which required:

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

[1] [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 1: "$\boldsymbol{x} \in \mathcal{O}$?" for UOV$\hat{+}$ with msolve[2] on a laptop.

[2] see https://msolve.lip6.fr/

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 1: "$\boldsymbol{x} \in \mathcal{O}$?" for UOV$\hat{+}$ with msolve[2] on a laptop.

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

[2] see https://msolve.lip6.fr/

Thank you for your attention!

Singular points of UOV

- $V(\mathcal{I})$ has a (large) positive-dimensional singular locus.
- $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$ generically.
- Algebraic singular points attack does not threaten UOV.
- Enumerative singular points attack is Kipnis-Shamir.

Singular points of UOV$\hat{+}$/VOX

- $\hat{+}$ transform does not hide (all) singularities.
- Target underlying singularities instead of "obvious" ones.
- Adapt "$\boldsymbol{x} \in \mathcal{O}$?" to UOV$\hat{+}$ efficiently.
- Improved cryptanalysis of UOV$\hat{+}$.

Code and logs available online : https://github.com/pi-r2/SingPoints

A key geometric property: dimension

Intuition of dimension from physics

$p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x})$: m “independant” constraints, n variables

$\Longrightarrow n - m$ degrees of freedom in $V(\mathcal{I})$.

A key geometric property: dimension

Intuition of dimension from physics

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

$\implies n - m$ degrees of freedom in $V(\mathcal{I})$.

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

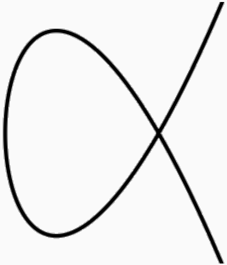
A key geometric property: dimension

Intuition of dimension from physics

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

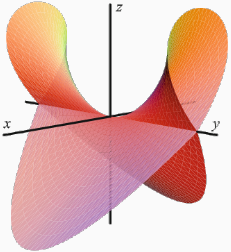
$\Longrightarrow n - m$ degrees of freedom in $V(\mathcal{I})$.

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



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

Figure 3: A curve has dimension 1



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

Figure 4: A hypersurface has dimension n-1

An enumerative approach to the computation of singular points

Bilinear modeling

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

An enumerative approach to the computation of singular points

Bilinear modeling

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

The [Kipnis, Shamir '98] attack computes singular points [3]

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

[3] [Luyten 2023], [Castryck, Beullens 2023]

An enumerative approach to the computation of singular points

Bilinear modeling

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

The [Kipnis, Shamir '98] attack computes singular points [3]

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

[3] [Luyten 2023], [Castryck, Beullens 2023]

An enumerative approach to the computation of singular points

Bilinear modeling

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

The [Kipnis, Shamir '98] attack computes singular points [3]

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

[3] [Luyten 2023], [Castryck, Beullens 2023]

An enumerative approach to the computation of singular points

Bilinear modeling

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

The [Kipnis, Shamir '98] attack computes singular points [3]

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

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

[3] [Luyten 2023], [Castryck, Beullens 2023]

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

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

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

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

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

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

Observation

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

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

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

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

Observation

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

Dimension computation [P. 2025]

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