Geometric approach to the cryptanalysis of UOV

Pierre Pébereau
Sorbonne Université, LIP6, CNRS, Thales SIX

April 2025

Motivation: Post Quantum Cryptography

NIST PQC Additional Signature Candidates

- 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.

Motivation: Post Quantum Cryptography

NIST PQC Additional Signature Candidates

- 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 $\mathbb{F}_q^n \mapsto \mathbb{F}_q^m$:

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

Motivation: Post Quantum Cryptography

NIST PQC Additional Signature Candidates

- 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 sample points $\boldsymbol{x} \in \mathbb{F}_q^n$ such that:

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

Motivation: Post Quantum Cryptography

NIST PQC Additional Signature Candidates

- 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 sample points $\boldsymbol{x} \in \mathbb{F}_q^n$ such that:

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

- In this case, $\boldsymbol{x}$ is a **signature** for *message*.

Crash course on polynomial systems

Algebra

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

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

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

Crash course on polynomial systems

Algebra

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

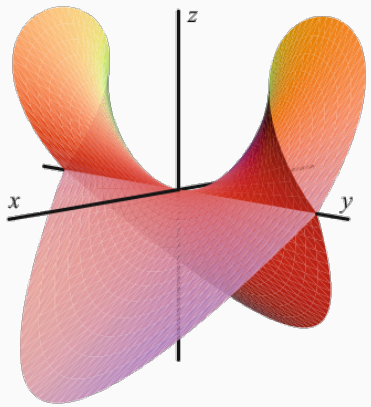
$$I := \{\sum_{i=1}^{m} a_i p_i(\boldsymbol{x}), (a_i) \in \mathbb{F}_q[\boldsymbol{x}]^m\}$$

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

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]

UOV public key

With $n \geq 2m$, a UOV(n, m, q) public key is a quadratic map $\boldsymbol{x} \mapsto \mathcal{P}(\boldsymbol{x}) = (p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x}))$. $(p_1, \ldots, p_m)$ generates an ideal:

$$I = \langle p_1, \ldots, p_m \rangle \subset \mathbb{F}_q[x_1, \ldots, x_n]$$

UOV public key

With $n \geq 2m$, a UOV(n, m, q) public key is a quadratic map $\boldsymbol{x} \mapsto \mathcal{P}(\boldsymbol{x}) = (p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x}))$. $(p_1, \ldots, p_m)$ generates an ideal:

$$I = \langle p_1, \ldots, p_m \rangle \subset \mathbb{F}_q[x_1, \ldots, x_n]$$

Geometric private key [Kipnis, Shamir 1998]

The private key is a linear subspace $\mathcal{O} \subset \mathbb{F}_q^n$ of dimension m:

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

Modern formulation [Kipnis, Patarin, Goubin 1999]

UOV public key

With $n \geq 2m$, a UOV(n, m, q) public key is a quadratic map $\boldsymbol{x} \mapsto \mathcal{P}(\boldsymbol{x}) = (p_1(\boldsymbol{x}), \ldots, p_m(\boldsymbol{x}))$. $(p_1, \ldots, p_m)$ generates an ideal:

$$I = \langle p_1, \ldots, p_m \rangle \subset \mathbb{F}_q[x_1, \ldots, x_n]$$

Geometric private key [Kipnis, Shamir 1998]

The private key is a linear subspace $\mathcal{O} \subset \mathbb{F}_q^n$ of dimension m:

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

Dimension observation

$$\dim \mathcal{O} = m \qquad \dim V(I) = n - m > m.$$

Table of Contents

Objective: Find $\mathcal{O} \subset V(I)$, the secret key.

Tangent spaces of the UOV variety

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

Tangent spaces

Let $\mathrm{Jac}_{\mathcal{P}} := (\frac{\partial p_i}{\partial x_j})_{i,j}$.The tangent space of V at $\boldsymbol{x} \in V$ is

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

Tangent spaces of the UOV variety

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

Tangent spaces

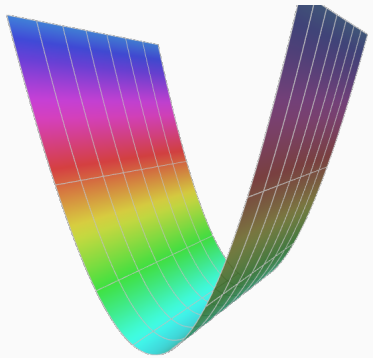
Let $\mathrm{Jac}_{\mathcal{P}} := (\frac{\partial p_i}{\partial x_j})_{i,j}$.The tangent space of V at $\boldsymbol{x} \in V$ is

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

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 $\mathcal{O}$.

Tangent spaces

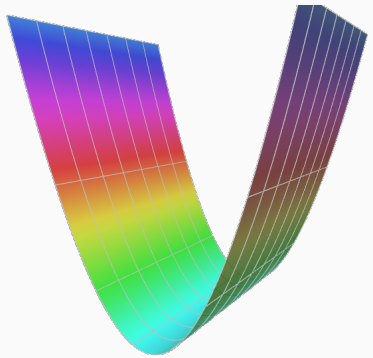
Let $\mathrm{Jac}_{\mathcal{P}} := (\frac{\partial p_i}{\partial x_j})_{i,j}$.The tangent space of V at $\boldsymbol{x} \in V$ is

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

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 the polar forms of $\mathcal{P}$ restricted to $T_{\boldsymbol{x}} V$. These matrices have low rank if $\boldsymbol{x} \in \mathcal{O}$.

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 $O(mn^\omega)$, $2 \leq \omega \leq 3$.

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 $O(mn^\omega)$, $2 \leq \omega \leq 3$.

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

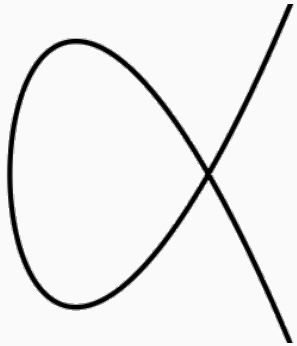
In practice with **SageMath** on my laptop (2.80GHz, 8GB RAM).

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

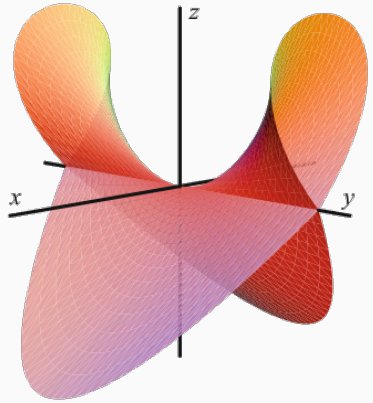
Table of Contents

Objective: Find $\mathcal{O} \subset V(I)$, the secret key.

From tangent spaces to singular points

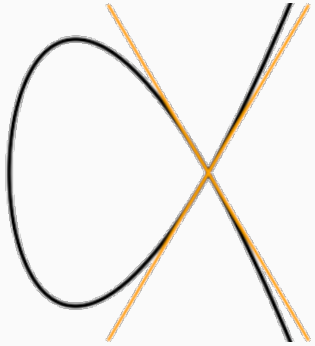


$y^2 = x^3 - 3x + 2$ in $\mathbb{R}^2$



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

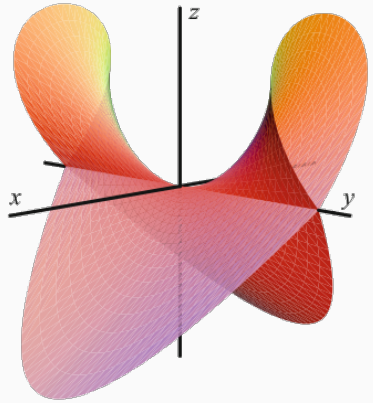
From tangent spaces to singular points



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

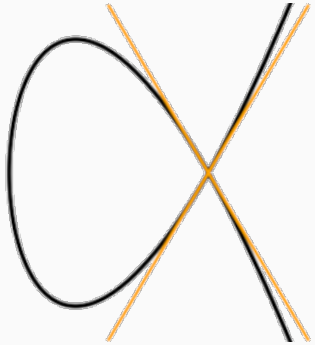
Singular point: (1,0)

(dimension 0)

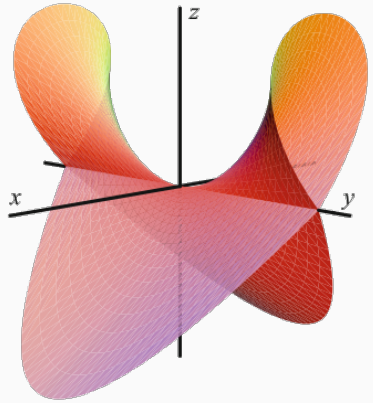


$x^2 - y^2z^2 + z^3$ in $\mathbb{R}^3$

From tangent spaces to singular points

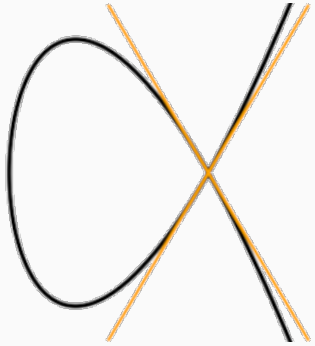


$y^2 = x^3 - 3x + 2$ in $\mathbb{R}^2$
Singular point: (1,0)
(dimension 0)

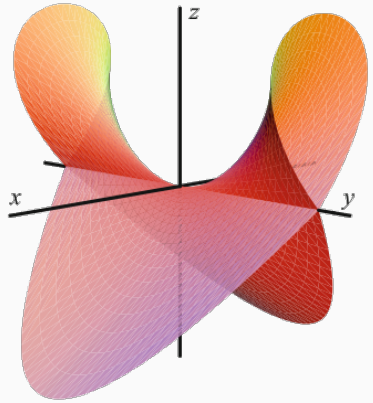


$x^2 - y^2z^2 + z^3$ in $\mathbb{R}^3$
Singular points: line (x=z=0)
(dimension 1)

From tangent spaces to singular points



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



$x^2 - y^2z^2 + z^3$ in $\mathbb{R}^3$
Singular points: line (x=z=0)
(dimension 1)

Definition

Let $I = \langle \mathcal{P} \rangle$ be a radical ideal of $\mathbb{K}[\boldsymbol{x}]$ of dimension $n - m$.

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

Singular points of UOV

$\mathcal{O} \subset V(I)$ is the UOV secret.

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

A large enough linear subspace in a variety imposes singularities:

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

Singular points of UOV

$\mathcal{O} \subset V(I)$ is the UOV secret.

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

A large enough linear subspace in a variety imposes singularities:

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

Generic Smoothness of a singular variety [P. 2025]

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

Singular points of UOV

$\mathcal{O} \subset V(I)$ is the UOV secret.

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

A large enough linear subspace in a variety imposes singularities:

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

Generic Smoothness of a singular variety [P. 2025]

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

Singular points: Old and new attacks

- Computing a **Gröbner basis** of the singular locus does **not** improve the cryptanalysis of UOV in small fields.

Singular points of UOV

$\mathcal{O} \subset V(I)$ is the UOV secret.

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

A large enough linear subspace in a variety imposes singularities:

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

Generic Smoothness of a singular variety [P. 2025]

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

Singular points: Old and new attacks

- Computing a **Gröbner basis** of the singular locus does **not** improve the cryptanalysis of UOV in small fields.
- [Kipnis-Shamir 1998] is a (hybrid) singular point computation.

Singular points of UOV

$\mathcal{O} \subset V(I)$ is the UOV secret.

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

A large enough linear subspace in a variety imposes singularities:

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

Generic Smoothness of a singular variety [P. 2025]

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

Singular points: Old and new attacks

- Computing a **Gröbner basis** of the singular locus does **not** improve the cryptanalysis of UOV in small fields.
- [Kipnis-Shamir 1998] is a (hybrid) singular point computation.
- The **grevlex** Gröbner basis contains **linear polynomials** that define $\mathcal{O}$: lex basis not needed (no FGLM step).

Table of Contents

Objective: Find $\mathcal{O} \subset V(I)$, 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?

I'd rather break my linear subspace than let you have it

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

- Start with a UOV variety W in $\mathbb{F}_q^n$ of dimension $n - s + t$ with a linear subspace $\mathcal{O}$ of dimension m.

I'd rather break my linear subspace than let you have it

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

- Start with a UOV variety W in $\mathbb{F}_q^n$ of dimension $n-s+t$ with a linear subspace $\mathcal{O}$ of dimension m.
- Intersect it with t random quadrics

I'd rather break my linear subspace than let you have it

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

- Start with a UOV variety W in $\mathbb{F}_q^n$ of dimension $n-s+t$ with a linear subspace $\mathcal{O}$ of dimension m.
- Intersect it with t random quadrics
- Obtain a variety $V(I)$ with no large linear subspace.

I'd rather break my linear subspace than let you have it

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

- Start with a UOV variety W in $\mathbb{F}_q^n$ of dimension $n-s+t$ with a linear subspace $\mathcal{O}$ of dimension m.
- Intersect it with t random quadrics
- Obtain a variety $V(I)$ with no large linear subspace.

Singular points (still) leak the secret **[P. 2025]**

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

I'd rather break my linear subspace than let you have it

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

- Start with a UOV variety W in $\mathbb{F}_q^n$ of dimension $n-s+t$ with a linear subspace $\mathcal{O}$ of dimension m.
- Intersect it with t random quadrics
- Obtain a variety $V(I)$ with no large linear subspace.

Singular points (still) leak the secret [P. 2025]

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

Cryptanalysis

- Kipnis-Shamir[1]: Guess $\boldsymbol{x} \in \mathrm{Sing}(V(I))$, check "$\mathcal{P}(\boldsymbol{x}) = 0$?".

[1] Singular point interpretation

I'd rather break my linear subspace than let you have it

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

- Start with a UOV variety W in $\mathbb{F}_q^n$ of dimension $n-s+t$ with a linear subspace $\mathcal{O}$ of dimension m.
- Intersect it with t random quadrics
- Obtain a variety $V(I)$ with no large linear subspace.

Singular points (still) leak the secret [P. 2025]

$$\mathrm{Sing}(V(I)) \subset \mathbf{Sing}(\boldsymbol{W}) \subset \mathcal{O}$$

Cryptanalysis

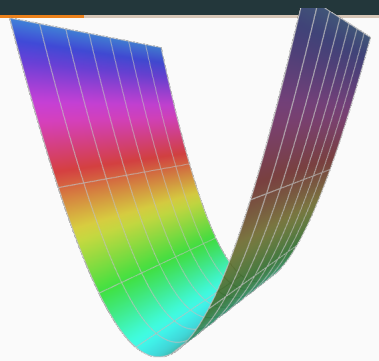
- Kipnis-Shamir[1]: Guess $\boldsymbol{x} \in \mathrm{Sing}(V(I))$, check "$\mathcal{P}(\boldsymbol{x}) = 0$?".
- [P. 2025]: Guess $\boldsymbol{x} \in \mathbf{Sing}(\boldsymbol{W})$, check "$\boldsymbol{x} \in \mathcal{O}$?".

[1] Singular point interpretation

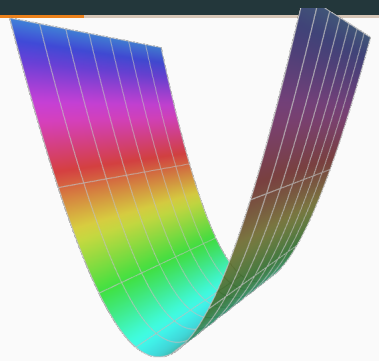
Check "$x \in \mathcal{O}$?", but do it fast

Tangent spaces again

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



Check "$x \in \mathcal{O}$?", but do it fast



Tangent spaces again

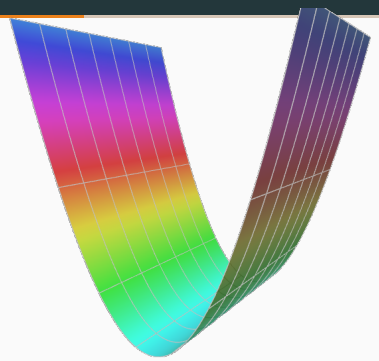
$x \in \mathcal{O} \implies \mathcal{O} \cap T_x V$ large dimension

Distinguisher

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

$\rightarrow$ **Compute Gröbner basis in polynomial time.**

Check "$x \in \mathcal{O}$?", but do it fast



Tangent spaces again

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

Distinguisher

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

$\rightarrow$ **Compute Gröbner basis in polynomial time.**

Singular points attack and asymptotic result [P. 2025]

Underlying singular points leak the trapdoor:

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

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

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

Figure 1: $\boldsymbol{x} \in \mathcal{O}$? with msolve on UOV$\hat{+}$.

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

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

Figure 1: $\boldsymbol{x} \in \mathcal{O}$? with msolve on UOV$\hat{+}$.

We add $\log_2(q) \times (n - 2m + t)$ 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$\hat{+}$.

Table of Contents

Objective: Find $\mathcal{O} \subset V(I)$, 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 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$\hat{+}$

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

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]

Practical attack on VOX

Dimension computation

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

Practical attack on VOX

Dimension computation

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

Subfield attack [P. 2024b]

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

Practical attack on VOX

Dimension computation

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

Subfield attack [P. 2024b]

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

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

Figure 3: Timing for the subfield attack on QR-$\mathrm{UOV}\hat{+}$ on my laptop.

[2] 400 CPU-hours on a server in practice.

Thank you for your attention!

One vector to full key recovery — PQC'24

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

Singular points of UOV and VOX — Eurocrypt'25

- $V(I)$ has a large **singular locus** generically included in $\mathcal{O}$.
- Key recovery from **one vector** for UOV$\hat{+}$ in polynomial time.

Future work

- New attacks with geometric approaches.
- Local properties of $V(I)$ reveal the secret, but we get nothing from generic points of $V(I)$: Are there non-generic global properties of the UOV variety?
- Study of efficient variants of UOV: SNOVA, MAYO.

Worst-case hardness result

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

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

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

Worst-case hardness result

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

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

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

This problem is NP-hard: it reduces to SAT.

Worst-case hardness result

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

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

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

This problem is NP-hard: it reduces to SAT.

For practical difficulty, see for example `mqchallenge.org`.

[Yasuda, Dahan, Huang, Takagi, Sakurai 2015]

A key geometric property: dimension

Intuition of dimension from physics

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

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

A key geometric property: dimension

Intuition of dimension from physics

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

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

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

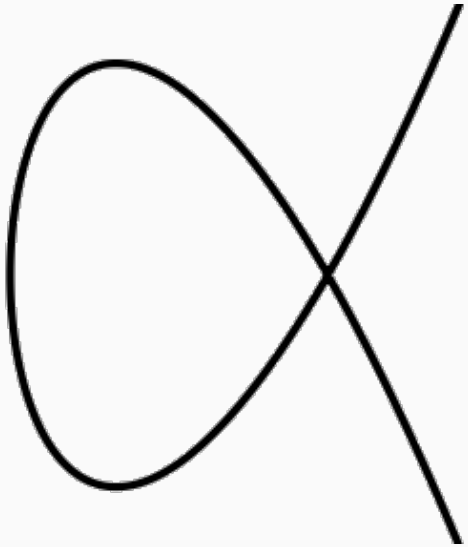
A key geometric property: dimension

Intuition of dimension from physics

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

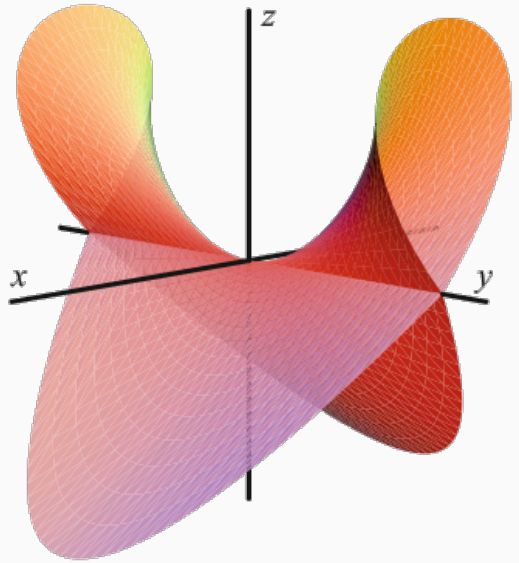
$\Longrightarrow n - s$ degrees of freedom in $V(I)$.

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



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

Figure 4: A curve has dimension 1



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

Figure 5: A hypersurface has dimension n-1

Proposed UOV$\hat{+}$ parameters

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

Question 1: are the polynomials individually special?

The public key polynomials $(p_1, \ldots, p_m)$ all vanish on $\mathcal{O}$.

$\forall 1 \leq i \leq s$, $\boldsymbol{x} \mapsto p_i(\boldsymbol{x})$ is a quadratic form of rank $n \geq 2m$.

Question 1: are the polynomials individually special?

The public key polynomials $(p_1, \ldots, p_m)$ all vanish on $\mathcal{O}$.

$\forall 1 \leq i \leq s$, $\boldsymbol{x} \mapsto p_i(\boldsymbol{x})$ is a quadratic form of rank $n \geq 2m$.

UOV and Number Theory

- $\mathcal{O}$ is an isotropic subspace of the public key quadratic forms.

Question 1: are the polynomials individually special?

The public key polynomials $(p_1, \ldots, p_m)$ all vanish on $\mathcal{O}$.
$\forall 1 \leq i \leq s$, $\boldsymbol{x} \mapsto p_i(\boldsymbol{x})$ is a quadratic form of rank $n \geq 2m$.

UOV and Number Theory

- $\mathcal{O}$ is an isotropic subspace of the public key quadratic forms.
- Forms of rank n admit[3] isotropic subspaces of dimension $n/2$.

[3] Compute a normal form in polynomial time to get $2^{n/2}$ of them.

Question 1: are the polynomials individually special?

The public key polynomials $(p_1, \ldots, p_m)$ all vanish on $\mathcal{O}$.
$\forall 1 \leq i \leq s$, $\boldsymbol{x} \mapsto p_i(\boldsymbol{x})$ is a quadratic form of rank $n \geq 2m$.

UOV and Number Theory

- $\mathcal{O}$ is an isotropic subspace of the public key quadratic forms.
- Forms of rank n admit[3] isotropic subspaces of dimension $n/2$.

Consequence

Individual UOV polynomials are indistinguishable from random degree two polynomials.

[3] Compute a normal form in polynomial time to get $2^{n/2}$ of them.