Genericity in multivariate cryptography

(or how to appease Reviewer B by removing heuristics)

Simon Abelard[1,2], Pierre Pébereau[3], Mohab Safey El Din[2]
[1]EPITA, [2]LIP6, Sorbonne Université, [3]COSIC, KU Leuven.



October 2026

Unbalanced Oil and Vinegar [Patarin '97] [Kipnis, Patarin, Goubin '99]

Multivariate signature schemes: a template

- **Public key**: a system of polynomial equations of degree two $\longrightarrow$ **Hard to solve**
- **Signature**: a solution of the public system of polynomial equations
- **Verification**: testing that a solution is correct $\longrightarrow$ **Easy to verify**

Unbalanced Oil and Vinegar [Patarin '97] [Kipnis, Patarin, Goubin '99]

Multivariate signature schemes: a template

- **Public key**: a system of polynomial equations of degree two $\longrightarrow$ **Hard to solve**
- **Signature**: a solution of the public system of polynomial equations
- **Verification**: testing that a solution is correct $\longrightarrow$ **Easy to verify**

Oil and Vinegar

Private key: reduce to the **linear** case [Patarin '97]

Example: oil is Y,Z; vinegar is X.

$$Z - XY = 0.$$



Unbalanced Oil and Vinegar [Patarin '97] [Kipnis, Patarin, Goubin '99]

Multivariate signature schemes: a template

- **Public key**: a system of polynomial equations of degree two $\longrightarrow$ **Hard to solve**
- **Signature**: a solution of the public system of polynomial equations
- **Verification**: testing that a solution is correct $\longrightarrow$ **Easy to verify**

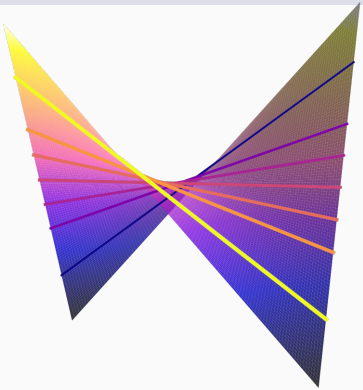
Oil and Vinegar

Private key: reduce to the **linear** case [Patarin '97]

Example: oil is Y,Z; vinegar is X.

$$Z - XY = 0.$$

Set $X = 1$, then the polynomial is linear



Unbalanced Oil and Vinegar [Patarin '97] [Kipnis, Patarin, Goubin '99]

Multivariate signature schemes: a template

- **Public key**: a system of polynomial equations of degree two $\longrightarrow$ **Hard to solve**
- **Signature**: a solution of the public system of polynomial equations
- **Verification**: testing that a solution is correct $\longrightarrow$ **Easy to verify**

Oil and Vinegar

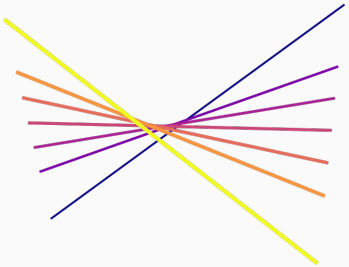
Private key: reduce to the **linear** case [Patarin '97]

Example: oil is Y,Z; vinegar is X.

$$Z - XY = 0.$$

Set $X = 1$, then the polynomial is linear

$$(1, 0, 0) + \mathbb{R}(0, 1, 1).$$



Unbalanced Oil and Vinegar [Patarin '97] [Kipnis, Patarin, Goubin '99]

Multivariate signature schemes: a template

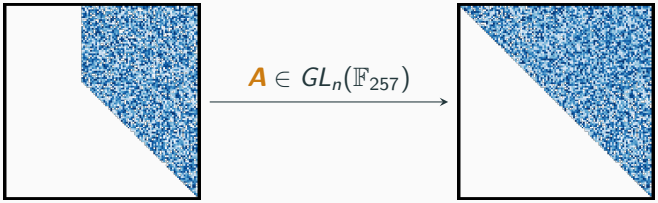
- **Public key**: a system of polynomial equations of degree two $\longrightarrow$ **Hard to solve**
- **Signature**: a solution of the public system of polynomial equations
- **Verification**: testing that a solution is correct $\longrightarrow$ **Easy to verify**

Original (U)OV formulation

Private key: polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ **linear** in $X_1, \ldots, X_o$, $A \in GL_n(\mathbb{F}_q)$.

Public key: polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, with $p_i = X^T \cdot P_i \cdot X = f_i \circ A$.

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



Public polynomial
$P_1 \in (\mathbb{F}_{257})^{n \times n}$

Unbalanced Oil and Vinegar [Patarin '97] [Kipnis, Patarin, Goubin '99]

Multivariate signature schemes: a template

- **Public key**: a system of polynomial equations of degree two $\longrightarrow$ **Hard to solve**
- **Signature**: a solution of the public system of polynomial equations
- **Verification**: testing that a solution is correct $\longrightarrow$ **Easy to verify**

Original (U)OV formulation

Private key: polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ **linear** in $X_1, \ldots, X_o$, $A \in GL_n(\mathbb{F}_q)$.

Public key: polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, with $p_i = X^T \cdot P_i \cdot X = f_i \circ A$.

Equivalent formulation: there exists a linear subspace $\mathcal{O}$ of dim. o such that

$$p_1(\mathcal{O}) = \cdots = p_m(\mathcal{O}) = 0.$$

For UOV, require that $o \geq m$.

Genericity in the Zariski topology

Zariski topology on $\mathbb{K}^n$

A property is **Zariski-generic** if it holds on a non-empty Zariski-open set.

Genericity in the Zariski topology

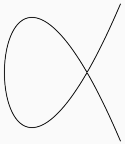
Zariski topology on $\mathbb{K}^n$

A property is **Zariski-generic** if it holds on a non-empty Zariski-open set.

Example: generic smoothness

The curve of equation $Y^2 - X^3 + 3X - 2 = 0$ is **singular**.

Are all curves of equation $Y^2 - X^3 - aX - b = 0$ singular?



Genericity in the Zariski topology

Zariski topology on $\mathbb{K}^n$

A property is **Zariski-generic** if it holds on a non-empty Zariski-open set.

Example: generic smoothness

The curve of equation $Y^2 - X^3 + 3X - 2 = 0$ is **singular**.
Are all curves of equation $Y^2 - X^3 - aX - b = 0$ singular?

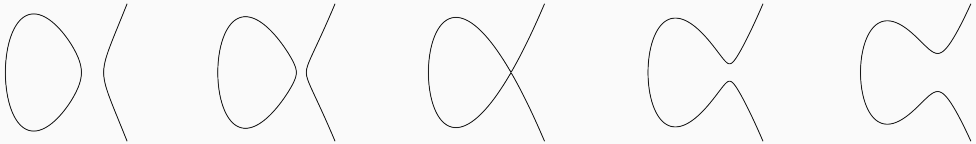


Figure 1: Curves in $\mathbb{R}^2$ defined by $Y^2 - X^3 - aX - 2$ for $a \in [-3.4, -2.6]$.

Genericity in the Zariski topology

Zariski topology on $\mathbb{K}^n$

A property is **Zariski-generic** if it holds on a non-empty Zariski-open set.

Example: generic smoothness

The curve of equation $Y^2 - X^3 + 3X - 2 = 0$ is **singular**.
Are all curves of equation $Y^2 - X^3 - aX - b = 0$ singular?



Figure 1: Curves in $\mathbb{R}^2$ defined by $Y^2 - X^3 - aX - 2$ for $a \in [-3.4, -2.6]$.

Methodology

Consider a, b as **variables** and study the equation $\mathrm{Jac}_E(a, b) = (0, 0)$.

$$\mathrm{Jac}_E(a, b) = (0, 0) \in \mathbb{K}(X, Y)[a, b] \implies \delta(a, b) = 4a^3 + 27b^2 = 0.$$

$$\mathrm{Jac}_{\mathcal{F}} = \begin{bmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial X_1} & \cdots & \frac{\partial f_m}{\partial X_n} \end{bmatrix}$$

Genericity in the Zariski topology

Zariski topology on $\mathbb{K}^n$

A property is **Zariski-generic** if it holds on a non-empty Zariski-open set.

Example: generic smoothness

The curve of equation $Y^2 - X^3 + 3X - 2 = 0$ is **singular**.
Are all curves of equation $Y^2 - X^3 - aX - b = 0$ singular?



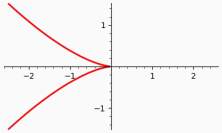
Figure 1: Curves in $\mathbb{R}^2$ defined by $Y^2 - X^3 - aX - 2$ for $a \in [-3.4, -2.6]$.

Methodology

Consider a, b as **variables** and study the equation $\mathrm{Jac}_E(a, b) = (0, 0)$.

$$\mathrm{Jac}_E(a, b) = (0, 0) \in \mathbb{K}(X, Y)[a, b] \implies \delta(a, b) = 4a^3 + 27b^2 = 0.$$

Therefore, if $\delta(a, b)$ is non-zero, $E_{a,b}$ is **smooth**.



Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence ($\dim V = n - m$)		

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence ($\dim V = n - m$)	Yes	Yes

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence ($\dim V = n - m$)	Yes	Yes
Smoothness		

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	Yes
Smoothness	Yes	

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence ($\dim V = n - m$)	Yes	Yes
Smoothness	Yes	No

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	Yes
Smoothness	Yes	No
Contains linear subspace of dim. 2		

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	Yes
Smoothness	Yes	No
Contains linear subspace of dim. 2	Yes	

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	Yes
Smoothness	Yes	No
Contains linear subspace of dim. 2	Yes	Yes

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	Yes
Smoothness	Yes	No
Contains linear subspace of dim. 2	Yes	Yes
Contains linear subspace of dim. 3		

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	Yes
Smoothness	Yes	No
Contains linear subspace of dim. 2	Yes	Yes
Contains linear subspace of dim. 3	Yes	

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	Yes
Smoothness	Yes	No
Contains linear subspace of dim. 2	Yes	Yes
Contains linear subspace of dim. 3	Yes	Yes

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	Yes
Smoothness	Yes	No
Contains linear subspace of dim. 2	Yes	Yes
Contains linear subspace of dim. 3	Yes	Yes
Contains linear subspace of dim. m		

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	Yes
Smoothness	Yes	No
Contains linear subspace of dim. 2	Yes	Yes
Contains linear subspace of dim. 3	Yes	Yes
Contains linear subspace of dim. m	No	

Cryptanalysis through the lense of genericity

Why do we care about generic properties?

Genericity (or lack thereof) can help us design attacks and analyze their complexities.

Pop quizz: which of these properties are **generic** for homogeneous polynomials with $n = 112$ variables and $m = 44$ equations?

(This is the UOV-Ip parameter set submitted to NIST.)

Property	Quadratic systems	UOV public keys
Regular sequence (dim $V = n - m$)	Yes	Yes
Smoothness	Yes	No
Contains linear subspace of dim. 2	Yes	Yes
Contains linear subspace of dim. 3	Yes	Yes
Contains linear subspace of dim. m	No	Yes

Fundamental example: How many equations characterize the UOV secret?

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

The (quadratic) Debarre and Manivel Bound **[Debarre, Manivel 1998]**

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

Fundamental example: How many equations characterize the UOV secret?

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

The (quadratic) Debarre and Manivel Bound **[Debarre, Manivel 1998]**

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

- If $\delta(n, m, o) < 0$, then X does not contain o-dimensional projective subspaces.

Fundamental example: How many equations characterize the UOV secret?

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

The (quadratic) Debarre and Manivel Bound [Debarre, Manivel 1998]

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

- If $\delta(n, m, o) < 0$, then X does not contain o-dimensional projective subspaces.
- Else, $\delta(n, m, o)$ is the dimension of the variety of o-dimensional projective subspaces in X.

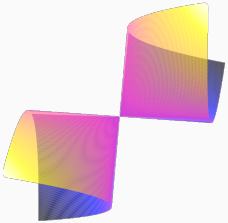
Fundamental example: How many equations characterize the UOV secret?

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

The (quadratic) Debarre and Manivel Bound [Debarre, Manivel 1998]

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

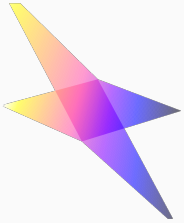
- If $\delta(n, m, o) < 0$, then X does not contain o-dimensional projective subspaces.
- Else, $\delta(n, m, o)$ is the dimension of the variety of o-dimensional projective subspaces in X.



$\mathcal{S}_1 : Z^2 + XY = 0$

Example: Quadric hypersurfaces in $\mathbb{R}^3$.

The theorem is projective: we work in $\mathbb{P}^2(\mathbb{R})$.



$\mathcal{S}_2 : (X + Y + Z)Z = 0$

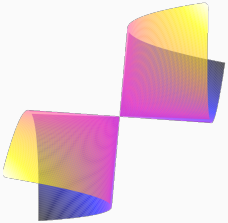
Fundamental example: How many equations characterize the UOV secret?

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

The (quadratic) Debarre and Manivel Bound [Debarre, Manivel 1998]

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

- If $\delta(n, m, o) < 0$, then X does not contain o-dimensional projective subspaces.
- Else, $\delta(n, m, o)$ is the dimension of the variety of o-dimensional projective subspaces in X.



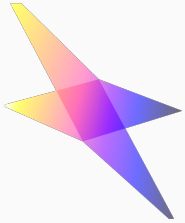
$\mathcal{S}_1 : Z^2 + XY = 0$

Example: Quadric hypersurfaces in $\mathbb{R}^3$.

The theorem is projective: we work in $\mathbb{P}^2(\mathbb{R})$.

$\delta(n = 2, m = 1, o = 1) = -1$

$\delta(n = 2, m = 1, o = 0) = 1$



$\mathcal{S}_2 : (X + Y + Z)Z = 0$

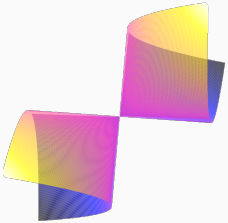
Fundamental example: How many equations characterize the UOV secret?

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

The (quadratic) Debarre and Manivel Bound [Debarre, Manivel 1998]

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

- If $\delta(n, m, o) < 0$, then X does not contain o-dimensional projective subspaces.
- Else, $\delta(n, m, o)$ is the dimension of the variety of o-dimensional projective subspaces in X.



$\mathcal{S}_1 : Z^2 + XY = 0$

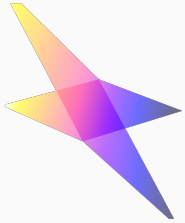
Example: Quadric hypersurfaces in $\mathbb{R}^3$.

The theorem is projective: we work in $\mathbb{P}^2(\mathbb{R})$.

$\delta(n = 2, m = 1, o = 1) = -1$

$\delta(n = 2, m = 1, o = 0) = 1$

Thus, a **generic** quadric hypersurface in $\mathbb{R}^3$ contains lines but does not contain planes.



$\mathcal{S}_2 : (X + Y + Z)Z = 0$

Fundamental example: How many equations characterize the UOV secret?

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

The (quadratic) Debarre and Manivel Bound [Debarre, Manivel 1998]

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

- If $\delta(n, m, o) < 0$, then X does not contain o-dimensional projective subspaces.
- Else, $\delta(n, m, o)$ is the dimension of the variety of o-dimensional projective subspaces in X.

Applications to UOV

- For all UOV parameters submitted to NIST, $\delta(n-1, \mathbf{4}, o-1) < 0$.

Fundamental example: How many equations characterize the UOV secret?

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

The (quadratic) Debarre and Manivel Bound [Debarre, Manivel 1998]

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

- If $\delta(n, m, o) < 0$, then X does not contain o-dimensional projective subspaces.
- Else, $\delta(n, m, o)$ is the dimension of the variety of o-dimensional projective subspaces in X.

Applications to UOV

- For all UOV parameters submitted to NIST, $\delta(n-1, \mathbf{4}, o-1) < 0$.
- The theorem shows that Reconciliation systems have the expected co-dimension $m\binom{o+2}{2}$.

$$1 \leq k \leq m,\ 1 \leq i \leq j \leq o, \quad P_k(X_i, X_j) = 0.$$

Fundamental example: How many equations characterize the UOV secret?

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

The (quadratic) Debarre and Manivel Bound [Debarre, Manivel 1998]

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

- If $\delta(n, m, o) < 0$, then X does not contain o-dimensional projective subspaces.
- Else, $\delta(n, m, o)$ is the dimension of the variety of o-dimensional projective subspaces in X.

Applications to UOV

- For all UOV parameters submitted to NIST, $\delta(n-1, \mathbf{4}, o-1) < 0$.
- The theorem shows that Reconciliation systems have the expected co-dimension $m\binom{o+2}{2}$.

$$1 \leq k \leq m,\ 1 \leq i \leq j \leq o, \quad P_k(X_i, X_j) = 0.$$

- The dimension of $\mathbb{G}_o(\mathbb{P}^n(\mathbb{K}))$ is $(o+1)(n-o)$, ie the number of coefficients in an echelon basis of an $(o+1)$-dimensional linear subspace of $\mathbb{K}^{n+1}$.

Contributions and Outline of the talk

Singularities of generic UOV keys. **[P. 2025]**

For a generic UOV key $\mathcal{P} \in \mathcal{U}$, we have $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

This result unlocks subsequent genericity results.

Contributions and Outline of the talk

Singularities of generic UOV keys. **[P. 2025]**

For a generic UOV key $\mathcal{P} \in \mathcal{U}$, we have $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

This result unlocks subsequent genericity results.

A family of examples. **This work**

The previous result holds in any finite field.

Address a limit of [P. 2025] which worked only over large fields.

Contributions and Outline of the talk

Singularities of generic UOV keys. [P. 2025]

For a generic UOV key $\mathcal{P} \in \mathcal{U}$, we have $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

This result unlocks subsequent genericity results.

A family of examples. This work

The previous result holds in any finite field.

Address a limit of [P. 2025] which worked only over large fields.

Common regularity assumptions are generic... This work

If $\mathcal{P} \in \mathcal{U}$, then $\mathcal{P}$ forms a regular sequence and $V(\mathcal{I})$ is an equidimensional complete intersection [...].

Support analysis of the direct attack and of some key recovery attacks. In particular, geometric attacks are well-defined.

Contributions and Outline of the talk

Singularities of generic UOV keys. [P. 2025]

For a generic UOV key $\mathcal{P} \in \mathcal{U}$, we have $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

This result unlocks subsequent genericity results.

A family of examples. This work

The previous result holds in any finite field.

Address a limit of [P. 2025] which worked only over large fields.

Common regularity assumptions are generic... This work

If $\mathcal{P} \in \mathcal{U}$, then $\mathcal{P}$ forms a regular sequence and $V(\mathcal{I})$ is an equidimensional complete intersection [...].

Support analysis of the direct attack and of some key recovery attacks. In particular, geometric attacks are well-defined.

...more exotic assumptions on MinRank also are. This work

For a generic UOV key $\mathcal{P} \in \mathcal{M}$, the determinantal ideals related to the Jacobian evaluated on $\mathcal{O}$ have the expected dimension.

Support the analysis of Rectangular MinRank attacks. No false positives in the Kipnis-Shamir attack.

Generic UOV keys

Indeterminate UOV secret key

Fix $O = \{1, \ldots, o\}$ (oil indices) and $V = \{o+1, \ldots, n\}$ (vinegar indices).
For $1 \leq k \leq m$,

$$\Phi^{(k)}(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \underbrace{\sum_{i \in O,\ j \in V} \alpha_{i,j}^{(k)}\, x_i x_j}_{\text{oil} \times \text{vinegar}} + \underbrace{\sum_{i \leq j \in V} \beta_{i,j}^{(k)}\, x_i x_j}_{\text{vinegar} \times \text{vinegar}}.$$

The coefficients $\theta = (\boldsymbol{\alpha}, \boldsymbol{\beta})$ live in $\overline{\mathbb{K}}^d$, with $d = m\left(o(n-o) + \frac{(n-o)(n-o+1)}{2}\right)$.

Generic UOV keys

Indeterminate UOV secret key

Fix $O = \{1, \ldots, o\}$ (oil indices) and $V = \{o+1, \ldots, n\}$ (vinegar indices).
For $1 \leq k \leq m$,

$$\Phi^{(k)}(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \underbrace{\sum_{i \in O,\ j \in V} \alpha_{i,j}^{(k)}\, x_i x_j}_{\text{oil} \times \text{vinegar}} + \underbrace{\sum_{i \leq j \in V} \beta_{i,j}^{(k)}\, x_i x_j}_{\text{vinegar} \times \text{vinegar}}.$$

The coefficients $\theta = (\boldsymbol{\alpha}, \boldsymbol{\beta})$ live in $\mathbb{K}^d$, with $d = m\left(o(n-o) + \frac{(n-o)(n-o+1)}{2}\right)$.

- The oil space is $\mathcal{O} = \{\boldsymbol{x} \mid x_{o+1} = \cdots = x_n = 0\}$.
- A secret key is a pair $(\theta, A) \in \mathbb{K}^d \times GL_n(\mathbb{K})$.
- The public key is $\mathcal{P} = \Phi_\theta \circ A$.

Generic UOV keys

Indeterminate UOV secret key

Fix $O = \{1, \ldots, o\}$ (oil indices) and $V = \{o+1, \ldots, n\}$ (vinegar indices).
For $1 \leq k \leq m$,

$$\Phi^{(k)}(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \underbrace{\sum_{i \in O,\ j \in V} \alpha_{i,j}^{(k)}\, x_i x_j}_{\text{oil} \times \text{vinegar}} + \underbrace{\sum_{i \leq j \in V} \beta_{i,j}^{(k)}\, x_i x_j}_{\text{vinegar} \times \text{vinegar}}.$$

The coefficients $\theta = (\boldsymbol{\alpha}, \boldsymbol{\beta})$ live in $\overline{\mathbb{K}}^d$, with $d = m\left(o(n-o) + \frac{(n-o)(n-o+1)}{2}\right)$.

- The oil space is $\mathcal{O} = \{\boldsymbol{x} \mid x_{o+1} = \cdots = x_n = 0\}$.
- A secret key is a pair $(\theta, A) \in \overline{\mathbb{K}}^d \times GL_n(\mathbb{K})$.
- The public key is $\mathcal{P} = \Phi_\theta \circ A$.

Generic UOV key

A property is **generic** if it holds for all θ in a non-empty Zariski-open subset of $\overline{\mathbb{K}}^d$.

Generic UOV keys

Indeterminate UOV secret key

Fix $O = \{1, \ldots, o\}$ (oil indices) and $V = \{o+1, \ldots, n\}$ (vinegar indices).
For $1 \leq k \leq m$,

$$\Phi^{(k)}(\boldsymbol{x}, \boldsymbol{\alpha}, \boldsymbol{\beta}) = \underbrace{\sum_{i \in O,\ j \in V} \alpha_{i,j}^{(k)}\, x_i x_j}_{\text{oil} \times \text{vinegar}} + \underbrace{\sum_{i \leq j \in V} \beta_{i,j}^{(k)}\, x_i x_j}_{\text{vinegar} \times \text{vinegar}}.$$

The coefficients $\theta = (\boldsymbol{\alpha}, \boldsymbol{\beta})$ live in $\overline{\mathbb{K}}^d$, with $d = m\left(o(n-o) + \frac{(n-o)(n-o+1)}{2}\right)$.

- The oil space is $\mathcal{O} = \{\boldsymbol{x} \mid x_{o+1} = \cdots = x_n = 0\}$.
- A secret key is a pair $(\theta, A) \in \overline{\mathbb{K}}^d \times GL_n(\mathbb{K})$.
- The public key is $\mathcal{P} = \Phi_\theta \circ A$.

Generic UOV key

A property is **generic** if it holds for all θ in a non-empty Zariski-open subset of $\overline{\mathbb{K}}^d$.

The properties we study are preserved by A through the chain rule, so we may study them for the secret map Φ_θ.

For generic UOV keys, all singularities lie in $\mathcal{O}$.

Structured equations yield a structured Jacobian. [P. 2025]

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{matrix} 1 \\ \vdots \\ m \end{matrix} \overset{\begin{matrix} 1 \cdots\cdots o & o+1 \cdots\cdots\cdots n \end{matrix}}{\begin{bmatrix} 0 & J_2 \end{bmatrix}}$$

- There are singularities in $\mathcal{O}$.
- Are there singular points outside of $\mathcal{O}$, that may hinder attacks or enable distinguishers?

For generic UOV keys, all singularities lie in $\mathcal{O}$.

Structured equations yield a structured Jacobian. [P. 2025]

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{matrix} 1 \\ \vdots \\ m \end{matrix} \overset{\begin{matrix} 1 \cdots\cdots o & o+1 \cdots\cdots\cdots n \end{matrix}}{\begin{bmatrix} 0 & J_2 \end{bmatrix}}$$

- There are singularities in $\mathcal{O}$.
- Are there singular points outside of $\mathcal{O}$, that may hinder attacks or enable distinguishers?

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

For a generic UOV key, we have $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$, if $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p, p \gg 1$.

For generic UOV keys, all singularities lie in $\mathcal{O}$.

Structured equations yield a structured Jacobian. [P. 2025]

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} 1 \\ \vdots \\ m \end{array} \begin{bmatrix} 0 & J_2 \end{bmatrix}$$

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

- There are singularities in $\mathcal{O}$.
- Are there singular points outside of $\mathcal{O}$, that may hinder attacks or enable distinguishers?

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

There exists a Zariski-open set of UOV keys $\mathcal{U}$ such that for all $\mathcal{I} \in \mathcal{U}$, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

By Thom's weak transversality Theorem, $\mathcal{U}$ is non-empty if $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p, p \gg 1$.

For generic UOV keys, all singularities lie in $\mathcal{O}$.

Structured equations yield a structured Jacobian. [P. 2025]

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{matrix} 1 \\ \vdots \\ m \end{matrix} \overset{\begin{matrix} 1 \cdots\cdots o & o+1 \cdots\cdots\cdots n \end{matrix}}{\begin{bmatrix} 0 & J_2 \end{bmatrix}}$$

- There are singularities in $\mathcal{O}$.
- Are there singular points outside of $\mathcal{O}$, that may hinder attacks or enable distinguishers?

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

There exists a Zariski-open set of UOV keys $\mathcal{U}$ such that for all $\mathcal{I} \in \mathcal{U}$, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

By Thom's weak transversality Theorem, $\mathcal{U}$ is non-empty if $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p$, $p \gg 1$.

Fields used in UOV: $\mathbb{F}_{16}, \mathbb{F}_{256}$.

For generic UOV keys, all singularities lie in $\mathcal{O}$.

Structured equations yield a structured Jacobian. [P. 2025]

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} 1 \\ \vdots \\ m \end{array} \begin{bmatrix} 0 & J_2 \end{bmatrix}$$

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

- There are singularities in $\mathcal{O}$.
- Are there singular points outside of $\mathcal{O}$, that may hinder attacks or enable distinguishers?

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

There exists a Zariski-open set of UOV keys $\mathcal{U}$ such that for all $\mathcal{I} \in \mathcal{U}$, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

By Thom's weak transversality Theorem, $\mathcal{U}$ is non-empty if $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{F}_p$, $p \gg 1$.

Fields used in UOV: $\mathbb{F}_{16}, \mathbb{F}_{256}$.

It suffices to give examples in smaller fields to extend the result by proving $\mathcal{U} \neq \emptyset$.

Goal: construct a family of UOV keys whose Jacobians have full rank outside of $\mathcal{O}$.

Goal: construct a family of UOV keys whose Jacobians have full rank outside of $\mathcal{O}$.

Method: Define the Jacobian matrix, and obtain the quadratic map by integration.

In characteristic 2, there is a difficulty as there is no primitive to X_j with respect to X_j.

Goal: construct a family of UOV keys whose Jacobians have full rank outside of $\mathcal{O}$.

Method: Define the Jacobian matrix, and obtain the quadratic map by integration.

In characteristic 2, there is a difficulty as there is no primitive to X_j with respect to X_j.

$$J = \begin{array}{c} \begin{array}{cccccccccc} \partial X_n & \partial X_{n-1} & \cdots & \partial X_{n-m} & \partial X_{n-m-1} & \cdots & \partial X_{o+1} & \cdots & \partial X_{o+1-m} & \cdots & \partial X_1 \end{array} \\ \begin{bmatrix} X_{o+1} & X_{o+2} & \cdots & X_{o+1+m} & X_{o+2+m} & \cdots & X_n & & & & \\ X_o & X_{o+1} & \ddots & X_{o+m} & X_{o+1+m} & & & \ddots & & & \\ \vdots & \vdots & \ddots & \ddots & \ddots & & & & & & \\ X_{o+1-m} & X_{o+2-m} & \cdots & X_{o+1} & X_{o+2} & \cdots & & & X_n & & \end{bmatrix} \end{array}$$

A family of examples in finite fields of odd characteristic.

Goal: construct a family of UOV keys whose Jacobians have full rank outside of $\mathcal{O}$.

Method: Define the Jacobian matrix, and obtain the quadratic map by integration.

In characteristic 2, there is a difficulty as there is no primitive to X_j with respect to X_j.

$$J = \begin{bmatrix} \partial X_n & \partial X_{n-1} & \cdots & \partial X_{n-m} & \partial X_{n-m-1} & \cdots & \partial X_{o+1} & \cdots & \partial X_{o+1-m} & \cdots & \partial X_1 \\ X_{o+1} & X_{o+2} & \cdots & X_{o+1+m} & X_{o+2+m} & \cdots & X_n & & & & \\ X_o & X_{o+1} & \ddots & X_{o+m} & X_{o+1+m} & & & \ddots & & & \\ \vdots & \vdots & \ddots & \ddots & \ddots & & & & & & \\ X_{o+1-m} & X_{o+2-m} & \cdots & X_{o+1} & X_{o+2} & \cdots & & & X_n & & \end{bmatrix}$$

Sketch of proof.

$\boldsymbol{x} \notin \mathcal{O}$ if and only if there exists $o+1 \leq i \leq n$ such that $x_i \neq 0$.

On any such point, J contains a full-rank lower-triangular submatrix.

Goal: construct a family of UOV keys whose Jacobians have full rank outside of $\mathcal{O}$.

Method: Define the Jacobian matrix, and obtain the quadratic map by integration.

In characteristic 2, there is a difficulty as there is no primitive to X_j with respect to X_j.

$$f_k = \sum_{1 \le i \le n-o} X_{o+i} X_{n-i-(k-1)}.$$

$$J = \begin{array}{c} \begin{array}{cccccccccc} \partial X_n & \partial X_{n-1} & \cdots & \partial X_{n-m} & \partial X_{n-m-1} & \cdots & \partial X_{o+1} & \cdots & \partial X_{o+1-m} & \cdots & \partial X_1 \end{array} \\ \begin{bmatrix} X_{o+1} & X_{o+2} & \cdots & X_{o+1+m} & X_{o+2+m} & \cdots & X_n & & & & \\ X_o & X_{o+1} & \ddots & X_{o+m} & X_{o+1+m} & & & \ddots & & & \\ \vdots & \vdots & \ddots & \ddots & \ddots & & & & & & \\ X_{o+1-m} & X_{o+2-m} & \cdots & X_{o+1} & X_{o+2} & \cdots & & & X_n & & \end{bmatrix} \end{array}$$

Sketch of proof.

$\boldsymbol{x} \notin \mathcal{O}$ if and only if there exists $o+1 \le i \le n$ such that $x_i \neq 0$.

On any such point, J contains a full-rank lower-triangular submatrix.

Genericity of regularity properties.

Reminder: Definition of $\mathcal{U}$.

There exists a Zariski-open set of UOV keys $\mathcal{U}$ such that for all $\mathcal{P} \in \mathcal{U}$, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

Consider UOV parameters (n, m, o, q), with $m \leq o < n - m$.
Let $\mathcal{P} \in \mathcal{U}$ be a generic UOV key, and denote by $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$.

Genericity of regularity properties.

Reminder: Definition of $\mathcal{U}$.

There exists a Zariski-open set of UOV keys $\mathcal{U}$ such that for all $\mathcal{P} \in \mathcal{U}$, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

Consider UOV parameters (n, m, o, q), with $m \leq o < n - m$.
Let $\mathcal{P} \in \mathcal{U}$ be a generic UOV key, and denote by $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$.

UOV varieties are not too weird **This work**

- $\mathcal{O}$ is not an irreducible component of $V(\mathcal{I})$.

Genericity of regularity properties.

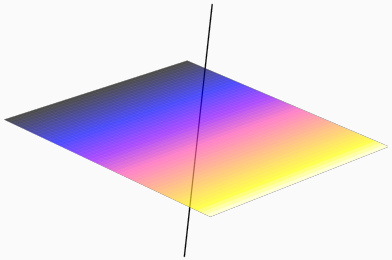
Reminder: Definition of $\mathcal{U}$.

There exists a Zariski-open set of UOV keys $\mathcal{U}$ such that for all $\mathcal{P} \in \mathcal{U}$, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

Consider UOV parameters (n, m, o, q), with $m \leq o < n - m$.
Let $\mathcal{P} \in \mathcal{U}$ be a generic UOV key, and denote by $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$.

UOV varieties are not too weird — **This work**

- $\mathcal{O}$ is not an irreducible component of $V(\mathcal{I})$.
- $V(\mathcal{I})$ is an equidimensional complete intersection.



The variety defined by $\begin{cases} XZ = 0 \\ XY = 0 \end{cases}$ is not equidimensional.

Genericity of regularity properties.

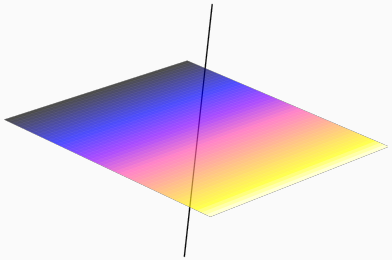
Reminder: Definition of $\mathcal{U}$.

There exists a Zariski-open set of UOV keys $\mathcal{U}$ such that for all $\mathcal{P} \in \mathcal{U}$, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

Consider UOV parameters (n, m, o, q), with $m \leq o < n - m$.
Let $\mathcal{P} \in \mathcal{U}$ be a generic UOV key, and denote by $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$.

UOV varieties are not too weird — **This work**

- $\mathcal{O}$ is not an irreducible component of $V(\mathcal{I})$.
- $V(\mathcal{I})$ is an equidimensional complete intersection.
- $\mathcal{I}$ is a radical ideal.



The variety defined by $\begin{cases} XZ = 0 \\ XY = 0 \end{cases}$ is not equidimensional.

Genericity of regularity properties.

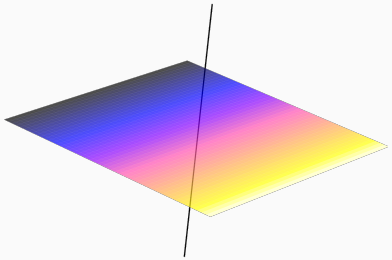
Reminder: Definition of $\mathcal{U}$.

There exists a Zariski-open set of UOV keys $\mathcal{U}$ such that for all $\mathcal{P} \in \mathcal{U}$, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$.

Consider UOV parameters (n, m, o, q), with $m \leq o < n - m$.
Let $\mathcal{P} \in \mathcal{U}$ be a generic UOV key, and denote by $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$.

UOV varieties are not too weird — **This work**

- $\mathcal{O}$ is not an irreducible component of $V(\mathcal{I})$.
- $V(\mathcal{I})$ is an equidimensional complete intersection.
- $\mathcal{I}$ is a radical ideal.
- $(p_1, \ldots, p_m)$ is a regular sequence.



The variety defined by $\begin{cases} XZ = 0 \\ XY = 0 \end{cases}$ is not equidimensional.

Supporting heuristics in the algebraic analysis of attacks.

Direct attack against UOV

Given $\boldsymbol{t} = \mathcal{H}(M) \in \mathbb{F}_q^m$, find $\boldsymbol{x} \in \mathbb{F}_q^n$ such that

$$p_1(\boldsymbol{x}) = t_1, \ \ldots, \ p_m(\boldsymbol{x}) = t_m,$$

by solving a quadratic polynomial system in n variables and m equations.

Supporting heuristics in the algebraic analysis of attacks.

Direct attack against UOV

Given $\boldsymbol{t} = \mathcal{H}(M) \in \mathbb{F}_q^m$, find $\boldsymbol{x} \in \mathbb{F}_q^n$ such that

$$p_1(\boldsymbol{x}) = t_1, \ \ldots, \ p_m(\boldsymbol{x}) = t_m,$$

by solving a quadratic polynomial system in n variables and m equations.

The analysis requires two hypotheses:

1. The public key $(p_1, \ldots, p_m)$ is a regular sequence.

Supporting heuristics in the algebraic analysis of attacks.

Direct attack against UOV

Given $\boldsymbol{t} = \mathcal{H}(M) \in \mathbb{F}_q^m$, find $\boldsymbol{x} \in \mathbb{F}_q^n$ such that

$$p_1(\boldsymbol{x}) = t_1, \ \ldots, \ p_m(\boldsymbol{x}) = t_m,$$

by solving a quadratic polynomial system in n variables and m equations.

The analysis requires two hypotheses:

1. The public key $(p_1, \ldots, p_m)$ is a regular sequence.
The system has the expected dimension, and the behavior of Gröbner bases algorithms is predictable when $n = m$.
$\longrightarrow$ Holds for all $\mathcal{P} \in \mathcal{U}$.

Supporting heuristics in the algebraic analysis of attacks.

Direct attack against UOV

Given $\boldsymbol{t} = \mathcal{H}(M) \in \mathbb{F}_q^m$, find $\boldsymbol{x} \in \mathbb{F}_q^n$ such that

$$p_1(\boldsymbol{x}) = t_1, \ \ldots, \ p_m(\boldsymbol{x}) = t_m,$$

by solving a quadratic polynomial system in n variables and m equations.

The analysis requires two hypotheses:

1. The public key $(p_1, \ldots, p_m)$ is a regular sequence.
The system has the expected dimension, and the behavior of Gröbner bases algorithms is predictable when $n = m$.
$\longrightarrow$ Holds for all $\mathcal{P} \in \mathcal{U}$.

2. For $k \geq 0$ and linear polynomials $h_1, \ldots, h_{n-m+k}$ in general position, $p_1, \ldots, p_m, h_1, \ldots, h_{n-m+k}$ is a semi-regular sequence.

Supporting heuristics in the algebraic analysis of attacks.

Direct attack against UOV

Given $\boldsymbol{t} = \mathcal{H}(M) \in \mathbb{F}_q^m$, find $\boldsymbol{x} \in \mathbb{F}_q^n$ such that

$$p_1(\boldsymbol{x}) = t_1, \ \ldots, \ p_m(\boldsymbol{x}) = t_m,$$

by solving a quadratic polynomial system in n variables and m equations.

The analysis requires two hypotheses:

1. The public key $(p_1, \ldots, p_m)$ is a regular sequence.
The system has the expected dimension, and the behavior of Gröbner bases algorithms is predictable when $n = m$.
$\longrightarrow$ Holds for all $\mathcal{P} \in \mathcal{U}$.

2. For $k \geq 0$ and linear polynomials $h_1, \ldots, h_{n-m+k}$ in general position, $p_1, \ldots, p_m, h_1, \ldots, h_{n-m+k}$ is a semi-regular sequence.
The behavior of Gröbner bases algorithms remains predictable when $n < m$.
$\longrightarrow$ Special case of Fröberg's conjecture [Fröberg 85].

Supporting heuristics in the algebraic analysis of attacks.

Direct attack against UOV

Given $\boldsymbol{t} = \mathcal{H}(M) \in \mathbb{F}_q^m$, find $\boldsymbol{x} \in \mathbb{F}_q^n$ such that

$$p_1(\boldsymbol{x}) = t_1, \ \ldots, \ p_m(\boldsymbol{x}) = t_m,$$

by solving a quadratic polynomial system in n variables and m equations.

The analysis requires two hypotheses:

1. The public key $(p_1, \ldots, p_m)$ is a regular sequence.
The system has the expected dimension, and the behavior of Gröbner bases algorithms is predictable when $n = m$.
$\longrightarrow$ Holds for all $\mathcal{P} \in \mathcal{U}$.

2. For $k \geq 0$ and linear polynomials $h_1, \ldots, h_{n-m+k}$ in general position, $p_1, \ldots, p_m, h_1, \ldots, h_{n-m+k}$ is a semi-regular sequence.
The behavior of Gröbner bases algorithms remains predictable when $n < m$.
$\longrightarrow$ Special case of Fröberg's conjecture [Fröberg 85].

This property is not a given in multivariate cryptography.

- (Perturbed) HFE systems did not define (semi-)regular sequences and could be distinguished from generic sequences at relatively low degrees (see [Petzoldt 17]).

Supporting heuristics in the algebraic analysis of attacks.

Direct attack against UOV

Given $\boldsymbol{t} = \mathcal{H}(M) \in \mathbb{F}_q^m$, find $\boldsymbol{x} \in \mathbb{F}_q^n$ such that

$$p_1(\boldsymbol{x}) = t_1, \ \ldots, \ p_m(\boldsymbol{x}) = t_m,$$

by solving a quadratic polynomial system in n variables and m equations.

The analysis requires two hypotheses:

1. The public key $(p_1, \ldots, p_m)$ is a regular sequence.
The system has the expected dimension, and the behavior of Gröbner bases algorithms is predictable when $n = m$.
$\longrightarrow$ Holds for all $\mathcal{P} \in \mathcal{U}$.

2. For $k \geq 0$ and linear polynomials $h_1, \ldots, h_{n-m+k}$ in general position, $p_1, \ldots, p_m, h_1, \ldots, h_{n-m+k}$ is a semi-regular sequence.
The behavior of Gröbner bases algorithms remains predictable when $n < m$.
$\longrightarrow$ Special case of Fröberg's conjecture [Fröberg 85].

This property is not a given in multivariate cryptography.

- (Perturbed) HFE systems did not define (semi-)regular sequences and could be distinguished from generic sequences at relatively low degrees (see [Petzoldt 17]).
- Irregular UOV keys (ie $n - m < o$) are not regular sequences (early MAYO parameters, QR-UOV/SNOVA big field instances, VOX, ...).

Determinantal varieties of UOV and application to MinRank attacks.

Dimension of determinantal varieties

- If $M \in \mathbb{K}[X_1, \ldots, X_n]^{p \times q}$, the ideal of minors of degree $r+1$ of M has codimension at most $(p-r) \times (q-r)$. [Bruns, Vetter 1988]

Determinantal varieties of UOV and application to MinRank attacks.

Dimension of determinantal varieties

- If $M \in \mathbb{K}[X_1, \ldots, X_n]^{p \times q}$, the ideal of minors of degree $r+1$ of M has codimension at most $(p-r) \times (q-r)$. [Bruns, Vetter 1988]
- Equality for **generic** polynomial matrices. [Faugère, Safey el Din, Spaenlehauer 2011]

Determinantal varieties of UOV and application to MinRank attacks.

Dimension of determinantal varieties

- If $M \in \mathbb{K}[X_1, \ldots, X_n]^{p \times q}$, the ideal of minors of degree $r+1$ of M has codimension at most $(p-r) \times (q-r)$. [Bruns, Vetter 1988]
- Equality for **generic** polynomial matrices. [Faugère, Safey el Din, Spaenlehauer 2011]

MinRank attacks against UOV and variants

- Rectangular MinRank [Beullens 22], [FI 23], [SFINU 26]

Determinantal varieties of UOV and application to MinRank attacks.

Dimension of determinantal varieties

- If $M \in \mathbb{K}[X_1, \ldots, X_n]^{p \times q}$, the ideal of minors of degree $r+1$ of M has codimension at most $(p-r) \times (q-r)$. [Bruns, Vetter 1988]
- Equality for **generic** polynomial matrices. [Faugère, Safey el Din, Spaenlehauer 2011]

MinRank attacks against UOV and variants

- Rectangular MinRank [Beullens 22], [FI 23], [SFINU 26]
- Tangent spaces and singular points [P. 24, 25]

All these attacks solve MinRank problems on Jacobian matrices.

Determinantal varieties of UOV and application to MinRank attacks.

Dimension of determinantal varieties

- If $M \in \mathbb{K}[X_1, \ldots, X_n]^{p \times q}$, the ideal of minors of degree $r+1$ of M has codimension at most $(p-r) \times (q-r)$. [Bruns, Vetter 1988]
- Equality for **generic** polynomial matrices. [Faugère, Safey el Din, Spaenlehauer 2011]

MinRank attacks against UOV and variants

- Rectangular MinRank [Beullens 22], [FI 23], [SFINU 26]
- Tangent spaces and singular points [P. 24, 25]

All these attacks solve MinRank problems on Jacobian matrices.

Jacobian matrices are not generic: cannot apply [FSS11] out of the box.

Determinantal varieties of UOV and application to MinRank attacks.

Dimension of determinantal varieties

- If $M \in \mathbb{K}[X_1, \ldots, X_n]^{p \times q}$, the ideal of minors of degree $r+1$ of M has codimension at most $(p-r) \times (q-r)$. [Bruns, Vetter 1988]
- Equality for **generic** polynomial matrices. [Faugère, Safey el Din, Spaenlehauer 2011]

MinRank attacks against UOV and variants

- Rectangular MinRank [Beullens 22], [FI 23], [SFINU 26]
- Tangent spaces and singular points [P. 24, 25]

All these attacks solve MinRank problems on Jacobian matrices.

Jacobian matrices are not generic: cannot apply [FSS11] out of the box.

Generic determinantal ideals of UOV and dimension of the tangent spaces **This work**

Consider (n, m, o, q) with $n \geq 2o$ and $n - m > o$. There exists a Zariski-open set of UOV keys $\mathcal{M}_r$ such that for all $\mathcal{F} \in \mathcal{M}_r$, the ideal $I(\mathcal{O}) \cap \mathrm{Minors}_{r+1}(\mathrm{Jac}_{\mathcal{F}})$ has the expected dimension.

Supporting heuristics in the geometric analysis of MinRank attacks.

Geometry of MinRank attacks [Suzuki, Furue, Ito, Nakamura, Uchiyama 26]

- The Rectangular MinRank attacks [Beullens 22], [Furue, Ikematsu 23] are, in a way, generalizations of the singular points attack [P. 25] (which generalizes the Kipnis-Shamir attack [Kipnis, Patarin, Goubin 99]).

Supporting heuristics in the geometric analysis of MinRank attacks.

Geometry of MinRank attacks **[Suzuki, Furue, Ito, Nakamura, Uchiyama 26]**

- The Rectangular MinRank attacks [Beullens 22], [Furue, Ikematsu 23] are, in a way, generalizations of the singular points attack [P. 25] (which generalizes the Kipnis-Shamir attack [Kipnis, Patarin, Goubin 99]).
- As a consequence, the study of determinantal ideals from singular points can be generalized to improve the Rectangular MinRank attacks against UOV variants.

Supporting heuristics in the geometric analysis of MinRank attacks.

Geometry of MinRank attacks **[Suzuki, Furue, Ito, Nakamura, Uchiyama 26]**

- The Rectangular MinRank attacks [Beullens 22], [Furue, Ikematsu 23] are, in a way, generalizations of the singular points attack [P. 25] (which generalizes the Kipnis-Shamir attack [Kipnis, Patarin, Goubin 99]).
- As a consequence, the study of determinantal ideals from singular points can be generalized to improve the Rectangular MinRank attacks against UOV variants.

These connections highlight a series of heuristics.

Supporting heuristics in the geometric analysis of MinRank attacks.

Geometry of MinRank attacks **[Suzuki, Furue, Ito, Nakamura, Uchiyama 26]**

- The Rectangular MinRank attacks [Beullens 22], [Furue, Ikematsu 23] are, in a way, generalizations of the singular points attack [P. 25] (which generalizes the Kipnis-Shamir attack [Kipnis, Patarin, Goubin 99]).
- As a consequence, the study of determinantal ideals from singular points can be generalized to improve the Rectangular MinRank attacks against UOV variants.

These connections highlight a series of heuristics.

- $\dim V(\mathcal{I}) = max(n-m, o)$ to apply the Jacobian Criterion. [P. 25, SFINU 26]
  $\longrightarrow$ holds for all $\mathcal{P} \in \mathcal{U}$.

Supporting heuristics in the geometric analysis of MinRank attacks.

Geometry of MinRank attacks [Suzuki, Furue, Ito, Nakamura, Uchiyama 26]

- The Rectangular MinRank attacks [Beullens 22], [Furue, Ikematsu 23] are, in a way, generalizations of the singular points attack [P. 25] (which generalizes the Kipnis-Shamir attack [Kipnis, Patarin, Goubin 99]).
- As a consequence, the study of determinantal ideals from singular points can be generalized to improve the Rectangular MinRank attacks against UOV variants.

These connections highlight a series of heuristics.

- $\dim V(\mathcal{I}) = max(n-m, o)$ to apply the Jacobian Criterion. [P. 25, SFINU 26]
  $\longrightarrow$ holds for all $\mathcal{P} \in \mathcal{U}$.
- $\mathrm{Sing}\, V(\mathcal{I}) \subset \mathcal{O}$ to obtain key recovery attacks. [KPG 99, P. 25, SFINU 26]
  $\longrightarrow$ holds for all $\mathcal{P} \in \mathcal{U}$.

Supporting heuristics in the geometric analysis of MinRank attacks.

Geometry of MinRank attacks [Suzuki, Furue, Ito, Nakamura, Uchiyama 26]

- The Rectangular MinRank attacks [Beullens 22], [Furue, Ikematsu 23] are, in a way, generalizations of the singular points attack [P. 25] (which generalizes the Kipnis-Shamir attack [Kipnis, Patarin, Goubin 99]).
- As a consequence, the study of determinantal ideals from singular points can be generalized to improve the Rectangular MinRank attacks against UOV variants.

These connections highlight a series of heuristics.

- $\dim V(\mathcal{I}) = max(n-m, o)$ to apply the Jacobian Criterion. [P. 25, SFINU 26]
  $\longrightarrow$ holds for all $\mathcal{P} \in \mathcal{U}$.
- $\mathrm{Sing}\, V(\mathcal{I}) \subset \mathcal{O}$ to obtain key recovery attacks. [KPG 99, P. 25, SFINU 26]
  $\longrightarrow$ holds for all $\mathcal{P} \in \mathcal{U}$.
- Jacobian determinantal ideals of UOV have the expected dimension. [SFINU 26]
  $\longrightarrow$ holds for all $\mathcal{P} \in \mathcal{M}_r$.

Kipnis-Shamir and singular points [KS 98], [KPG 99], [Luyten 2023], [P. 2025]

Kipnis-Shamir attack when $n < 2o + m$.

Write $P'_i = P_i + P_i^T$. We have $P'_i\mathcal{O} \subset \mathcal{O}^\perp$ for all i. $\dim P'_i\mathcal{O} \cap P'_j\mathcal{O} = 2o + m - n > 0$ and elements of $\mathcal{O}$ can be eigenvectors of $P_j'^{-1}P'_i$.

Kipnis-Shamir and singular points [KS 98], [KPG 99], [Luyten 2023], [P. 2025]

Kipnis-Shamir attack when $n < 2o + m$.

Write $P'_i = P_i + P_i^T$. We have $P'_i\mathcal{O} \subset \mathcal{O}^\perp$ for all i. $\dim P'_i\mathcal{O} \cap P'_j\mathcal{O} = 2o + m - n > 0$ and elements of $\mathcal{O}$ can be eigenvectors of $P_j'^{-1}P'_i$.

Geometric interpretation [Luyten 2023][P. 2025]

It holds that $\mathrm{Jac}_{\boldsymbol{x}}(\mathcal{P}) = 2(\boldsymbol{x}^T P'_1, \ldots, \boldsymbol{x}^T P'_m)^T$, thus a point $\boldsymbol{x} \in V$ is singular if and only if $\exists \boldsymbol{\lambda} \neq 0, (\lambda_1, \ldots, \lambda_m)\mathrm{Jac}_{\boldsymbol{x}}(\mathcal{P}) = 0 \in \mathbb{F}_q^n$ if and only if $\left(\sum_k \lambda_k P'_k\right)\boldsymbol{x} = 0$.

On the other hand, $\boldsymbol{x} \in \mathcal{O}$ is an eigenvector of $P_j'^{-1}P'_i$ if and only if $(P'_i - \lambda P'_j)\boldsymbol{x} = 0$.
$\rightarrow$**Kipnis-Shamir returns singular points of V.**

Experimental results.

Method

Compute Gröbner bases of ideals defined by UOV keys sampled uniformly at random in finite fields of various size and characteristic, with 1000 samples in each case.

n, m, o	r	$\mathcal{D}_{16}$	$\mathcal{D}_{31}$	$\mathcal{D}_{251}$	$\mathcal{D}_{1021}$	$\mathcal{D}_{4093}$
10, 4, 4	1	93.3%	96.5%	99.8%	100%	99.9%
10, 5, 5	1	99.9%	99.9%	100%	100%	100%
	2	93.1%	97.6%	99.4%	99.7%	100%
12, 5, 5	1	99.5%	100%	100%	100%	100%
12, 7, 5	1	100%	99.9%	100%	100%	100%
	2	94.4%	97.6%	99.6%	99.8%	100%
12, 6, 6	1	100%	100%	100%	100%	100%
	2	99.4%	100%	100%	100%	100%
14, 6, 6	1	100%	100%	100%	100%	100%
14, 8, 6	1	100%	99.6%	100%	100%	100%

Figure 2: Proportion of UOV keys in the Zariski open sets $\mathcal{M}_{m-r}$.

Experimental results.

Method

Compute Gröbner bases of ideals defined by UOV keys sampled uniformly at random in finite fields of various size and characteristic, with 1000 samples in each case.

When $r = 1$, we obtain a result on both $\mathcal{U}$ and $\mathcal{M}_{m-r}$. $\mathcal{U}$ can also be studied by running Kipnis-Shamir attacks.

n, m, o	r	$\mathcal{D}_{16}$	$\mathcal{D}_{31}$	$\mathcal{D}_{251}$	$\mathcal{D}_{1021}$	$\mathcal{D}_{4093}$
10, 4, 4	1	93.3%	96.5%	99.8%	100%	99.9%
10, 5, 5	1	99.9%	99.9%	100%	100%	100%
	2	93.1%	97.6%	99.4%	99.7%	100%
12, 5, 5	1	99.5%	100%	100%	100%	100%
12, 7, 5	1	100%	99.9%	100%	100%	100%
	2	94.4%	97.6%	99.6%	99.8%	100%
12, 6, 6	1	100%	100%	100%	100%	100%
	2	99.4%	100%	100%	100%	100%
14, 6, 6	1	100%	100%	100%	100%	100%
14, 8, 6	1	100%	99.6%	100%	100%	100%

Figure 2: Proportion of UOV keys in the Zariski open sets $\mathcal{M}_{m-r}$.

Experimental results.

Method

Compute Gröbner bases of ideals defined by UOV keys sampled uniformly at random in finite fields of various size and characteristic, with 1000 samples in each case.

When $r = 1$, we obtain a result on both $\mathcal{U}$ and $\mathcal{M}_{m-r}$. $\mathcal{U}$ can also be studied by running Kipnis-Shamir attacks.

n, m, o	r	$\mathcal{D}_{16}$	$\mathcal{D}_{31}$	$\mathcal{D}_{251}$	$\mathcal{D}_{1021}$	$\mathcal{D}_{4093}$
10, 4, 4	1	93.3%	96.5%	99.8%	100%	99.9%
10, 5, 5	1	99.9%	99.9%	100%	100%	100%
	2	93.1%	97.6%	99.4%	99.7%	100%
12, 5, 5	1	99.5%	100%	100%	100%	100%
12, 7, 5	1	100%	99.9%	100%	100%	100%
	2	94.4%	97.6%	99.6%	99.8%	100%
12, 6, 6	1	100%	100%	100%	100%	100%
	2	99.4%	100%	100%	100%	100%
14, 6, 6	1	100%	100%	100%	100%	100%
14, 8, 6	1	100%	99.6%	100%	100%	100%

Figure 2: Proportion of UOV keys in the Zariski open sets $\mathcal{M}_{m-r}$.

Remark on UOV public keys forming regular sequences.

Widely reproduced experiments in the literature (see e.g. [Faugère, Perret 09]).
Unsurprisingly, we are also able to reproduce these results (with 100% success, even in $\mathbb{F}_2$).
Method: sample UOV keys uniformly and compute the Hilbert series of the sequence.

Open problems and conclusion

Weak keys from failure of genericity

[Beullens 2025] attack on SNOVA exploits failures of genericity to find increasing rank defects for decreasing proportions of public keys.

Open problems and conclusion

Weak keys from failure of genericity

[Beullens 2025] attack on SNOVA exploits failures of genericity to find increasing rank defects for decreasing proportions of public keys.

1. Can one quantify the proportion of keys that fail a given genericity assumption?

Open problems and conclusion

Weak keys from failure of genericity

[Beullens 2025] attack on SNOVA exploits failures of genericity to find increasing rank defects for decreasing proportions of public keys.

1. Can one quantify the proportion of keys that fail a given genericity assumption?
2. Can one leverage failure of genericity assumptions to improve or obtain attacks?

Open problems and conclusion

Weak keys from failure of genericity

[Beullens 2025] attack on SNOVA exploits failures of genericity to find increasing rank defects for decreasing proportions of public keys.

1. Can one quantify the proportion of keys that fail a given genericity assumption?
2. Can one leverage failure of genericity assumptions to improve or obtain attacks?

$\longrightarrow$ *Genericity results are not proofs of security.*

Open problems and conclusion

Weak keys from failure of genericity

[Beullens 2025] attack on SNOVA exploits failures of genericity to find increasing rank defects for decreasing proportions of public keys.

1. Can one quantify the proportion of keys that fail a given genericity assumption?
2. Can one leverage failure of genericity assumptions to improve or obtain attacks?

$\longrightarrow$ *Genericity results are not proofs of security.*

Adapting results from code-based crypto

Gröbner basis computations to find points can be sped-up on some non-radical ideals (see [Bardet, Lemoine, Tillich 2026]).

Open problems and conclusion

Weak keys from failure of genericity

[Beullens 2025] attack on SNOVA exploits failures of genericity to find increasing rank defects for decreasing proportions of public keys.

1. Can one quantify the proportion of keys that fail a given genericity assumption?
2. Can one leverage failure of genericity assumptions to improve or obtain attacks?

$\longrightarrow$ *Genericity results are not proofs of security.*

Adapting results from code-based crypto

Gröbner basis computations to find points can be sped-up on some non-radical ideals (see [Bardet, Lemoine, Tillich 2026]).

- Regularity of other attacks (Reconciliation, Intersection), and specifically on structured variants (SNOVA).

Open problems and conclusion

Weak keys from failure of genericity

[Beullens 2025] attack on SNOVA exploits failures of genericity to find increasing rank defects for decreasing proportions of public keys.

1. Can one quantify the proportion of keys that fail a given genericity assumption?
2. Can one leverage failure of genericity assumptions to improve or obtain attacks?

$\longrightarrow$ *Genericity results are not proofs of security.*

Adapting results from code-based crypto

Gröbner basis computations to find points can be sped-up on some non-radical ideals (see [Bardet, Lemoine, Tillich 2026]).

- Regularity of other attacks (Reconciliation, Intersection), and specifically on structured variants (SNOVA).
- Study the Fröberg conjecture specialized to multivariate cryptography (finite fields, quadratic polynomials).

Open problems and conclusion

Weak keys from failure of genericity

[Beullens 2025] attack on SNOVA exploits failures of genericity to find increasing rank defects for decreasing proportions of public keys.

1. Can one quantify the proportion of keys that fail a given genericity assumption?
2. Can one leverage failure of genericity assumptions to improve or obtain attacks?

$\longrightarrow$ *Genericity results are not proofs of security.*

Adapting results from code-based crypto

Gröbner basis computations to find points can be sped-up on some non-radical ideals (see [Bardet, Lemoine, Tillich 2026]).

- Regularity of other attacks (Reconciliation, Intersection), and specifically on structured variants (SNOVA).
- Study the Fröberg conjecture specialized to multivariate cryptography (finite fields, quadratic polynomials).

Preliminary version in Chap. 5 of my thesis: `https://theses.hal.science/tel-05605746`.
Experiments and code on GitHub soon, ask for code by email!