Geometric approach to the cryptanalysis of post-quantum multivariate signature schemes

Pierre Pébereau
Sorbonne Université, LIP6, CNRS, Thales SIX

December 16th, 2025

Ancient problem, modern solutions

Historical ciphers

- Polybus (150 B.C.)
- Caesar (50 B.C.)
- Vigenère (1586)

pen-and-paper ciphers

Ancient problem, modern solutions

Historical ciphers

- Polybus (150 B.C.)
- Caesar (50 B.C.)
- Vigenère (1586)

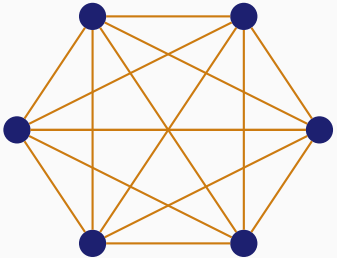
pen-and-paper ciphers

Symmetric cryptography

- One-time-pad (1917)
- Enigma (WWII)
- DES/AES (1977/2000)

electromechanical/block ciphers

Secret key: one key per **link**:
6 participants: 15 keys.
100 participants: 4950 keys.



Ancient problem, modern solutions

Historical ciphers

- Polybus (150 B.C.)
- Caesar (50 B.C.)
- Vigenère (1586)

pen-and-paper ciphers

Symmetric cryptography

- One-time-pad (1917)
- Enigma (WWII)
- DES/AES (1977/2000)

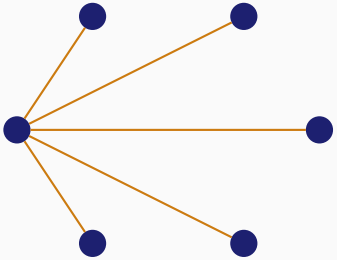
electromechanical/block ciphers

Public key cryptography

- Diffie, Hellman (1973)
- Rivest, Shamir, Adleman (1977)
- EdDSA (2011)

$\longrightarrow$ secure internet, credit cards ...

Secret key: one key per **link**:
6 participants: 15 keys.
100 participants: 4950 keys.



Public key: one key per **node**:
6 participants: 6 keys.
100 participants: 100 keys.

Ancient problem, modern solutions

Historical ciphers

- Polybus (150 B.C.)
- Caesar (50 B.C.)
- Vigenère (1586)

pen-and-paper ciphers

Symmetric cryptography

- One-time-pad (1917)
- Enigma (WWII)
- DES/AES (1977/2000)

electromechanical/block ciphers

Public key cryptography

- Diffie, Hellman (1973)
- Rivest, Shamir, Adleman (1977)
- EdDSA (2011)

$\longrightarrow$ secure internet, credit cards ...

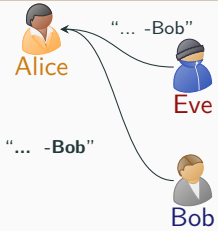
Modern cybersecurity goals

- **Confidentiality**: the information is only available to the intended recipient.
- **Integrity**: the information has not been modified after being sent.
- **Authenticity**: the information was sent by a specific, authenticated sender.

The public key revolution [Diffie, Hellman 1973]

Problem

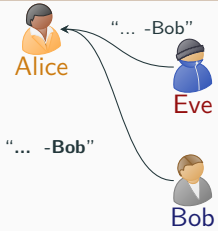
- How to **authenticate** oneself over an **untrusted** network?
- How to verify **integrity** over an **untrusted** network?



The public key revolution [Diffie, Hellman 1973]

Problem

- How to **authenticate** oneself over an **untrusted** network?
- How to verify **integrity** over an **untrusted** network?



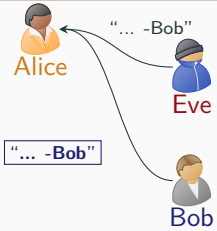
Solution: Public key cryptography [Diffie, Hellman 1973]

- **Bob** generates a **key pair**: a private key, and a public key **available to all**

The public key revolution [Diffie, Hellman 1973]

Problem

- How to **authenticate** oneself over an **untrusted** network?
- How to verify **integrity** over an **untrusted** network?



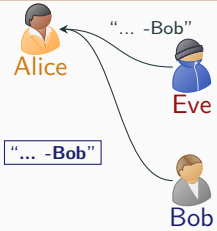
Solution: Public key cryptography [Diffie, Hellman 1973]

- **Bob** generates a **key pair**: a private key, and a public key **available to all**
- **Bob** **signs** his message with his private key

The public key revolution [Diffie, Hellman 1973]

Problem

- How to **authenticate** oneself over an **untrusted** network?
- How to verify **integrity** over an **untrusted** network?



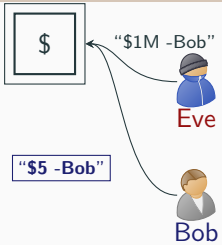
Solution: Public key cryptography [Diffie, Hellman 1973]

- **Bob** generates a **key pair**: a private key, and a public key **available to all**
- **Bob** **signs** his message with his private key
- public key enables **Alice** to **verify Bob**'s **signature** of the message

The public key revolution [Diffie, Hellman 1973]

Problem

- How to **authenticate** oneself over an **untrusted** network?
- How to verify **integrity** over an **untrusted** network?



Solution: Public key cryptography [Diffie, Hellman 1973]

- **Bob** generates a **key pair**: a private key, and a public key **available to all**
- **Bob** **signs** his message with his private key
- public key enables **Alice** to **verify Bob**'s **signature** of the message

Can **Eve** pretend to be **Bob**?

New revolution: Post Quantum Cryptography

Signatures in protocols

- TLS: create a **secure** channel over an untrusted network. 🔒 in your browser
- DNSSEC, SSH, ...

New revolution: Post Quantum Cryptography

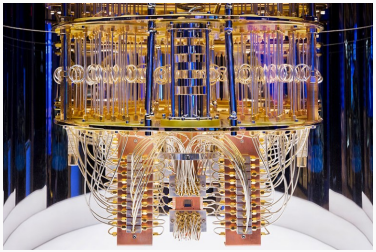
Signatures in protocols

- TLS: create a **secure** channel over an untrusted network. 🔒 in your browser
- DNSSEC, SSH, ...

Quantum threat

If **Eve** has a large quantum computer, she can compute private keys in these protocols [Shor 94].

Can we obtain **Post-Quantum** TLS?



Source: IBM Research.

New revolution: Post Quantum Cryptography

Signatures in protocols

- TLS: create a **secure** channel over an untrusted network. 🔒 in your browser
- DNSSEC, SSH, ...

Good news: many quantum-hard problems

- Finding short vectors in Euclidean lattices

Quantum threat

If **Eve** has a large quantum computer, she can compute private keys in these protocols [Shor 94].

Can we obtain **Post-Quantum** TLS?

New revolution: Post Quantum Cryptography

Signatures in protocols

- TLS: create a **secure** channel over an untrusted network. 🔒 in your browser
- DNSSEC, SSH, ...

Good news: many quantum-hard problems

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

Quantum threat

If **Eve** has a large quantum computer, she can compute private keys in these protocols [Shor 94].

Can we obtain **Post-Quantum** TLS?

New revolution: Post Quantum Cryptography

Signatures in protocols

- TLS: create a **secure** channel over an untrusted network. 🔒 in your browser
- DNSSEC, SSH, ...

Good news: many quantum-hard problems

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

Quantum threat

If **Eve** has a large quantum computer, she can compute private keys in these protocols [Shor 94].

Can we obtain **Post-Quantum** TLS?

Bad news: security is expensive

Severe impact on performance and **size** of cryptographic data causes fragmentation

New revolution: Post Quantum Cryptography

Signatures in protocols

- TLS: create a **secure** channel over an untrusted network. 🔒 in your browser
- DNSSEC, SSH, ...

Good news: many quantum-hard problems

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

Quantum threat

If **Eve** has a large quantum computer, she can compute private keys in these protocols [Shor 94].

Can we obtain **Post-Quantum** TLS?

Bad news: security is expensive

Severe impact on performance and **size** of cryptographic data causes fragmentation

	Signature	Public key
EdDSA	64 bytes	32 bytes
ML-DSA	**2 420** bytes	**1 312** bytes

New revolution: Post Quantum Cryptography

Signatures in protocols

- TLS: create a **secure** channel over an untrusted network. 🔒 in your browser
- DNSSEC, SSH, ...

Good news: many quantum-hard problems

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

Quantum threat

If **Eve** has a large quantum computer, she can compute private keys in these protocols [Shor 94].

Can we obtain **Post-Quantum** TLS?

Bad news: security is expensive

Severe impact on performance and **size** of cryptographic data causes fragmentation

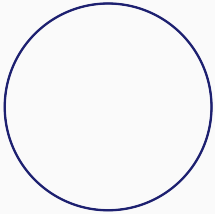
	Signature	Public key
EdDSA	64 bytes	32 bytes
ML-DSA	**2 420** bytes	**1 312** bytes

Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

$$X^2 + Y^2 - 1 = 0$$



Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

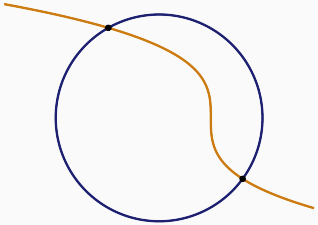
$$2X + 3Y^3 - 1 = 0$$

Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

$$X^2 + Y^2 - 1 = 0$$
$$2X + 3Y^3 - 1 = 0$$

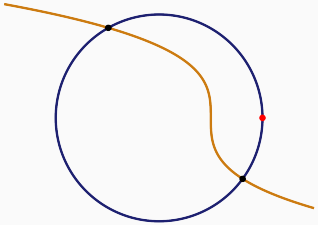


Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

$$X^2 + Y^2 - 1 = 0$$
$$2X + 3Y^3 - 1 = 0$$



Polynomial system solving is NP

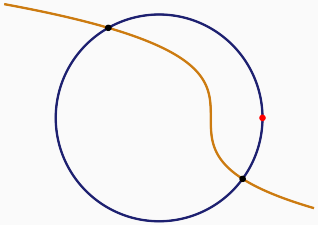
- Testing a solution is **easy**: "Is $(1, 0)$ a solution?"

Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

$$1 \times 1 + 0 \times 0 - 1 = 0$$
$$2X + 3Y^3 - 1 = 0$$



Polynomial system solving is NP

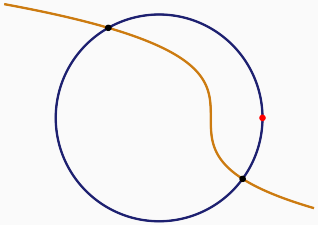
- Testing a solution is **easy**: "Is $(1, 0)$ a solution?"

Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

$$0 = 0 \text{ YES}$$
$$2X + 3Y^3 - 1 = 0$$



Polynomial system solving is NP

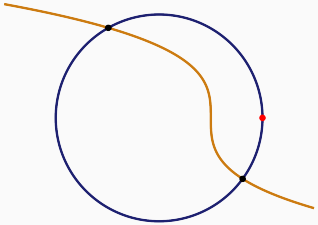
- Testing a solution is **easy**: "Is $(1, 0)$ a solution?"

Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

$$0 = 0 \text{ YES}$$
$$2 \times 1 + 3 \times 0 - 1 = 0$$



Polynomial system solving is NP

- Testing a solution is **easy**: "Is $(1, 0)$ a solution?"

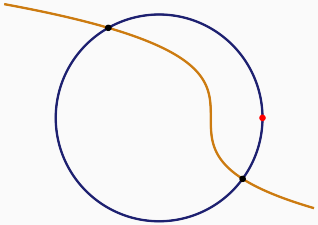
Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

$0 = 0$ YES

$1 = 0$ NO



Polynomial system solving is NP

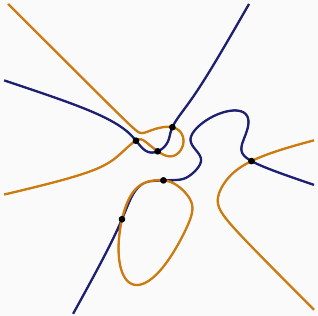
- Testing a solution is **easy**: "Is $(1, 0)$ a solution?" $\longrightarrow$ NO.

Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

$$X^6 + 2X^5Y - 3X^4Y^2 + X^3Y^3 + 4X^2Y^4 + 3XY^5 - 3Y^6 - 4X^5 - 2X^4Y - X^3Y^2 - X^2Y^3 + 4XY^4 - 2Y^5 + 4X^4 - 4X^3Y - 3X^2Y^2 + Y^4 - 3X^3 + 2X^2Y + 2XY^2 + 4Y^3 + 2X^2 + 4XY - 4Y^2 + X - 3Y + 1 = 0$$
$$- X^6 + 4X^5Y + 3X^4Y^2 + 3X^3Y^3 + 3X^2Y^4 - XY^5 + Y^6 + 2X^5 - 3X^4Y + X^2Y^3 + XY^4 + 3Y^5 + 3X^4 + 3X^3Y - 2X^2Y^2 - XY^3 - Y^4 + X^3 - 2X^2Y + 2XY^2 + 4Y^3 + 3X^2 - 2XY - 4Y^2 - 3X - 4Y + 1 = 0$$



Polynomial system solving is NP

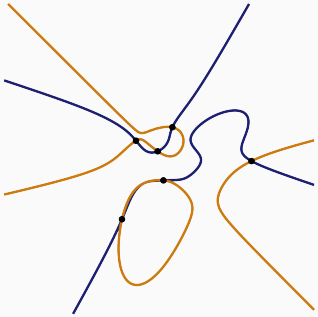
- Testing a solution is **easy**: "Is $(1, 0)$ a solution?"

Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

$$X^6 + 2X^5Y - 3X^4Y^2 + X^3Y^3 + 4X^2Y^4 + 3XY^5 - 3Y^6 - 4X^5 - 2X^4Y - X^3Y^2 - X^2Y^3 + 4XY^4 - 2Y^5 + 4X^4 - 4X^3Y - 3X^2Y^2 + Y^4 - 3X^3 + 2X^2Y + 2XY^2 + 4Y^3 + 2X^2 + 4XY - 4Y^2 + X - 3Y + 1 = 0$$
$$- X^6 + 4X^5Y + 3X^4Y^2 + 3X^3Y^3 + 3X^2Y^4 - XY^5 + Y^6 + 2X^5 - 3X^4Y + X^2Y^3 + XY^4 + 3Y^5 + 3X^4 + 3X^3Y - 2X^2Y^2 - XY^3 - Y^4 + X^3 - 2X^2Y + 2XY^2 + 4Y^3 + 3X^2 - 2XY - 4Y^2 - 3X - 4Y + 1 = 0$$



Polynomial system solving is NP-hard

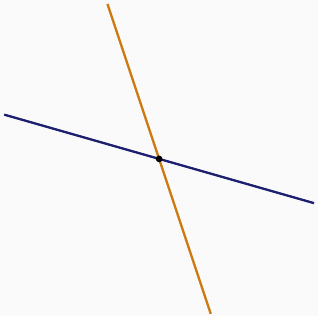
- Testing a solution is **easy**: "Is $(1, 0)$ a solution?"
- Finding a solution is **hard in degree at least two**. see [Garey, Johnson 1979]

Systems of multivariate polynomial equations

Algebraic geometry

The set of solutions of an **algebraic** equation is a **geometric** object called a **variety**.

$$2X + 7Y = 0$$
$$3X + 1Y = 0$$



Polynomial system solving is NP-hard

- Testing a solution is **easy**: "Is $(1, 0)$ a solution?"
- Finding a solution is **hard in degree at least two**. see [Garey, Johnson 1979]

Solving linear systems of equations is easy

Polynomial time algorithms for many linear algebra problems.

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]

Multivariate signature schemes: a template

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

Oil and Vinegar

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

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

$$Z - XY = 0.$$

Multivariate signature schemes: a template

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

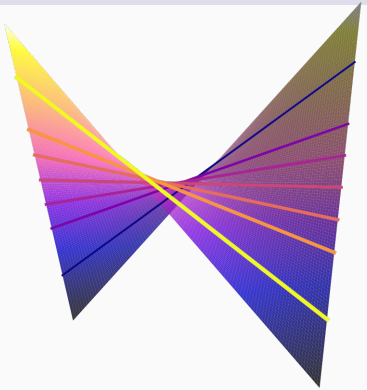
Oil and Vinegar

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



Multivariate signature schemes: a template

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

Oil and Vinegar

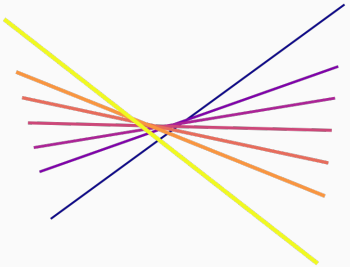
Private key: reduce to the **linear** case [Patarin '97]

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

$$Z - XY = 0.$$

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

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



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 $p_i = X^T \cdot P_i \cdot X = f_i \circ A$.

Multivariate signature schemes: a template

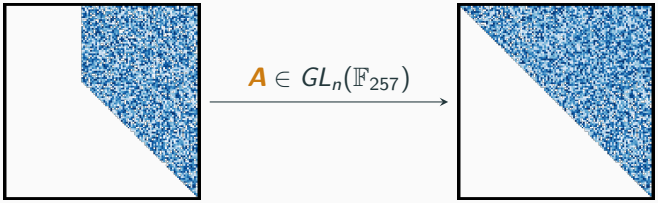
- **Public key**: a system of polynomial equations of degree two $\longrightarrow$ **Hard to solve**
- **Signature**: a solution of the public system of polynomial equations
- **Verification**: testing that a solution is correct $\longrightarrow$ **Easy to verify**

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

Cryptanalysis of UOV: forgery

Problem

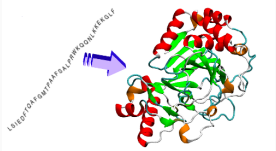
Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

Cryptanalysis of UOV: forgery

Problem

Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

Applications: *biology*, *optimization*, *physics*, *robotics*, ...

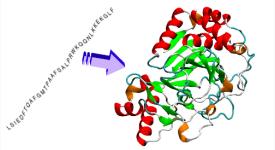


Cryptanalysis of UOV: forgery

Problem

Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

Applications: *biology*, *optimization*, *physics*, *robotics*, ...



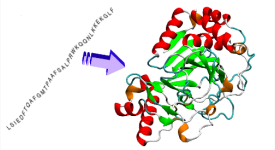
Mathematical history: [Descartes 1637], [Hilbert 1890], [Macaulay 1916], ...

Cryptanalysis of UOV: forgery

Problem

Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

Applications: *biology*, *optimization*, *physics*, *robotics*, ...



Mathematical history: [Descartes 1637], [Hilbert 1890], [Macaulay 1916], ...

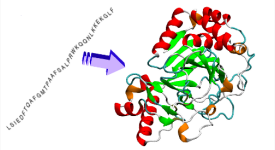
Gröbner basis algorithms & complexity: [Buchberger '65], [Lazard '83], [Giusti '84], [Traverso '89] [Faugère '99, 02], [Bardet, Faugère, Salvy 04, 05, 15].

Cryptanalysis of UOV: forgery

Problem

Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

Applications: *biology*, *optimization*, *physics*, *robotics*, ...



Mathematical history: [Descartes 1637], [Hilbert 1890], [Macaulay 1916], ...

Gröbner basis algorithms & complexity: [Buchberger '65], [Lazard '83], [Giusti '84], [Traverso '89] [Faugère '99, 02], [Bardet, Faugère, Salvy 04, 05, 15].

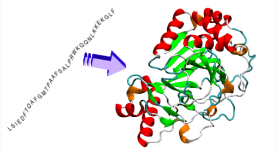
Quantum algorithms: [Grover '96], [Faugère, Horan, Kahrobaei, Kaplan, Kashefi, Perret 17], [Bernstein, Yang 17]

Cryptanalysis of UOV: forgery

Problem

Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

Applications: *biology*, *optimization*, *physics*, *robotics*, ...



Generators
degree d

Gröbner basis
algorithm

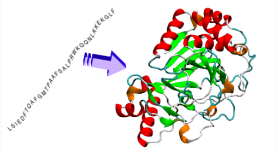
Mathematical history: [Descartes 1637], [Hilbert 1890], [Macaulay 1916], ...
Gröbner basis algorithms & complexity: [Buchberger '65], [Lazard '83], [Giusti '84], [Traverso '89] [Faugère '99, 02], [Bardet, Faugère, Salvy 04, 05, 15].
Quantum algorithms: [Grover '96], [Faugère, Horan, Kahrobaei, Kaplan, Kashefi, Perret 17], [Bernstein, Yang 17]

Cryptanalysis of UOV: forgery

Problem

Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

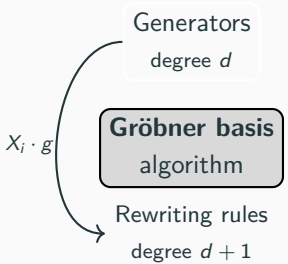
Applications: *biology*, *optimization*, *physics*, *robotics*, ...



Mathematical history: [Descartes 1637], [Hilbert 1890], [Macaulay 1916], ...

Gröbner basis algorithms & complexity: [Buchberger '65], [Lazard '83], [Giusti '84], [Traverso '89] [Faugère '99, 02], [Bardet, Faugère, Salvy 04, 05, 15].

Quantum algorithms: [Grover '96], [Faugère, Horan, Kahrobaei, Kaplan, Kashefi, Perret 17], [Bernstein, Yang 17]

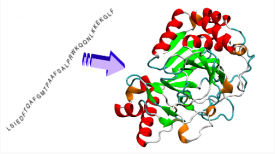


Cryptanalysis of UOV: forgery

Problem

Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

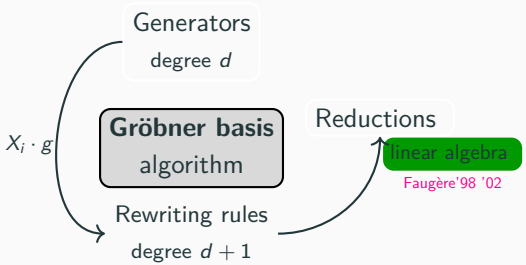
Applications: *biology*, *optimization*, *physics*, *robotics*, ...



Mathematical history: [Descartes 1637], [Hilbert 1890], [Macaulay 1916], ...

Gröbner basis algorithms & complexity: [Buchberger '65], [Lazard '83], [Giusti '84], [Traverso '89] [Faugère '99, 02], [Bardet, Faugère, Salvy 04, 05, 15].

Quantum algorithms: [Grover '96], [Faugère, Horan, Kahrobaei, Kaplan, Kashefi, Perret 17], [Bernstein, Yang 17]



Cryptanalysis of UOV: forgery

Problem

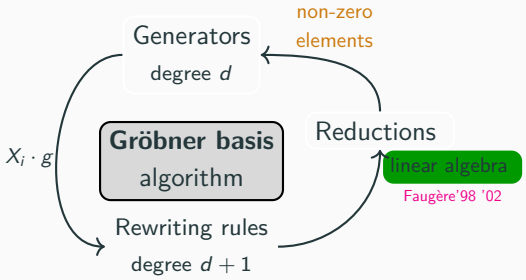
Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

Applications: *biology*, *optimization*, *physics*, *robotics*, ...

Mathematical history: [Descartes 1637], [Hilbert 1890], [Macaulay 1916], ...

Gröbner basis algorithms & complexity: [Buchberger '65], [Lazard '83], [Giusti '84], [Traverso '89] [Faugère '99, 02], [Bardet, Faugère, Salvy 04, 05, 15].

Quantum algorithms: [Grover '96], [Faugère, Horan, Kahrobaei, Kaplan, Kashefi, Perret 17], [Bernstein, Yang 17]

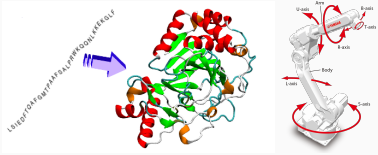


Cryptanalysis of UOV: forgery

Problem

Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

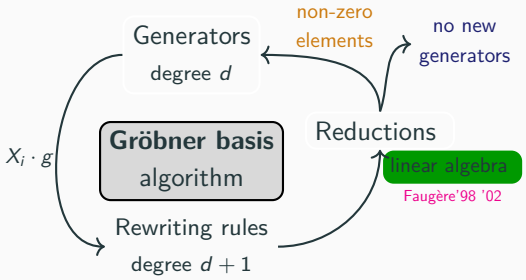
Applications: *biology*, *optimization*, *physics*, *robotics*, ...



Mathematical history: [Descartes 1637], [Hilbert 1890], [Macaulay 1916], ...

Gröbner basis algorithms & complexity: [Buchberger '65], [Lazard '83], [Giusti '84], [Traverso '89] [Faugère '99, 02], [Bardet, Faugère, Salvy 04, 05, 15].

Quantum algorithms: [Grover '96], [Faugère, Horan, Kahrobaei, Kaplan, Kashefi, Perret 17], [Bernstein, Yang 17]

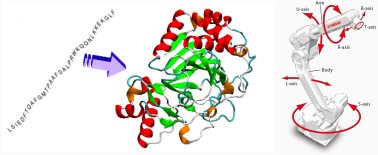


Cryptanalysis of UOV: forgery

Problem

Is it hard to find **a** solution of a *random* system of quadratic equations over a finite field?

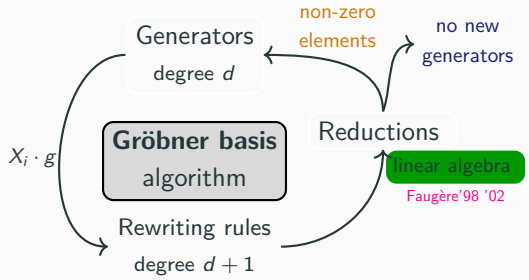
Applications: *biology, optimization, physics, robotics*, ...



Mathematical history: [Descartes 1637], [Hilbert 1890], [Macaulay 1916], ...

Gröbner basis algorithms & complexity: [Buchberger '65], [Lazard '83], [Giusti '84], [Traverso '89] [Faugère '99, 02], [Bardet, Faugère, Salvy 04, 05, 15].

Quantum algorithms: [Grover '96], [Faugère, Horan, Kahrobaei, Kaplan, Kashefi, Perret 17], [Bernstein, Yang 17]



Direct attack

With Gröbner basis algorithms, public systems are **indistinguishable** from random systems.

n, m	UOV	Generic
$10, 4$	6,16,6	6,16,6
$12, 5$	7, 32, 7	7, 32, 7
$15, 6$	9, 64, 8	9, 64, 8
$17, 7$	10, 128, 9	10, 128, 8

Dimension, degree and degree of regularity for systems in n variables and m quadratic equations.

Exploiting the geometry of UOV

Original UOV formulation [Patarin 1997] [Kipnis, Patarin, Goubin 1999]

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

Public key: $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, $\mathcal{I} = \langle p_1, \ldots, p_m \rangle, A \in GL_n(\mathbb{F}_q)$, $p_i = f_i \circ A$.

Exploiting the geometry of UOV

Original UOV formulation [Patarin 1997] [Kipnis, Patarin, Goubin 1999]

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

Private key: there exists a **linear subspace** $\mathcal{O} \subset V(\mathcal{I})$, $\dim \mathcal{O} = o$. [Kipnis Shamir 1998]

Public key: $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, $\mathcal{I} = \langle p_1, \ldots, p_m \rangle, A \in GL_n(\mathbb{F}_q)$, $p_i = f_i \circ A$.

Exploiting the geometry of UOV

Original UOV formulation [Patarin 1997] [Kipnis, Patarin, Goubin 1999]

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

Private key: there exists a **linear subspace** $\mathcal{O} \subset V(\mathcal{I})$, $\dim \mathcal{O} = o$. [Kipnis Shamir 1998]

Public key: $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, $\mathcal{I} = \langle p_1, \ldots, p_m \rangle, A \in GL_n(\mathbb{F}_q)$, $p_i = f_i \circ A$.

Reduction to linear algebra [Kipnis-Shamir 1998] [Kipnis, Patarin, Goubin 1999]

- $n = 2o$: $\mathcal{O}$ is an *invariant subspace* of some public matrix.
  Polynomial-time attack, by computing $O(1)$ characteristic polynomials.

Exploiting the geometry of UOV

Original UOV formulation [Patarin 1997] [Kipnis, Patarin, Goubin 1999]

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

Private key: there exists a **linear subspace** $\mathcal{O} \subset V(\mathcal{I})$, $\dim \mathcal{O} = o$. [Kipnis Shamir 1998]

Public key: $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, $\mathcal{I} = \langle p_1, \ldots, p_m \rangle, A \in GL_n(\mathbb{F}_q)$, $p_i = f_i \circ A$.

Reduction to linear algebra [Kipnis-Shamir 1998] [Kipnis, Patarin, Goubin 1999]

- $n = 2o$: $\mathcal{O}$ is an *invariant subspace* of some public matrix.
  Polynomial-time attack, by computing $O(1)$ characteristic polynomials.
- $n > 2o$: $\mathcal{O}$ contains *eigenvectors* of some public matrices with probability $\approx q^{2o-n}$.
  Exponential-time attack, by computing $O(q^{n-2o})$ characteristic polynomials.

Tangent spaces of the UOV variety

Notations

Public key: polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n], \mathcal{I} = \langle p_1, \ldots, p_m \rangle$ **radical**, $\operatorname{codim}\mathcal{I} = m$.
Private key: a linear subspace $\mathcal{O} \subset V := V(\mathcal{I})$, where V is an **equidimensional variety**.

Tangent spaces of the UOV variety

Notations

Public key: polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ **radical**, $\operatorname{codim}\mathcal{I} = m$.

Private key: a linear subspace $\mathcal{O} \subset V := V(\mathcal{I})$, where V is an **equidimensional variety**.

Can we distinguish points of $V \setminus \mathcal{O}$ from points of $\mathcal{O}$? **[P. PQC 2024]**

Tangent spaces of the UOV variety

Notations

Public key: polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n], \mathcal{I} = \langle p_1, \ldots, p_m \rangle$ **radical**, $\operatorname{codim}\mathcal{I} = m$.
Private key: a linear subspace $\mathcal{O} \subset V := V(\mathcal{I})$, where V is an **equidimensional variety**.

Can we distinguish points of $V \setminus \mathcal{O}$ from points of $\mathcal{O}$? **[P. PQC 2024]**

- YES, there exists a **polynomial-time** algorithm deciding $\boldsymbol{x} \in \mathcal{O}$.

Tangent spaces of the UOV variety

Notations

Public key: polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ **radical**, $\operatorname{codim}\mathcal{I} = m$.
Private key: a linear subspace $\mathcal{O} \subset V := V(\mathcal{I})$, where V is an **equidimensional variety**.

Can we distinguish points of $V \setminus \mathcal{O}$ from points of $\mathcal{O}$? **[P. PQC 2024]**

- YES, there exists a **polynomial-time** algorithm deciding $\boldsymbol{x} \in \mathcal{O}$.
- As a byproduct, recover the *full* private key from one vector.

Tangent spaces of the UOV variety

Notations

Public key: polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$, $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ **radical**, $\operatorname{codim}\mathcal{I} = m$.
Private key: a linear subspace $\mathcal{O} \subset V := V(\mathcal{I})$, where V is an **equidimensional variety**.

Can we distinguish points of $V \setminus \mathcal{O}$ from points of $\mathcal{O}$? **[P. PQC 2024]**

- YES, there exists a **polynomial-time** algorithm deciding $\boldsymbol{x} \in \mathcal{O}$.
- As a byproduct, recover the *full* private key from one vector.

Previous result: Reconciliation **[Ding, Yang, Chen, Chen, Cheng 2008]**

Given **one vector** $x \in \mathcal{O}$ and $\mathcal{P}$, compute a basis of $\mathcal{O}$ in time exponential in n, m.

Tangent spaces of the UOV variety

Input: a point $\boldsymbol{x} \in V$.

Geometric observation

A linear subspace is tangent to itself.

Tangent spaces of the UOV variety

Input: a point $\boldsymbol{x} \in V$.

Geometric observation

A linear subspace is tangent to itself.

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

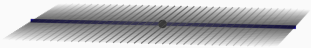
Tangent spaces of the UOV variety

Input: a point $\boldsymbol{x} \in V$.

Geometric observation

A linear subspace is tangent to itself.

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



Tangent spaces of the UOV variety

Input: a point $\boldsymbol{x} \in V$.

Geometric observation

A linear subspace is tangent to itself.

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

Tangent spaces of the UOV variety

Input: a point $\boldsymbol{x} \in V$.

Geometric observation

A linear subspace is tangent to itself.

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

Tangent space at a regular point

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

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

$$\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}) = \begin{pmatrix} \frac{\partial p_1}{\partial X_1} & \cdots & \frac{\partial p_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial p_m}{\partial X_1} & \cdots & \frac{\partial p_m}{\partial X_n} \end{pmatrix}$$

Tangent spaces of the UOV variety

Input: a point $\boldsymbol{x} \in V$.

Geometric observation

A linear subspace is tangent to itself.

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

Tangent space at a regular point

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

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

$$\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{x}) = \begin{pmatrix} \frac{\partial p_1}{\partial X_1} & \cdots & \frac{\partial p_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial p_m}{\partial X_1} & \cdots & \frac{\partial p_m}{\partial X_n} \end{pmatrix}$$

Algorithm

Compute the restriction of $\mathcal{P}$ to $T_{\boldsymbol{x}} V$. Matrices have low rank if and only if $\boldsymbol{x} \in \mathcal{O}$.

Consequence: One vector to rule them all

Contribution: more than we bargained for **[P. PQC 2024]**

Given **one vector** $x \in \mathcal{O}$ and $\mathcal{P} = (p_1, \ldots, p_m)$, compute a basis of $\mathcal{O}$ in polynomial-time $O(mn^\omega)$, where $2 \leq \omega \leq 3$ is the exponent of matrix multiplication.

Consequence: One vector to rule them all

Contribution: more than we bargained for **[P. PQC 2024]**

Given **one vector** $x \in \mathcal{O}$ and $\mathcal{P} = (p_1, \ldots, p_m)$, compute a basis of $\mathcal{O}$ in polynomial-time $O(mn^\omega)$, where $2 \leq \omega \leq 3$ is the exponent of matrix multiplication.

Security level	I	I	III	V
n, m	112, 44	160, 64	184, 72	244, 96
Time	1.7s	4.4s	5.7s	13.3s
[DCCCY 08] (gates)	2^{55}	2^{65}	2^{75}	2^{92}
This work (gates)	2^{33}	2^{33}	2^{36}	2^{37}

Previous result: Reconciliation **[Ding, Yang, Chen, Chen, Cheng 2008]**

Given **one vector** $x \in \mathcal{O}$ and $\mathcal{P}$, compute a basis of $\mathcal{O}$ in time exponential in n, m.

Complexity estimates and practical results with SageMath.

Experimental hardware: Intel i7 running at 2.80GHz with 8GB RAM.

Implementation available under MIT licence.

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

Singular points of UOV and VOX

Limits of our previous result and locality of the UOV secret

- Not a full attack: require **side-channel** or **cryptanalysis** to obtain a vector $\boldsymbol{x} \in \mathcal{O}$.

Singular points of UOV and VOX

Limits of our previous result and locality of the UOV secret

- Not a full attack: require **side-channel** or **cryptanalysis** to obtain a vector $\boldsymbol{x} \in \mathcal{O}$.
- The points of $V(\mathcal{I}) \setminus \mathcal{O}$ give **no information** on $\mathcal{O}$ (or even its existence).

Singular points of UOV and VOX

Limits of our previous result and locality of the UOV secret

- Not a full attack: require **side-channel** or **cryptanalysis** to obtain a vector $\boldsymbol{x} \in \mathcal{O}$.
- The points of $V(\mathcal{I}) \setminus \mathcal{O}$ give **no information** on $\mathcal{O}$ (or even its existence).

Questions

- Can we leverage tangent space structure in a key recovery attack?
- Consequences for UOV variants submitted to NIST?

Singular points of UOV and VOX

Limits of our previous result and locality of the UOV secret

- Not a full attack: require **side-channel** or **cryptanalysis** to obtain a vector $\boldsymbol{x} \in \mathcal{O}$.
- The points of $V(\mathcal{I}) \setminus \mathcal{O}$ give **no information** on $\mathcal{O}$ (or even its existence).

Questions

- Can we leverage tangent space structure in a key recovery attack?
- Consequences for UOV variants submitted to NIST?

Results **[P. Eurocrypt 2025]**

- YES, one obtains an **algebraic** variant of the **Kipnis-Shamir attack** [KPG '99].

Singular points of UOV and VOX

Limits of our previous result and locality of the UOV secret

- Not a full attack: require **side-channel** or **cryptanalysis** to obtain a vector $\boldsymbol{x} \in \mathcal{O}$.
- The points of $V(\mathcal{I}) \setminus \mathcal{O}$ give **no information** on $\mathcal{O}$ (or even its existence).

Questions

- Can we leverage tangent space structure in a key recovery attack?
- Consequences for UOV variants submitted to NIST?

Results **[P. Eurocrypt 2025]**

- YES, one obtains an **algebraic** variant of the **Kipnis-Shamir attack** [KPG '99].
- Attack does not break UOV, but applies succesfully to UOV$\hat{+}$/VOX.

Singular points and dimension of the tangent space

Tangent space and Jacobian matrix

Assume V equidimensional and $\mathcal{I}$ radical. The tangent space to V at $\boldsymbol{x}$ is the kernel of the Jacobian matrix evaluated at $\boldsymbol{x}$.

$$E : Y^2 - X^3 + 3X - 2 = 0.$$

Singular points and dimension of the tangent space

Tangent space and Jacobian matrix

Assume V equidimensional and $\mathcal{I}$ radical. The tangent space to V at $\boldsymbol{x}$ is the kernel of the Jacobian matrix evaluated at $\boldsymbol{x}$.

$\mathrm{Jac}_E(X, Y) = \left(\frac{\partial E}{\partial X}, \frac{\partial E}{\partial Y}\right) = (-3X^2 + 3, 2Y).$

$E : Y^2 - X^3 + 3X - 2 = 0.$

Singular points and dimension of the tangent space

Tangent space and Jacobian matrix

Assume V equidimensional and $\mathcal{I}$ radical. The tangent space to V at $\boldsymbol{x}$ is the kernel of the Jacobian matrix evaluated at $\boldsymbol{x}$.

$\mathrm{Jac}_E(X, Y) = \left(\frac{\partial E}{\partial X}, \frac{\partial E}{\partial Y}\right) = (-3X^2 + 3, 2Y).$

$E : Y^2 - X^3 + 3X - 2 = 0.$

Singular points and dimension of the tangent space

Tangent space and Jacobian matrix

Assume V equidimensional and $\mathcal{I}$ radical. The tangent space to V at $\boldsymbol{x}$ is the kernel of the Jacobian matrix evaluated at $\boldsymbol{x}$.

$$\mathrm{Jac}_E(X, Y) = \left(\tfrac{\partial E}{\partial X}, \tfrac{\partial E}{\partial Y}\right) = (-3X^2 + 3, 2Y).$$
$$\mathrm{Jac}_E(1, 0) = (0, 0).$$

$$E : Y^2 - X^3 + 3X - 2 = 0.$$

Singular points and dimension of the tangent space

Tangent space and Jacobian matrix

Assume V equidimensional and $\mathcal{I}$ radical. The tangent space to V at $\boldsymbol{x}$ is the kernel of the Jacobian matrix evaluated at $\boldsymbol{x}$.

$$\mathrm{Jac}_E(X, Y) = \left(\tfrac{\partial E}{\partial X}, \tfrac{\partial E}{\partial Y}\right) = (-3X^2 + 3, 2Y).$$
$$\mathrm{Jac}_E(1, 0) = (0, 0).$$

Singular points and tangent spaces

$\boldsymbol{x} \in V$ is singular if the Jacobian matrix evaluated at $\boldsymbol{x}$ has a rank defect.

$$E : Y^2 - X^3 + 3X - 2 = 0.$$

Singular points and dimension of the tangent space

Tangent space and Jacobian matrix

Assume V equidimensional and $\mathcal{I}$ radical. The tangent space to V at $\boldsymbol{x}$ is the kernel of the Jacobian matrix evaluated at $\boldsymbol{x}$.

$$\mathrm{Jac}_E(X, Y) = \left(\tfrac{\partial E}{\partial X}, \tfrac{\partial E}{\partial Y}\right) = (-3X^2 + 3, 2Y).$$
$$\mathrm{Jac}_E(1, 0) = (0, 0).$$

Singular points and tangent spaces

$\boldsymbol{x} \in V$ is singular if the Jacobian matrix evaluated at $\boldsymbol{x}$ has a rank defect.

$$E : Y^2 - X^3 + 3X - 2 = 0.$$

Previous work on geometric attacks

[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

Structured equations yield a structured Jacobian

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

Private key $\mathcal{F}$: m polynomials linear in $\boldsymbol{X_1}, \ldots, \boldsymbol{X_o}$, a linear map A: $1 \leq i \leq m, \quad p_i = f_i \circ A$.

Structured equations yield a structured Jacobian

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

Private key $\mathcal{F}$: m polynomials linear in $X_1, \ldots, X_o$, a linear map A: $1 \leq i \leq m$, $\quad p_i = f_i \circ A$.

Secret Jacobian **[P. Eurocrypt 2025]**

The Jacobian of $\mathcal{F}$ has a special shape :

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \begin{array}{cccccc} \partial X_1 & \cdots & \partial X_o & \partial X_{o+1} & \cdots & \partial X_n \end{array} \\ \left[\begin{array}{cc|c} \multicolumn{2}{c|}{J_1} & J_2 \end{array}\right] \end{array}$$

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 polynomials linear in $X_1, \ldots, X_o$, a linear map A: $1 \leq i \leq m, \quad p_i = f_i \circ A$.

Secret Jacobian **[P. Eurocrypt 2025]**

The Jacobian of $\mathcal{F}$ has a special shape when evaluated at $x \in \mathcal{O}$:

$$\mathrm{Jac}_{\mathcal{F}}(x) = \begin{array}{c} \begin{array}{cccccc} \partial X_1 & \cdots & \partial X_o & \partial X_{o+1} & \cdots & \partial X_n \end{array} \\ \left[\begin{array}{cc|c} \multicolumn{2}{c|}{\multirow{2}{*}{0}} & \multirow{2}{*}{J_2} \\ & & \end{array}\right] \end{array}$$

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 polynomials linear in $\boldsymbol{X_1}, \ldots, \boldsymbol{X_o}$, a linear map A: $1 \leq i \leq m, \quad p_i = f_i \circ A$.

Secret Jacobian **[P. Eurocrypt 2025]**

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \begin{array}{cccccc} \partial \boldsymbol{X_1} & \cdots & \partial \boldsymbol{X_o} & \partial \boldsymbol{X_{o+1}} & \cdots & \partial \boldsymbol{X_n} \end{array} \\ \left[\begin{array}{ccc|ccc} & & & & & \\ & \mathbf{0} & & & J_2 & \\ & & & & & \end{array}\right] \end{array}$$

Where $\boldsymbol{J_1} \in \mathbb{F}_q[\boldsymbol{X_{o+1}}, \ldots, \boldsymbol{X_n}]^{m \times o}$ and $J_2 \in \mathbb{F}_q[\boldsymbol{X_1}, \ldots, \boldsymbol{X_n}]^{m \times (n-o)}$.

Main theorem: Dimension of the singular locus of $V(\mathcal{I})$ **[P. Eurocrypt 2025]**

UOV varieties admit a **positive dimensional** singular locus:

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

An algebraic attack targeting singular points

Generic smoothness outside of the secret subspace $\mathcal{O}$ **[P. Eurocrypt 2025]**

For a **generic** UOV variety, $\mathcal{I}$ is **radical** and $V(\mathcal{I})$ is **equidimensional of codimension** m.
In addition, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$ (if the base field is large enough).

An algebraic attack targeting singular points

Generic smoothness outside of the secret subspace $\mathcal{O}$ **[P. Eurocrypt 2025]**

For a **generic** UOV variety, $\mathcal{I}$ is **radical** and $V(\mathcal{I})$ is **equidimensional of codimension** m.
In addition, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$ (if the base field is large enough).

Singular point attack **[P. Eurocrypt 2025]**

Perform an exponential time **key recovery** by computing **singularities of the public key**.

An algebraic attack targeting singular points

Generic smoothness outside of the secret subspace $\mathcal{O}$ **[P. Eurocrypt 2025]**

For a **generic** UOV variety, $\mathcal{I}$ is **radical** and $V(\mathcal{I})$ is **equidimensional of codimension** m. In addition, $\mathrm{Sing}(V(\mathcal{I})) \subset \mathcal{O}$ (if the base field is large enough).

Singular point attack **[P. Eurocrypt 2025]**

Perform an exponential time **key recovery** by computing **singularities of the public key**.

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

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

However, algebraic attack is more expensive than [KPG99] if q is "small".

Can the singularities be hidden to prevent attacks?

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

In a UOV private key, replace $\boldsymbol{t} \leq \mathbf{8}$ polynomials by random quadratic polynomials, then **mix**.

$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ A, \quad \mathcal{I} = \langle p_1, \ldots, p_o \rangle.$$

Can the singularities be hidden to prevent attacks?

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

In a UOV private key, replace $\boldsymbol{t} \leq \mathbf{8}$ polynomials by random quadratic polynomials, then **mix**.

$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ A, \quad \mathcal{I} = \langle p_1, \ldots, p_o \rangle.$$

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

Can the singularities be hidden to prevent attacks?

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

In a UOV private key, replace $t \leq 8$ polynomials by random quadratic polynomials, then **mix**.

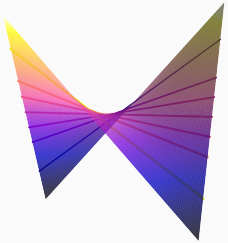
$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ A, \quad \mathcal{I} = \langle p_1, \ldots, p_o \rangle.$$

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

Geometric interpretation

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

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



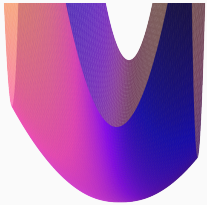
Can the singularities be hidden to prevent attacks?

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

In a UOV private key, replace $t \leq 8$ polynomials by random quadratic polynomials, then **mix**.

$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ A, \quad \mathcal{I} = \langle p_1, \ldots, p_o \rangle.$$

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



Geometric interpretation

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

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

Can the singularities be hidden to prevent attacks?

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

In a UOV private key, replace $t \leq 8$ polynomials by random quadratic polynomials, then **mix**.

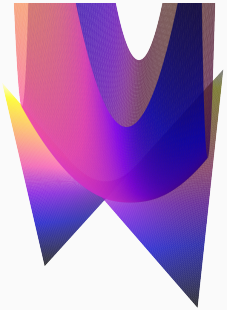
$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ A, \quad \mathcal{I} = \langle p_1, \ldots, p_o \rangle.$$

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

Geometric interpretation

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

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



Can the singularities be hidden to prevent attacks?

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

In a UOV private key, replace $\boldsymbol{t} \leq \mathbf{8}$ polynomials by random quadratic polynomials, then **mix**.

$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ A, \quad \mathcal{I} = \langle p_1, \ldots, p_o \rangle.$$

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

Geometric interpretation

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

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

Can the singularities be hidden to prevent attacks?

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

In a UOV private key, replace $t \leq 8$ polynomials by random quadratic polynomials, then **mix**.

$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ A, \quad \mathcal{I} = \langle p_1, \ldots, p_o \rangle.$$

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

Geometric interpretation

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

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

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \begin{matrix} \partial \boldsymbol{X_1} & \cdots & \partial \boldsymbol{X_o} & \partial \boldsymbol{X_{o+1}} & \cdots & \partial \boldsymbol{X_n} \end{matrix} \\ \left[\begin{array}{ccc|c} & & & J_1 & & \\ \hline & & & & & \\ & 0 & & & J_2 & \\ & & & & & \end{array}\right] \begin{matrix} \\ \\ t+1 \\ \vdots \\ o \end{matrix} \end{array}$$

$$\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{X}) = \mathcal{S}^{-1}\mathrm{Jac}_{\mathcal{F}}(A^{-1}\boldsymbol{X}) \cdot A^{-1}$$

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \begin{matrix} \partial \boldsymbol{X_1} & \cdots & \partial \boldsymbol{X_o} & \partial \boldsymbol{X_{o+1}} & \cdots & \partial \boldsymbol{X_n} \end{matrix} \\ \left[\begin{array}{ccc|c} & & & J_1 \\ \hline 0 & & & J_2 \end{array}\right] \end{array} \begin{matrix} \\ \\ t+1 \\ \vdots \\ o \end{matrix}$$

$$\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{X}) = \boldsymbol{\mathcal{S}}^{-1}\mathrm{Jac}_{\mathcal{F}}(A^{-1}\boldsymbol{X}) \cdot A^{-1}$$

Observation

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

Structured equations yield a structured Jacobian bis

Underlying UOV Jacobian

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

$$\mathrm{Jac}_{\mathcal{F}}(\boldsymbol{x}) = \begin{array}{c} \begin{array}{cccccc} \partial \boldsymbol{X_1} & \cdots & \partial \boldsymbol{X_o} & \partial \boldsymbol{X_{o+1}} & \cdots & \partial \boldsymbol{X_n} \end{array} \\ \left[\begin{array}{cc|c} \multicolumn{2}{c|}{} & J_1 \\ \multicolumn{2}{c|}{\multirow{2}{*}{0}} & \multirow{2}{*}{J_2} \\ \multicolumn{2}{c|}{} & \\ \hline \multicolumn{3}{c}{} \end{array}\right] \begin{array}{l} \\ \\ t+1 \\ \vdots \\ o \end{array} \end{array}$$

$$\mathrm{Jac}_{\mathcal{P}}(\boldsymbol{X}) = \boldsymbol{\mathcal{S}}^{-1}\mathrm{Jac}_{\mathcal{F}}(A^{-1}\boldsymbol{X}) \cdot A^{-1}$$

Observation

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

Dimension computation [P. 2025]

$\hat{+}$ reduces the dimension of the singular locus by at most $\boldsymbol{2t}$ compared with UOV.

From singular points to a key recovery attack

$V(\mathcal{I})$ is the UOV$\hat{+}$ 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 UOV$\hat{+}$ 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 UOV$\hat{+}$ 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: $O(q^{n-o+2t}n^{\omega})$. Same as Kipnis Shamir [KPG'99] attack against UOV$\hat{+}$.

From singular points to a key recovery attack

$V(\mathcal{I})$ is the UOV$\hat{+}$ 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: $O(q^{n-o+2t}n^{\omega})$. Same as Kipnis Shamir [KPG'99] attack against UOV$\hat{+}$.

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

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

Expected number of trials: $O(q^{n-2o+t})$

From singular points to a key recovery attack

$V(\mathcal{I})$ is the UOV$\hat{+}$ 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: $O(q^{n-o+2t}n^{\omega})$. Same as Kipnis Shamir [KPG'99] attack against UOV$\hat{+}$.

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

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

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

From singular points to a key recovery attack

$V(\mathcal{I})$ is the UOV$\hat{+}$ 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: $O(q^{n-o+2t}n^{\omega})$. Same as Kipnis Shamir [KPG'99] attack against UOV$\hat{+}$.

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

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

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

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

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

Previous result for UOV [P. 2024]

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

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

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

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

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

Restricting to the tangent space $T_x V$

$\mathcal{P}_{|T_x V}(x)$ is an **easy** UOV$\hat{+}$ instance if $x \in \mathcal{O}$.

$\longrightarrow$ **Decide in polynomial time.**

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

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

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

Decide $x \in \mathcal{O}$? using $O\left(\binom{n-o+2t-3}{4}^2 \binom{n-2o+2t+1}{2}\right) \subset O(n^{10})$ arithmetic operations.

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

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

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

Decide $x \in \mathcal{O}$? using $O\left(\binom{n-o+2t-3}{4}^2 \binom{n-2o+2t+1}{2}\right) \subset O(n^{10})$ arithmetic operations.

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

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

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

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

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

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

Decide $x \in \mathcal{O}$? using $O\left(\binom{n-o+2t-3}{4}^2 \binom{n-2o+2t+1}{2}\right) \subset O(n^{10})$ arithmetic operations.

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

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

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

Previous result

This attack improves the Kipnis-Shamir attack which required:

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

Practical results and bit complexity

Parameters	I	III	V
$\log_2$ gates	2^{39}	2^{41}	2^{43}
Time	2.3s	7.1s	16.4s

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

Intel i7 @ 2.80GHz, 8GB RAM.

[1] msolve.lip6.fr *Implementation under MIT licence*

Practical results and bit complexity

Parameters	I	III	V
$\log_2$ gates	2^{39}	2^{41}	2^{43}
Time	2.3s	7.1s	16.4s

Figure 1: $\boldsymbol{x} \in \mathcal{O}$? with msolve[1] on UOV$\hat{+}$.
Intel i7 @ 2.80GHz, 8GB RAM.
[1] msolve.lip6.fr *Implementation under MIT licence*

Parameters	I	III	V
Security level ($\log_2$ gates)	2^{143}	2^{207}	2^{272}
Kipnis-Shamir ($\log_2$ gates)	2^{166}	2^{233}	2^{313}
This work ($\log_2$ gates)	$\mathbf{2^{140}}$	$\mathbf{2^{188}}$	$\mathbf{2^{243}}$

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

Practical results and bit complexity

Parameters	I	III	V
$\log_2$ gates	2^{39}	2^{41}	2^{43}
Time	2.3s	7.1s	16.4s

Figure 1: $x \in \mathcal{O}$? with msolve[1] on UOV$\hat{+}$.
Intel i7 @ 2.80GHz, 8GB RAM.
[1] msolve.lip6.fr *Implementation under MIT licence*

Parameters	I	III	V
Security level ($\log_2$ gates)	2^{143}	2^{207}	2^{272}
Kipnis-Shamir ($\log_2$ gates)	2^{166}	2^{233}	2^{313}
This work ($\log_2$ gates)	$\mathbf{2^{140}}$	$\mathbf{2^{188}}$	$\mathbf{2^{243}}$

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

Cryptanalysis

- Initial UOV$\hat{+}$ parameter sets **do not meet NIST security requirement**.
- We propose alternative parameters for UOV$\hat{+}$ achieving between 27%-44% (expanded) public key size reduction compared with UOV.

Practical results and bit complexity

Parameters	I	III	V
$\log_2$ gates	2^{39}	2^{41}	2^{43}
Time	2.3s	7.1s	16.4s

Figure 1: $\boldsymbol{x} \in \mathcal{O}$? with msolve[1] on UOV$\hat{+}$.
Intel i7 @ 2.80GHz, 8GB RAM.
[1] msolve.lip6.fr *Implementation under MIT licence*

Parameters	I	III	V
Security level ($\log_2$ gates)	2^{143}	2^{207}	2^{272}
Kipnis-Shamir ($\log_2$ gates)	2^{166}	2^{233}	2^{313}
This work ($\log_2$ gates)	$\mathbf{2^{140}}$	$\mathbf{2^{188}}$	$\mathbf{2^{243}}$

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

Cryptanalysis

- Initial UOV$\hat{+}$ parameter sets **do not meet NIST security requirement**.
- We propose alternative parameters for UOV$\hat{+}$ achieving between 27%-44% (expanded) public key size reduction compared with UOV.

Can we do better?

Special case of UOV$\hat{+}$ called VOX with **additional structure** was submitted to NIST.

Can we exploit that structure to improve our attack?

Practical attack on VOX [Patarin, Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud 2023]

Dimension computation for VOX, seen as QR-UOV$\hat{+}(q, n, m, t, \ell)$

Practical attack on VOX [Patarin, Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud 2023]

Dimension computation for VOX, seen as QR-UOV$\hat{+}(q, n, m, t, \ell)$

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

Practical attack on VOX [Patarin, Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud 2023]

Dimension computation for VOX, seen as QR-UOV$\hat{+}(q, n, m, t, \ell)$

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

Initial VOX parameters are insecure

MinRank attack [Furue, Ikematsu 2023]
Direct attack [P. 2024b]

Parameters	I	III	V
ℓ	6	7	8
ℓ'	6	7	8
Time	0.03s	0.11s	0.32s

Timing for the subfield attack on VOX, on Intel i7 @ 2.80GHz 8GB RAM with msolve.

Practical attack on VOX [Patarin, Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud 2023]

Dimension computation for VOX, seen as QR-UOV$\hat{+}(q, n, m, t, \ell)$

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

Initial VOX parameters are insecure

MinRank attack [Furue, Ikematsu 2023]
Direct attack [P. 2024b]

Subfield attack [P. 2024b]

Alternative parameters exposed to direct attack through **subfields** $\mathbb{F}_{q^{\ell'}} \subset \mathbb{F}_{q^\ell}$.

Parameters	I	III	V
ℓ	6	7	8
ℓ'	6	7	8
Time	0.03s	0.11s	0.32s

Ic	IIIa	Vb
9	15	14
3	**5**	**7**
400h[1]	83.4s	12.4s

Timing for the subfield attack on VOX, on Intel i7 @ 2.80GHz 8GB RAM with msolve.

Implementation available under MIT licence.

[1] on Intel Xeon E7-4820, at 2.00GHz, peaking at 54.3GB RAM usage.

Future and on-going work - 1

Precomputations for undetermined systems

Task: Reduce $MQ(n, m)$ to $MQ(m - \mathbf{k}, m - \mathbf{k})$. For UOV, $k = 1$ in any field [Cheng, Hashimoto, Miura, Takagi 2014]. Can we go **beyond** $k = 1$?
$\longrightarrow$ *WIP*: Adapt work of Reid for $k = 2$.

Future and on-going work - 1

Precomputations for undetermined systems

Task: Reduce $MQ(n, m)$ to $MQ(m - \mathbf{k}, m - \mathbf{k})$. For UOV, $k = 1$ in any field [Cheng, Hashimoto, Miura, Takagi 2014]. Can we go **beyond** $k = 1$?
$\longrightarrow$ *WIP*: Adapt work of Reid for $k = 2$.

Genericity results on UOV

Are non-generic UOV keys **weaker**?
Generalize genericity results to all UOV variants.
$\longrightarrow$ *ex*: non-radical ideal implies easier attack?

Future and on-going work - 1

Precomputations for undetermined systems

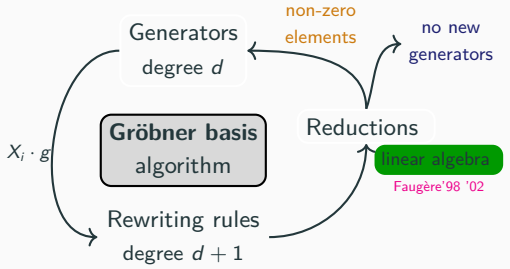
Task: Reduce $MQ(n, m)$ to $MQ(m - \mathbf{k}, m - \mathbf{k})$. For UOV, $k = 1$ in any field [Cheng, Hashimoto, Miura, Takagi 2014]. Can we go **beyond** $k = 1$?
$\longrightarrow$ *WIP*: Adapt work of Reid for $k = 2$.

Genericity results on UOV

Are non-generic UOV keys **weaker**?
Generalize genericity results to all UOV variants.
$\longrightarrow$ *ex*: non-radical ideal implies easier attack?

Linear polynomials in Gröbner bases

If $\mathcal{J}$ radical and $V(\mathcal{J}) \subset \mathcal{O}$, then DRL Gröbner bases of $\mathcal{J}$ contain **linear polynomials**.



Future and on-going work - 1

Precomputations for undetermined systems

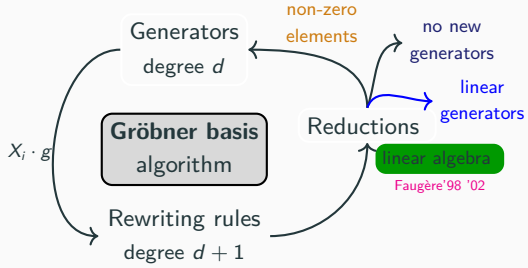
Task: Reduce $MQ(n, m)$ to $MQ(m - \mathbf{k}, m - \mathbf{k})$. For UOV, $k = 1$ in any field [Cheng, Hashimoto, Miura, Takagi 2014]. Can we go **beyond** $k = 1$?
$\longrightarrow$ *WIP*: Adapt work of Reid for $k = 2$.

Genericity results on UOV

Are non-generic UOV keys **weaker**?
Generalize genericity results to all UOV variants.
$\longrightarrow$ *ex*: non-radical ideal implies easier attack?

Linear polynomials in Gröbner bases

If $\mathcal{J}$ radical and $V(\mathcal{J}) \subset \mathcal{O}$, then DRL Gröbner bases of $\mathcal{J}$ contain **linear polynomials**.



Future and on-going work - 2

Cryptanalysis of MAYO [Beullens 21]

Small dimension of secret subspace defeats UOV attacks.

- Algebraic structure induced by MAYO's whipped-up transform?
- Exploit **large** pre-image of signatures in EUF-CMA attacks?

	Signature (bytes)	Public key (bytes)
UOV-Ip	128	43 576
MAYO-1	454	1420
MAYO-2	186	4912

Figure 3: Sizes at security level one.

Future and on-going work - 2

Cryptanalysis of MAYO [Beullens 21]

Small dimension of secret subspace defeats UOV attacks.

- Algebraic structure induced by MAYO's whipped-up transform?
- Exploit **large** pre-image of signatures in EUF-CMA attacks?

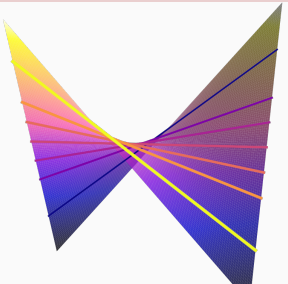
Polar varieties of UOV

$$V = V(\langle p_1, p_2, p_3 \rangle)$$

$$\mathrm{crit}(\pi_A, V) := \{\boldsymbol{x} \in V,\ d_{\boldsymbol{x}}\pi_A \text{ not surjective}\}$$

	Signature (bytes)	Public key (bytes)
UOV-Ip	128	43 576
MAYO-1	454	1420
MAYO-2	186	4912

Figure 3: Sizes at security level one.



Future and on-going work - 2

Cryptanalysis of MAYO [Beullens 21]

Small dimension of secret subspace defeats UOV attacks.

- Algebraic structure induced by MAYO's whipped-up transform?
- Exploit **large** pre-image of signatures in EUF-CMA attacks?

	Signature (bytes)	Public key (bytes)
UOV-Ip	128	43 576
MAYO-1	454	1420
MAYO-2	186	4912

Figure 3: Sizes at security level one.

Polar varieties of UOV

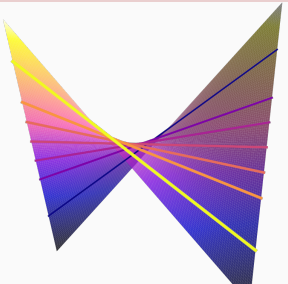
$$V = V(\langle p_1, p_2, p_3 \rangle)$$

$$\mathrm{crit}(\pi_A, V) := \{\boldsymbol{x} \in V,\ d_{\boldsymbol{x}}\pi_A \text{ not surjective}\}$$

$$\mathcal{O}^\perp \subset A \implies \mathcal{O} \subset \mathrm{crit}(\pi_A, V)$$

$$\mathcal{O} \subset \mathrm{crit}(\pi_{A_1}, V) \cap \cdots \cap \mathrm{crit}(\pi_{A_\ell}, V)$$

$$\left(\bigcap \mathrm{crit}(\pi_{A_i}, V)\right) \setminus Z = \mathrm{crit}\left(\bigcap \pi_{A_i}, V\right) \setminus Z$$



Future and on-going work - 2

Cryptanalysis of MAYO [Beullens 21]

Small dimension of secret subspace defeats UOV attacks.

- Algebraic structure induced by MAYO's whipped-up transform?
- Exploit **large** pre-image of signatures in EUF-CMA attacks?

	Signature (bytes)	Public key (bytes)
UOV-Ip	128	43 576
MAYO-1	454	1420
MAYO-2	186	4912

Figure 3: Sizes at security level one.

Polar varieties of UOV

$$V = V(\langle p_1, p_2, p_3 \rangle)$$

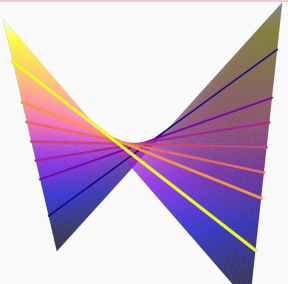
$$\mathrm{crit}(\pi_A, V) := \{\boldsymbol{x} \in V,\ d_{\boldsymbol{x}}\pi_A \text{ not surjective}\}$$

$$\mathcal{O}^\perp \subset A \implies \mathcal{O} \subset \mathrm{crit}(\pi_A, V)$$

$$\mathcal{O} \subset \mathrm{crit}(\pi_{A_1}, V) \cap \cdots \cap \mathrm{crit}(\pi_{A_\ell}, V)$$

$$\left(\bigcap \mathrm{crit}(\pi_{A_i}, V)\right) \setminus Z = \mathrm{crit}\left(\bigcap \pi_{A_i}, V\right) \setminus Z$$

$\longrightarrow$ Dimension, degree and computational cost understood for a fixed projection.



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%

Genericity in the Zariski topology

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

Zariski-closed sets are algebraic varieties.

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

Genericity in the Zariski topology

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

Zariski-closed sets are algebraic varieties.

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 $E_{a,b} : Y^2 - X^3 - aX - b = 0$ singular?

Genericity in the Zariski topology

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

Zariski-closed sets are algebraic varieties.

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 $E_{a,b} : Y^2 - X^3 - aX - b = 0$ singular?

Methodology

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

Genericity in the Zariski topology

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

Zariski-closed sets are algebraic varieties.

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 $E_{a,b} : Y^2 - X^3 - aX - b = 0$ singular?

Methodology

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

$$\mathrm{Jac}_E(a, b) = (0, 0) \iff \delta(a, b) = 4a^3 + 27b^2 = 0.$$

Genericity in the Zariski topology

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

Zariski-closed sets are algebraic varieties.

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 $E_{a,b} : Y^2 - X^3 - aX - b = 0$ singular?

Methodology

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

$$\mathrm{Jac}_E(a, b) = (0, 0) \iff \delta(a, b) = 4a^3 + 27b^2 = 0.$$

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

Genericity in the Zariski topology

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

Zariski-closed sets are algebraic varieties.

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 $E_{a,b} : Y^2 - X^3 - aX - b = 0$ singular?

Methodology

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

$$\mathrm{Jac}_E(a, b) = (0, 0) \iff \delta(a, b) = 4a^3 + 27b^2 = 0.$$

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

Examples of generic properties of UOV ideals and varieties:

- UOV keys generically generate radical ideals of the expected dimension.
- UOV varieties are generically equidimensional complete intersections.
- UOV varieties are generically smooth... outside of $\mathcal{O}$.

Genericity in the Zariski topology

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

Zariski-closed sets are algebraic varieties.

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 $E_{a,b} : Y^2 - X^3 - aX - b = 0$ singular?

Methodology

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

$$\mathrm{Jac}_E(a, b) = (0, 0) \iff \delta(a, b) = 4a^3 + 27b^2 = 0.$$

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

Examples of generic properties of UOV ideals and varieties:

- UOV keys generically generate radical ideals of the expected dimension.
- UOV varieties are generically equidimensional complete intersections.
- UOV varieties are generically smooth... outside of $\mathcal{O}$.

How many equations characterize the secret?

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

The Debarre and Manivel Bound[1] **[Debarre, Manivel 1998]**

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

[1] The original statement is for arbitrary degrees.

How many equations characterize the secret?

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

The Debarre and Manivel Bound[1] **[Debarre, Manivel 1998]**

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

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

[1] The original statement is for arbitrary degrees.

How many equations characterize the secret?

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

The Debarre and Manivel Bound[1] **[Debarre, Manivel 1998]**

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

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

[1] The original statement is for arbitrary degrees.

How many equations characterize the secret?

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

The Debarre and Manivel Bound[1] **[Debarre, Manivel 1998]**

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

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

Application to UOV

If $\alpha = \frac{n}{s}$ is a constant, then a UOV secret is characterized by a constant number of polynomials from the public key.
For practical parameters, 3 or 4 polynomials are enough.

[1] The original statement is for arbitrary degrees.