One vector to rule them all: Key recovery from one vector in UOV schemes

Pierre Pébereau
Sorbonne Université, LIP6, CNRS, Thales SIX

June 12, 2024

Building cryptography from (quantum-)hard problems

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

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

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

This problem is NP-hard: reduces to SAT

Building cryptography from (quantum-)hard problems

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

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

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

This problem is NP-hard: reduces to SAT

Multivariate Quadratic Cryptography

A multivariate signature scheme is defined by a key pair $(\mathcal{P}, \mathcal{S})$:

Building cryptography from (quantum-)hard problems

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

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

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

This problem is NP-hard: reduces to SAT

Multivariate Quadratic Cryptography

A multivariate signature scheme is defined by a key pair $(\mathcal{P}, \mathcal{S})$:

- The public key $\mathcal{P}$ is an instance of MQ(n, m, q), $n > m$.

Building cryptography from (quantum-)hard problems

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

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

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

This problem is NP-hard: reduces to SAT

Multivariate Quadratic Cryptography

A multivariate signature scheme is defined by a key pair $(\mathcal{P}, \mathcal{S})$:

- The public key $\mathcal{P}$ is an instance of MQ(n, m, q), $n > m$.
- The secret key $\mathcal{S}$ enables, for all $\boldsymbol{t} \in \mathbb{F}_q^m$, to efficiently find $\boldsymbol{x} \in \mathbb{F}_q^n$ s.t. $\mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}$

Quadratic equations and square matrices

Example

$$3 \cdot x^2 + 2 \cdot xy + 1 \cdot y^2$$

Quadratic equations and square matrices

Example

$$3 \cdot x^2 + 2 \cdot xy + 1 \cdot y^2 = \begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

Quadratic equations and square matrices

Example

$$3 \cdot x^2 + 2 \cdot xy + 1 \cdot y^2 = \begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

Representation

$$\sum_{1 \leq i,j \leq n}^{n} a_{i,j} x_i x_j = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \cdot \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Quadratic equations and square matrices

Example

$$3 \cdot x^2 + 2 \cdot xy + 1 \cdot y^2 = \begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

Representation

$$\sum_{1 \leq i,j \leq n}^{n} a_{i,j} x_i x_j = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \cdot \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Structured equations $\iff$ structured matrices

UOV: Original formulation

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

Secret key: - m quadratic polynomials $\boldsymbol{x}^T F_i \boldsymbol{x} \in \mathbb{F}_q[x_1, \ldots, x_n]$
linear in $x_1, \ldots, x_m$.
- invertible change of variables A.

Figure 1: UOV key pair in $\mathbb{F}_{257}$

UOV: Original formulation

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

Secret key: - m quadratic polynomials $\boldsymbol{x}^T F_i \boldsymbol{x} \in \mathbb{F}_q[x_1, \ldots, x_n]$

linear in $x_1, \ldots, x_m$.

- invertible change of variables A.

Public key: m quadratic polynomials $\boldsymbol{x}^T P_i \boldsymbol{x}$.

$$\mathcal{P} = \mathcal{F} \circ A = (A^T F_1 A, \ldots, A^T F_m A)$$

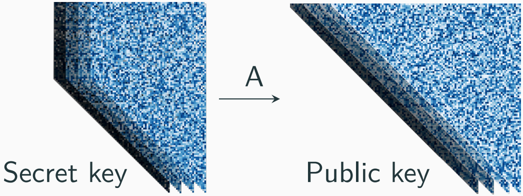


Figure 1: UOV key pair in $\mathbb{F}_{257}$

UOV: Original formulation

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

Secret key: - m quadratic polynomials $\boldsymbol{x}^T F_i \boldsymbol{x} \in \mathbb{F}_q[x_1, \ldots, x_n]$
linear in $x_1, \ldots, x_m$.
- invertible change of variables A.

Public key: m quadratic polynomials $\boldsymbol{x}^T P_i \boldsymbol{x}$.

$$\mathcal{P} = \mathcal{F} \circ A = (A^T F_1 A, \ldots, A^T F_m A)$$

Naming conventions and parameters

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

UOV: Original formulation

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

Secret key: - m quadratic polynomials $\boldsymbol{x}^T F_i \boldsymbol{x} \in \mathbb{F}_q[x_1, \ldots, x_n]$
linear in $x_1, \ldots, x_m$.
- invertible change of variables A.

Public key: m quadratic polynomials $\boldsymbol{x}^T P_i \boldsymbol{x}$.

$$\mathcal{P} = \mathcal{F} \circ A = (A^T F_1 A, \ldots, A^T F_m A)$$

Naming conventions and parameters

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

In practice: $\underbrace{2m <}_{\text{[KS98]}} n$ [Kipnis, Shamir 1998]

UOV: Original formulation

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

Secret key: - m quadratic polynomials $\boldsymbol{x}^T F_i \boldsymbol{x} \in \mathbb{F}_q[x_1, \ldots, x_n]$
linear in $x_1, \ldots, x_m$.
- invertible change of variables A.

Public key: m quadratic polynomials $\boldsymbol{x}^T P_i \boldsymbol{x}$.

$$\mathcal{P} = \mathcal{F} \circ A = (A^T F_1 A, \ldots, A^T F_m A)$$

Naming conventions and parameters

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

In practice: $\underbrace{2m <}_{\text{[KS98]}} n \underbrace{\leq 3m}_{\text{Key sizes}}$ [Kipnis, Shamir 1998]

UOV: Signatures and Parameters

Small signatures

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

UOV: Signatures and Parameters

Small signatures

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

	NIST SL	n	m	$\mathbb{F}_q$	|pk| (bytes)	|sk| (bytes)	|cpk| (bytes)	|sig+salt| (bytes)
ov-Ip	1	112	44	$\mathbb{F}_{256}$	278 432	237 912	43 576	128
ov-Is	1	160	64	$\mathbb{F}_{16}$	412 160	348 720	66 576	96
ov-III	3	184	72	$\mathbb{F}_{256}$	1 225 440	1 044 336	189 232	200
ov-V	5	244	96	$\mathbb{F}_{256}$	2 869 440	2 436 720	446 992	260

[Beullens, Chen, Hung, Kannwischer, Peng, Shih, Yang 2023]

Figure 2: Modern UOV parameters

UOV: Alternative formulation

$$\mathcal{P}, \mathcal{S} = (P_1, \dots, P_m), (F_1, \dots, F_m, A)$$

Equivalent characterisation of the trapdoor [Beullens 2020]

Trapdoor: subspace $\mathcal{O} \subset \mathbb{F}_q^n$ of dimension m such that

$$\forall (\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}^2, \quad \boldsymbol{x}^T P_1 \boldsymbol{y} = \cdots = \boldsymbol{x}^T P_m \boldsymbol{y} = 0$$

UOV: Alternative formulation

$$\mathcal{P}, \mathcal{S} = (P_1, \ldots, P_m), (F_1, \ldots, F_m, A)$$

Equivalent characterisation of the trapdoor [Beullens 2020]

Trapdoor: subspace $\mathcal{O} \subset \mathbb{F}_q^n$ of dimension m such that

$$\forall (\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}^2, \quad \boldsymbol{x}^T P_1 \boldsymbol{y} = \cdots = \boldsymbol{x}^T P_m \boldsymbol{y} = 0$$

Observation 1

The first m columns of A^{-1} form a basis of $\mathcal{O}$.

UOV: Alternative formulation

$$\mathcal{P}, \mathcal{S} = (P_1, \ldots, P_m), (F_1, \ldots, F_m, A)$$

Equivalent characterisation of the trapdoor [Beullens 2020]

Trapdoor: subspace $\mathcal{O} \subset \mathbb{F}_q^n$ of dimension m such that

$$\forall (\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}^2, \quad \boldsymbol{x}^T P_1 \boldsymbol{y} = \cdots = \boldsymbol{x}^T P_m \boldsymbol{y} = 0$$

Observation 1

The first m columns of A^{-1} form a basis of $\mathcal{O}$.

Observation 2

All vectors in $\mathcal{O}$ are signatures of the message $(0, \ldots, 0) \in \mathbb{F}_q^m$.

Forgery

Goal: Find **a** signature $\boldsymbol{x} \in \mathbb{F}_q^n$ for a **single** message $\boldsymbol{t} \in \mathbb{F}_q^m$.

$$V_{\boldsymbol{t}} := \{\boldsymbol{x} \in \mathbb{F}_q^n \quad | \quad \mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}\}$$

Cryptanalysis

Forgery

Goal: Find **a** signature $\boldsymbol{x} \in \mathbb{F}_q^n$ for a **single** message $\boldsymbol{t} \in \mathbb{F}_q^m$.

$$V_{\boldsymbol{t}} := \{\boldsymbol{x} \in \mathbb{F}_q^n \quad | \quad \mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}\}$$

Find a point in a **variety of dimension** $n - m$

Cryptanalysis

Forgery

Goal: Find **a** signature $\boldsymbol{x} \in \mathbb{F}_q^n$ for a **single** message $\boldsymbol{t} \in \mathbb{F}_q^m$.

$$V_{\boldsymbol{t}} := \{\boldsymbol{x} \in \mathbb{F}_q^n \quad | \quad \mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}\}$$

Find a point in a **variety of dimension** $n - m$

Key recovery

Goal: find an equivalent secret key.

$$\mathcal{O} \subset \{\boldsymbol{x} \in \mathbb{F}_q^n \quad | \quad \mathcal{P}(\boldsymbol{x}) = \boldsymbol{0}\}$$

Cryptanalysis

Forgery

Goal: Find **a** signature $\boldsymbol{x} \in \mathbb{F}_q^n$ for a **single** message $\boldsymbol{t} \in \mathbb{F}_q^m$.

$$V_{\boldsymbol{t}} := \{\boldsymbol{x} \in \mathbb{F}_q^n \quad | \quad \mathcal{P}(\boldsymbol{x}) = \boldsymbol{t}\}$$

Find a point in a **variety of dimension** $n - m$

Key recovery

Goal: find an equivalent secret key.

$$\mathcal{O} \subset \{\boldsymbol{x} \in \mathbb{F}_q^n \quad | \quad \mathcal{P}(\boldsymbol{x}) = \boldsymbol{0}\}$$

Find a **linear subspace of dimension** m **in** $V_{\boldsymbol{0}}$

Contributions

Main result

Given **one vector** $x \in \mathcal{O}$ and the public key, compute a basis of $\mathcal{O}$ in polynomial-time $O(mn^{\omega})$, $2 \leq \omega \leq 3$.

Contributions

Main result

Given **one vector** $x \in \mathcal{O}$ and the public key, compute a basis of $\mathcal{O}$ in polynomial-time $O(mn^{\omega})$, $2 \leq \omega \leq 3$.

n,m	112, 44	160, 64	184, 72	244, 96
Time	1.7s	4.4s	5.7s	13.3s

Figure 3: Implementation of our attack with **sagemath** on a laptop

Contributions

Main result

Given **one vector** $x \in \mathcal{O}$ and the public key, compute a basis of $\mathcal{O}$ in polynomial-time $O(mn^{\omega})$, $2 \leq \omega \leq 3$.

n,m	112, 44	160, 64	184, 72	244, 96
Time	1.7s	4.4s	5.7s	13.3s

Figure 3: Implementation of our attack with **sagemath** on a laptop

Corollary

Decide whether "$x \in \mathcal{O}$?" in polynomial-time $O(mn^{\omega})$.

Contributions

Main result

Given **one vector** $x \in \mathcal{O}$ and the public key, compute a basis of $\mathcal{O}$ in polynomial-time $O(mn^{\omega})$, $2 \leq \omega \leq 3$.

n,m	112, 44	160, 64	184, 72	244, 96
Time	1.7s	4.4s	5.7s	13.3s

Figure 3: Implementation of our attack with **sagemath** on a laptop

Corollary

Decide whether "$x \in \mathcal{O}$?" in polynomial-time $O(mn^{\omega})$.

n,m	112, 44	160, 64	184, 72	244, 96
Time	0.2s	0.5s	0.7s	1.5s

Figure 4: Implementation of "$\boldsymbol{x} \in \mathcal{O}$?" with **sagemath** on a laptop

Previous work

Side-Channel Attacks

[Aulbach, Campos, Krämer, Samardjiska, Stöttinger CHES2023] previously obtained a similar result, with a polynomial key recovery from one vector.

n	112	160	184	244
Time	19m34s		3h7m55s	11h41m7s

Figure 5: Implementation in the context of side-channel attacks

State-of-the-art of Key Recovery Attacks

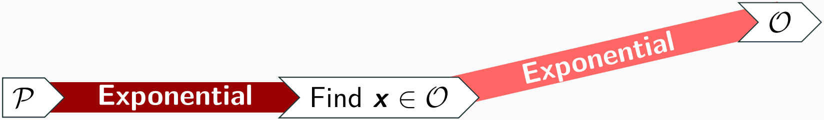
Reconciliation [Ding, Yang, Chen, Chen, Cheng 2008], [Beullens 2020/21]

Attacks benefit from knowledge of some vectors of $\mathcal{O}$:
additional equations in quadratic system

State-of-the-art of Key Recovery Attacks

Reconciliation [Ding, Yang, Chen, Chen, Cheng 2008], [Beullens 2020/21]

Attacks benefit from knowledge of some vectors of $\mathcal{O}$:
additional equations in quadratic system $\to$ Reconciliation

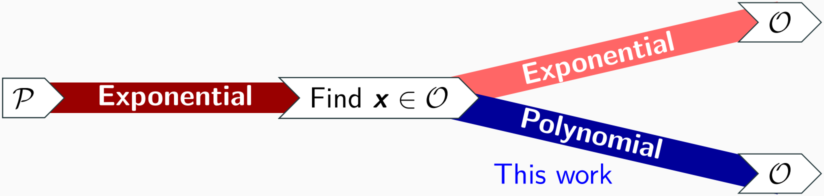


Reconciliation **[Ding, Yang, Chen, Chen, Cheng 2008], [Beullens 2020/21]**

Attacks benefit from knowledge of some vectors of $\mathcal{O}$:
additional equations in quadratic system $\rightarrow$ Reconciliation

This work

Any vector in $\mathcal{O}$ characterizes it $\rightarrow$ Polynomial reconciliation



Contribution: The algorithm

$$\mathcal{P}, \mathcal{S} : (P_1, \ldots, P_m), \mathcal{O}$$

Equivalent characterisation of the trapdoor [Beullens 2020]

Trapdoor: subspace $\mathcal{O}$ of dimension m such that

$$\forall (\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}^2, \quad \boldsymbol{x}^T P_1 \boldsymbol{y} = \cdots = \boldsymbol{x}^T P_m \boldsymbol{y} = 0$$

Contribution: The algorithm

$$\mathcal{P}, \mathcal{S} : (P_1, \ldots, P_m), \mathcal{O}$$

Equivalent characterisation of the trapdoor [Beullens 2020]

Trapdoor: subspace $\mathcal{O}$ of dimension m such that

$$\forall (\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}^2, \quad \boldsymbol{x}^T P_1 \boldsymbol{y} = \cdots = \boldsymbol{x}^T P_m \boldsymbol{y} = 0$$

Reformulation

$$\forall \boldsymbol{x} \in \mathcal{O}, \quad \mathcal{O} \subset J(\boldsymbol{x}) := \ker(\boldsymbol{x}^T P_1) \cap \ldots \cap \ker(\boldsymbol{x}^T P_m)$$

Contribution: The algorithm

$$\mathcal{P}, \mathcal{S} : (P_1, \ldots, P_m), \mathcal{O}$$

Equivalent characterisation of the trapdoor [Beullens 2020]

Trapdoor: subspace $\mathcal{O}$ of dimension m such that

$$\forall (\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{O}^2, \quad \boldsymbol{x}^T P_1 \boldsymbol{y} = \cdots = \boldsymbol{x}^T P_m \boldsymbol{y} = 0$$

Reformulation

$$\forall \boldsymbol{x} \in \mathcal{O}, \quad \mathcal{O} \subset J(\boldsymbol{x}) := \ker(\boldsymbol{x}^T P_1) \cap \ldots \cap \ker(\boldsymbol{x}^T P_m)$$

Observation

$J(\boldsymbol{x})$ is of dimension $n - m$ generically.

Contribution: The algorithm

Reduction

Restriction $\mathcal{P}_{|J(\boldsymbol{x})} \to$ UOV instance with same trapdoor but less variables.

Contribution: The algorithm

Reduction

Restriction $\mathcal{P}_{|J(\boldsymbol{x})} \to$ UOV instance with same trapdoor but less variables.

$$P_i = A^T \left(\begin{array}{c|c} 0 & \\ \hline & \end{array}\right) A \in \mathbb{F}_q^{n \times n}$$

Contribution: The algorithm

Reduction

Restriction $\mathcal{P}_{|J(\boldsymbol{x})} \to$ UOV instance with same trapdoor but less variables.

$$P_i = A^T \left(\begin{array}{c|c} 0 & \\ \hline & \end{array}\right) A \in \mathbb{F}_q^{n \times n}$$

$$\implies P_{i|J(x)} = B^T \left(\begin{array}{c|c} 0 & \\ \hline & \end{array}\right) B \in \mathbb{F}_q^{n-m \times n-m}$$

Contribution: The algorithm

Reduction

Restriction $\mathcal{P}_{|J(\boldsymbol{x})} \to$ UOV instance with same trapdoor but less variables.

$$P_i = A^T \left(\begin{array}{c|c} 0 & \\ \hline & \end{array}\right) A \in \mathbb{F}_q^{n \times n}$$

$$\implies P_{i|J(x)} = B^T \left(\begin{array}{c|c} 0 & \\ \hline & \end{array}\right) B \in \mathbb{F}_q^{n-m \times n-m}$$

Concluding the attack

$$n - m \leq 2m \implies P_{i|J(x)} \text{ is singular.}$$

Contribution: Complexity analysis

Complexity of the attack

1. Computing $J(\boldsymbol{x})$, kernel of $m \times n$ matrix $O(mn^2)$

Contribution: Complexity analysis

Complexity of the attack

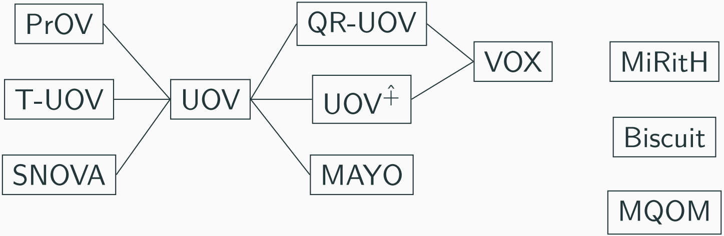
1. Computing $J(\boldsymbol{x})$, kernel of $m \times n$ matrix $O(mn^2)$
2. Computing the restrictions: $P_{i|J(\boldsymbol{x})} = B^T P_i B$ $O(mn^\omega)$

Contribution: Complexity analysis

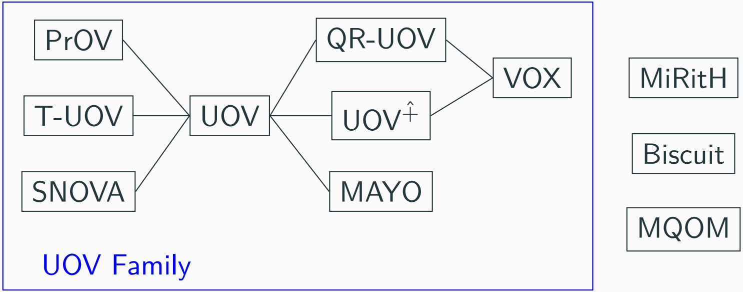
Complexity of the attack

1. Computing $J(\boldsymbol{x})$, kernel of $m \times n$ matrix $O(mn^2)$
2. Computing the restrictions: $P_{i|J(\boldsymbol{x})} = B^T P_i B$ $O(mn^\omega)$
3. Kernel computations $O(mn^\omega)$
4. Total cost: $\boldsymbol{O(mn^\omega)}$

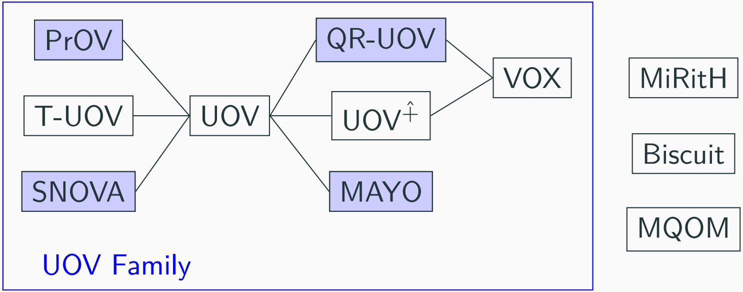
Multivariate Post-Quantum Zoo at NIST



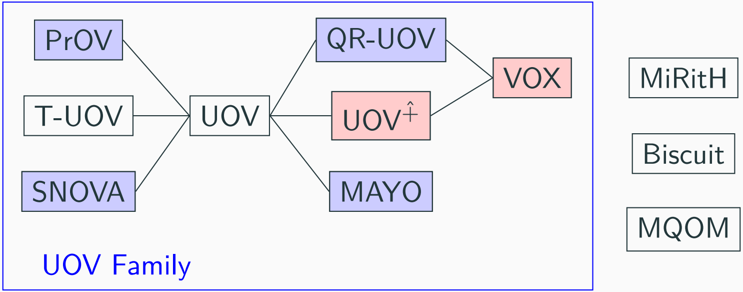
Multivariate Post-Quantum Zoo at NIST



Multivariate Post-Quantum Zoo at NIST



Multivariate Post-Quantum Zoo at NIST



Key recovery attacks from "$x \in \mathcal{O}$?" on UOV($\hat{+}$)

UOV$\hat{+}$

Replace $t \leq 8$ equations with random equations and mix.

$$\mathcal{P} = \mathcal{S} \cdot (F_1 \circ A, \ldots, F_t \circ A, F_{t+1} \circ A, \ldots, F_m \circ A)$$

Key recovery attacks from "$x \in \mathcal{O}$?" on UOV($\hat{+}$)

UOV$\hat{+}$

Replace $t \leq 8$ equations with random equations and mix.

$$\mathcal{P} = \mathcal{S} \cdot (F_1 \circ A, \ldots, F_t \circ A, F_{t+1} \circ A, \ldots, F_m \circ A)$$

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

- This work: need t vectors in $\mathcal{O}$ to decide in $O(mn^\omega)$

Key recovery attacks from "$x \in \mathcal{O}$?" on UOV($\hat{+}$)

UOV$\hat{+}$

Replace $t \leq 8$ equations with random equations and mix.

$$\mathcal{P} = \mathcal{S} \cdot (F_1 \circ A, \ldots, F_t \circ A, F_{t+1} \circ A, \ldots, F_m \circ A)$$

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

- This work: need t vectors in $\mathcal{O}$ to decide in $O(mn^{\omega})$
- [P. 2024b]: need 1 vector to decide in $O(q^t n^{\omega})$

Key recovery attacks from "$x \in \mathcal{O}$?" on UOV($\hat{+}$)

UOV$\hat{+}$

Replace $t \leq 8$ equations with random equations and mix.

$$\mathcal{P} = \mathcal{S} \cdot (F_1 \circ A, \ldots, F_t \circ A, F_{t+1} \circ A, \ldots, F_m \circ A)$$

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

- This work: need t vectors in $\mathcal{O}$ to decide in $O(mn^\omega)$
- [P. 2024b]: need 1 vector to decide in $O(q^t n^\omega)$

Improve Kipnis-Shamir attack against UOV$\hat{+}$ [P. 2024b]

$$\implies O(q^{3t}) \to O(q^{2t} \cdot \text{poly}(n))$$

Perspectives

Contributions

- One secret vector $\rightarrow$ polynomial key recovery.
- Distinguish secret vectors from random signatures of 0.

New directions

- Efficiently generalize tools to more UOV schemes
- Key recovery attacks targeting one vector

Links

`https://github.com/pi-r2/OneVector`

Application to UOV variants in the NIST competition

For schemes that are instances of UOV $\rightarrow$ direct application

- QR-UOV
- SNOVA
- PrOV
- Result already known on MAYO [Beullens 2021]

Application to UOV variants in the NIST competition

For schemes that are instances of UOV $\rightarrow$ direct application

- QR-UOV
- SNOVA
- PrOV
- Result already known on MAYO [Beullens 2021]

More work required for schemes using modified UOV keys.

- Can it be faster on $\text{UOV}^{\hat{+}}$?
- T-UOV