TU Graz

SCIENCE
PASSION
TECHNOLOGY

Lightweight UOV Accelerator with Oil Space Blinding

Florian Krieger

Institute of Information Security, Graz University of Technology

RIGOLETTO
HIGH PERFORMANCE
RISC-V SOLUTIONS

Outline

1 Motivation and Background

2 Lightweight UOV Acceleration

3 Side-Channel Security of UOV

NIST's Additional Signatures: Round 2 → 3

Multivariate

UOV
MAYO
QR-UOV
SNOVA

Isogeny

SQIsign

MPC-in-the-Head

MQOM
SDitH
Mirath
PERK
RYDE

Symmetric

FAEST

Code-based

CROSS
LESS

Lattice

HAWK

NIST's Additional Signatures: Round 2 → 3

Multivariate

UOV
MAYO
QR-UOV
SNOVA

Isogeny

SQIsign

MPC-in-the-Head

MQOM
SDitH
~~Mirath~~
~~PERK~~
~~RYDE~~

Symmetric

FAEST

Code-based

~~CROSS~~
~~LESS~~

Lattice

~~HAWK~~

Why MV? Why UOV? [Beu+25b]

Multivariate (MV) schemes

UOV (Unbalanced Oil and Vinegar)

Why MV? Why UOV? [Beu+25b]

Multivariate (MV) schemes

- ⊕ Small signatures, fast signing and verification

UOV (Unbalanced Oil and Vinegar)

Why MV? Why UOV? [Beu+25b]

Multivariate (MV) schemes

- ⊕ Small signatures, fast signing and verification
- ⊕ Decades of cryptanalysis

UOV (Unbalanced Oil and Vinegar)

Why MV? Why UOV? [Beu+25b]

Multivariate (MV) schemes

- ⊕ Small signatures, fast signing and verification
- ⊕ Decades of cryptanalysis
- ⊖ Large public keys (kB - MB)

UOV (Unbalanced Oil and Vinegar)

Why MV? Why UOV? [Beu+25b]

Multivariate (MV) schemes

- ⊕ Small signatures, fast signing and verification
- ⊕ Decades of cryptanalysis
- ⊖ Large public keys (kB - MB)

UOV (Unbalanced Oil and Vinegar)

- ⊕ Best signing latency and signature size among MV candidates [WP26]

Why MV? Why UOV? [Beu+25b]

Multivariate (MV) schemes

- ⊕ Small signatures, fast signing and verification
- ⊕ Decades of cryptanalysis
- ⊖ Large public keys (kB - MB)

UOV (Unbalanced Oil and Vinegar)

- ⊕ Best signing latency and signature size among MV candidates [WP26]
- ⊕ Conservative

Why MV? Why UOV? [Beu+25b]

Multivariate (MV) schemes

- ⊕ Small signatures, fast signing and verification
- ⊕ Decades of cryptanalysis
- ⊖ Large public keys (kB - MB)

UOV (Unbalanced Oil and Vinegar)

- ⊕ Best signing latency and signature size among MV candidates [WP26]
- ⊕ Conservative
- → Same core operations as MAYO [Beu+25a]

Why MV? Why UOV? [Beu+25b]

Multivariate (MV) schemes

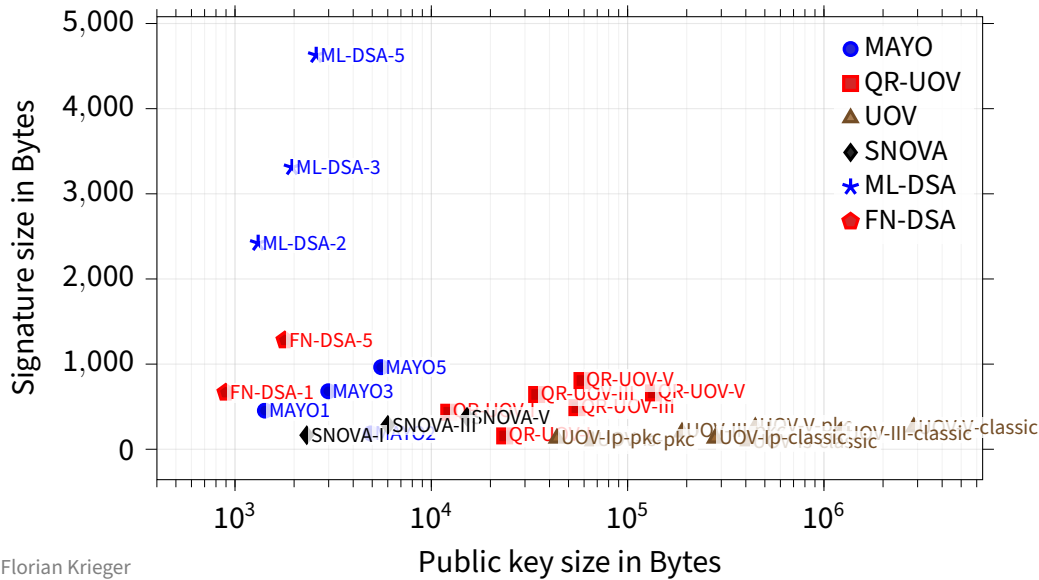
- ⊕ Small signatures, fast signing and verification
- ⊕ Decades of cryptanalysis
- ⊖ Large public keys (kB - MB)

UOV (Unbalanced Oil and Vinegar)

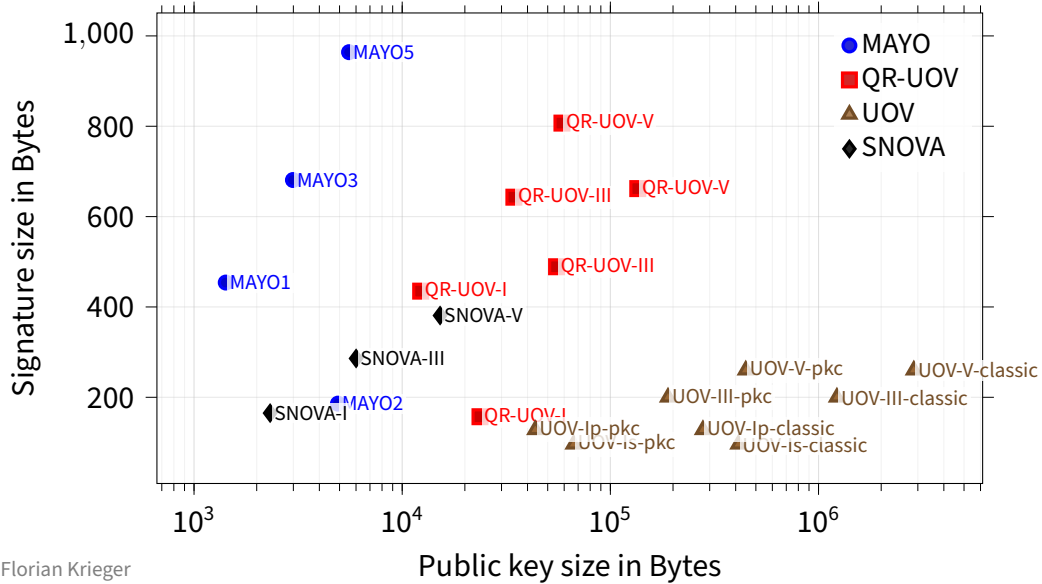
- ⊕ Best signing latency and signature size among MV candidates [WP26]
- ⊕ Conservative
- → Same core operations as MAYO [Beu+25a]

Rigoletto Goal: Lightweight PQC Co-processor

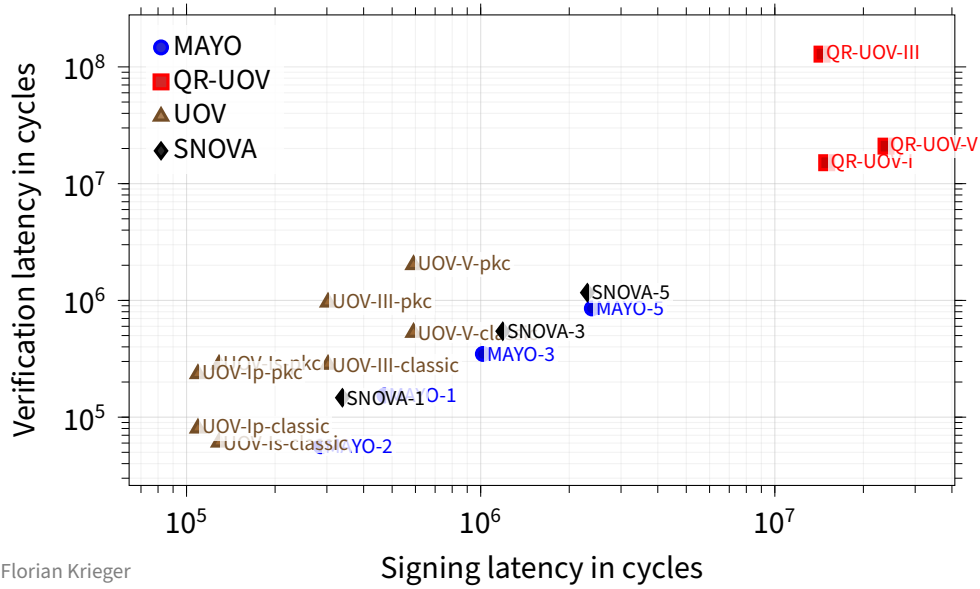
Key and Signature Sizes [WP26]



Key and Signature Sizes [WP26]



Performance in SW [WP26]



How UOV Works

Public map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, $q \in \{16, 256\}$

How UOV Works

Public map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, $q \in \{16, 256\}$

$$\mathcal{P}(\mathbf{x}) = (p_0(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x}))$$

How UOV Works

Public map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, $q \in \{16, 256\}$

$$\mathcal{P}(\mathbf{x}) = (p_0(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x}))$$

$$p_i(\mathbf{x}) = \mathbf{x}^\top \mathbf{P}_i \mathbf{x} = \mathbf{x}^\top \underbrace{\begin{bmatrix} \mathbf{P}_i^{(1)} & \mathbf{P}_i^{(2)} \\ \mathbf{0} & \mathbf{P}_i^{(3)} \end{bmatrix}}_{\text{public key}} \mathbf{x}$$

How UOV Works

Public map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$**,** $q \in \{16, 256\}$

$$\mathcal{P}(\mathbf{x}) = (p_0(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x}))$$

$$p_i(\mathbf{x}) = \mathbf{x}^\top \mathbf{P}_i \mathbf{x} = \mathbf{x}^\top \underbrace{\begin{bmatrix} \mathbf{P}_i^{(1)} & \mathbf{P}_i^{(2)} \\ \mathbf{0} & \mathbf{P}_i^{(3)} \end{bmatrix}}_{\text{public key}} \mathbf{x}$$

Verification: Signature **s** and msg

$$\mathbf{t} \leftarrow \mathcal{H}(\text{msg})$$

How UOV Works

Public map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, $q \in \{16, 256\}$

$$\mathcal{P}(\mathbf{x}) = (p_0(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x}))$$

$$p_i(\mathbf{x}) = \mathbf{x}^\top \mathbf{P}_i \mathbf{x} = \mathbf{x}^\top \underbrace{\begin{bmatrix} \mathbf{P}_i^{(1)} & \mathbf{P}_i^{(2)} \\ \mathbf{0} & \mathbf{P}_i^{(3)} \end{bmatrix}}_{\text{public key}} \mathbf{x}$$

Verification: Signature **s** and msg

$$\mathbf{t} \leftarrow \mathcal{H}(\text{msg})$$

$$\mathcal{P}(\mathbf{s}) \stackrel{?}{=} \mathbf{t}$$

How UOV Works

Public map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, $q \in \{16, 256\}$

$$\mathcal{P}(\mathbf{x}) = (p_0(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x}))$$

$$p_i(\mathbf{x}) = \mathbf{x}^\top \mathbf{P}_i \mathbf{x} = \mathbf{x}^\top \underbrace{\begin{bmatrix} \mathbf{P}_i^{(1)} & \mathbf{P}_i^{(2)} \\ \mathbf{0} & \mathbf{P}_i^{(3)} \end{bmatrix}}_{\text{public key}} \mathbf{x}$$

Verification: Signature **s** and msg

$$\mathbf{t} \leftarrow \mathcal{H}(\text{msg})$$

$$\mathcal{P}(\mathbf{s}) \stackrel{?}{=} \mathbf{t}$$

Trapdoor (secret key)

A secret m-dimensional **oil space** O in which $\mathcal{P}$ vanishes

$$\forall \mathbf{o} \in O : \mathcal{P}(\mathbf{o}) = \mathbf{0}$$

How UOV Works

Public map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, $q \in \{16, 256\}$

$$\mathcal{P}(\mathbf{x}) = (p_0(\mathbf{x}), \ldots, p_{m-1}(\mathbf{x}))$$

$$p_i(\mathbf{x}) = \mathbf{x}^\top \mathbf{P}_i \mathbf{x} = \mathbf{x}^\top \underbrace{\begin{bmatrix} \mathbf{P}_i^{(1)} & \mathbf{P}_i^{(2)} \\ \mathbf{0} & \mathbf{P}_i^{(3)} \end{bmatrix}}_{\text{public key}} \mathbf{x}$$

Verification: Signature **s** and msg

$$\mathbf{t} \leftarrow \mathcal{H}(\text{msg})$$

$$\mathcal{P}(\mathbf{s}) \stackrel{?}{=} \mathbf{t}$$

Trapdoor (secret key)

A secret m-dimensional **oil space** O in which $\mathcal{P}$ vanishes

$$\forall \mathbf{o} \in O : \mathcal{P}(\mathbf{o}) = \mathbf{0}$$

$\bar{\mathbf{O}}$ is a basis of O

How UOV Works: Signing

1. Given $\bar{\mathbf{O}}$ (a basis of O), find $\mathbf{s}$ such that $\mathcal{P}(\mathbf{s}) = \mathbf{t}$.

How UOV Works: Signing

1. Given $\bar{\mathbf{O}}$ (a basis of O), find $\mathbf{s}$ such that $\mathcal{P}(\mathbf{s}) = \mathbf{t}$.
2. $\mathbf{s} = \mathbf{v} + \mathbf{o}$

How UOV Works: Signing

1. Given $\bar{\mathbf{O}}$ (a basis of O), find $\mathbf{s}$ such that $\mathcal{P}(\mathbf{s}) = \mathbf{t}$.
2. $\mathbf{s} = \mathbf{v} + \mathbf{o}$
3. Sample random $\mathbf{v}$

How UOV Works: Signing

1. Given $\bar{\mathbf{O}}$ (a basis of O), find $\mathbf{s}$ such that $\mathcal{P}(\mathbf{s}) = \mathbf{t}$.
2. $\mathbf{s} = \mathbf{v} + \mathbf{o}$
3. Sample random $\mathbf{v}$
4. Solve $\mathcal{P}(\mathbf{s}) = \mathcal{P}(\mathbf{v} + \mathbf{o}) = \underbrace{\mathcal{P}(\mathbf{v})}_{\text{const.}} + \underbrace{\mathcal{P}(\mathbf{o})}_{=\mathbf{0}_m} + \underbrace{\mathcal{P}'(\mathbf{v}, \mathbf{o})}_{\text{linear in } \mathbf{o}} = \mathbf{t}$ for $\mathbf{o} \in O$

How UOV Works: Signing

1. Given $\bar{\mathbf{O}}$ (a basis of O), find $\mathbf{s}$ such that $\mathcal{P}(\mathbf{s}) = \mathbf{t}$.
2. $\mathbf{s} = \mathbf{v} + \mathbf{o}$
3. Sample random $\mathbf{v}$
4. Solve $\mathcal{P}(\mathbf{s}) = \mathcal{P}(\mathbf{v} + \mathbf{o}) = \underbrace{\mathcal{P}(\mathbf{v})}_{\text{const.}} + \underbrace{\mathcal{P}(\mathbf{o})}_{=\mathbf{0}_m} + \underbrace{\mathcal{P}'(\mathbf{v}, \mathbf{o})}_{\text{linear in } \mathbf{o}} = \mathbf{t}$ for $\mathbf{o} \in O$

   → Linear equation system

UOV Signing and Verification (with some details omitted)

- Key expansion

UOV.Sign(csk, μ)

1: $\mathsf{seed}_{\mathsf{pk}}, \bar{\mathbf{O}} \leftarrow \mathsf{Shake}_{256}(\mathsf{csk})$
2: $\{\mathbf{P}_i^{(1)}\}, \{\mathbf{P}_i^{(2)}\} \leftarrow \mathsf{AES}_{128}\mathsf{CTR}(\mathsf{seed}_{\mathsf{pk}})$
3: $\mathsf{salt} \xleftarrow{\$} \{0,1\}^{\mathsf{salt\_len}}$, $\mathbf{t} \leftarrow \mathsf{Shake}_{256}(\mu \,\|\, \mathsf{salt})$
4: **for** $\mathsf{ctr} = 0$ **upto** 255 **do**
5: $\quad \mathbf{v} \leftarrow \mathsf{Shake}_{256}(\mu \| \mathsf{salt} \| \mathsf{seed}_{\mathsf{sk}} \| \mathsf{ctr})$
6: $\quad \mathbf{A} \leftarrow \mathbf{0}_{m \times m}, \quad \mathbf{y} \leftarrow \mathbf{0}_m$
7: $\quad$ **for** $i = 0$ **upto** $m - 1$ **do**
8: $\quad\quad \mathbf{A}[i,:] \leftarrow \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)^\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}}$
9: $\quad\quad \mathbf{y}[i] \leftarrow \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v}$
10: $\quad$ Solve $\mathbf{Ax} = \mathbf{t} - \mathbf{y}$ for $\mathbf{x}$ if possible, else repeat
11: $\quad \mathbf{s} \leftarrow \begin{pmatrix} \mathbf{v} \\ \mathbf{0}_m \end{pmatrix} + \bar{\mathbf{O}}\mathbf{x}$; **return** $\sigma = (\mathbf{s}, \mathsf{salt})$

UOV Signing and Verification (with some details omitted)

Key expansion Hashing

UOV.Sign(csk, μ)

1: $\mathsf{seed}_{\mathsf{pk}}, \bar{\mathbf{O}} \leftarrow \mathsf{Shake}_{256}(\mathsf{csk})$
2: $\{\mathbf{P}_i^{(1)}\}, \{\mathbf{P}_i^{(2)}\} \leftarrow \mathsf{AES}_{128}\mathsf{CTR}(\mathsf{seed}_{\mathsf{pk}})$
3: $\mathsf{salt} \xleftarrow{\$} \{0,1\}^{\mathsf{salt\_len}}$, $\mathbf{t} \leftarrow \mathsf{Shake}_{256}(\mu \,\|\, \mathsf{salt})$
4: **for** $\mathsf{ctr} = 0$ **upto** 255 **do**
5: $\quad \mathbf{v} \leftarrow \mathsf{Shake}_{256}(\mu \| \mathsf{salt} \| \mathsf{seed}_{\mathsf{sk}} \| \mathsf{ctr})$
6: $\quad \mathbf{A} \leftarrow \mathbf{0}_{m \times m}, \quad \mathbf{y} \leftarrow \mathbf{0}_m$
7: $\quad$ **for** $i = 0$ **upto** $m - 1$ **do**
8: $\quad\quad \mathbf{A}[i,:] \leftarrow \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)^\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}}$
9: $\quad\quad \mathbf{y}[i] \leftarrow \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v}$
10: $\quad$ Solve $\mathbf{Ax} = \mathbf{t} - \mathbf{y}$ for $\mathbf{x}$ if possible, else repeat
11: $\quad \mathbf{s} \leftarrow \binom{\mathbf{v}}{\mathbf{0}_m} + \bar{\mathbf{O}}\mathbf{x}$; **return** $\sigma = (\mathbf{s}, \mathsf{salt})$

UOV Signing and Verification (with some details omitted)

Key expansion Hashing Build linear system

UOV.Sign(csk, μ)

1: $\mathsf{seed}_{\mathsf{pk}}, \bar{\mathbf{O}} \leftarrow \mathrm{Shake}_{256}(\mathsf{csk})$
2: $\{\mathbf{P}_i^{(1)}\}, \{\mathbf{P}_i^{(2)}\} \leftarrow \mathrm{AES}_{128}\mathrm{CTR}(\mathsf{seed}_{\mathsf{pk}})$
3: $\mathsf{salt} \xleftarrow{\$} \{0,1\}^{\mathsf{salt\_len}}$, $\mathbf{t} \leftarrow \mathrm{Shake}_{256}(\mu \,\|\, \mathsf{salt})$
4: **for** $\mathsf{ctr} = 0$ **upto** 255 **do**
5: $\quad \mathbf{v} \leftarrow \mathrm{Shake}_{256}(\mu \| \mathsf{salt} \| \mathsf{seed}_{\mathsf{sk}} \| \mathsf{ctr})$
6: $\quad \mathbf{A} \leftarrow \mathbf{0}_{m \times m}, \quad \mathbf{y} \leftarrow \mathbf{0}_m$
7: $\quad$ **for** $i = 0$ **upto** $m - 1$ **do**
8: $\quad\quad \mathbf{A}[i,:] \leftarrow \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)^\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}}$
9: $\quad\quad \mathbf{y}[i] \leftarrow \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v}$
10: $\quad$ Solve $\mathbf{Ax} = \mathbf{t} - \mathbf{y}$ for $\mathbf{x}$ if possible, else repeat
11: $\quad \mathbf{s} \leftarrow \begin{pmatrix} \mathbf{v} \\ \mathbf{0}_m \end{pmatrix} + \bar{\mathbf{O}}\mathbf{x}$; **return** $\sigma = (\mathbf{s}, \mathsf{salt})$

UOV Signing and Verification (with some details omitted)

Key expansion Hashing Build linear system Solve

UOV.Sign(csk, μ)

1: $\mathsf{seed}_{\mathsf{pk}}, \bar{\mathbf{O}} \leftarrow \mathsf{Shake}_{256}(\mathsf{csk})$

2: $\{\mathbf{P}_i^{(1)}\}, \{\mathbf{P}_i^{(2)}\} \leftarrow \mathsf{AES}_{128}\mathsf{CTR}(\mathsf{seed}_{\mathsf{pk}})$

3: $\mathsf{salt} \xleftarrow{\$} \{0,1\}^{\mathsf{salt\_len}}$, $\mathbf{t} \leftarrow \mathsf{Shake}_{256}(\mu \,\|\, \mathsf{salt})$

4: **for** ctr $= 0$ **upto** 255 **do**

5: $\quad \mathbf{v} \leftarrow \mathsf{Shake}_{256}(\mu \| \mathsf{salt} \| \mathsf{seed}_{\mathsf{sk}} \| \mathsf{ctr})$

6: $\quad \mathbf{A} \leftarrow \mathbf{0}_{m \times m}, \quad \mathbf{y} \leftarrow \mathbf{0}_m$

7: $\quad$ **for** $i = 0$ **upto** $m - 1$ **do**

8: $\quad\quad \mathbf{A}[i,:] \leftarrow \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)^\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}}$

9: $\quad\quad \mathbf{y}[i] \leftarrow \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v}$

10: $\quad$ Solve $\mathbf{Ax} = \mathbf{t} - \mathbf{y}$ for $\mathbf{x}$ if possible, else repeat

11: $\quad \mathbf{s} \leftarrow \begin{pmatrix} \mathbf{v} \\ \mathbf{0}_m \end{pmatrix} + \bar{\mathbf{O}}\mathbf{x}$; $\quad$ **return** $\sigma = (\mathbf{s}, \mathsf{salt})$

The Research Problem: Lightweight UOV Acceleration

- No lightweight UOV hardware accelerator
- UOV needs large memories
  - Up to 1.6 MB in existing HW
  - Problematic for low-end deployment
- Lightweight SCA countermeasures

Lightweight UOV Acceleration

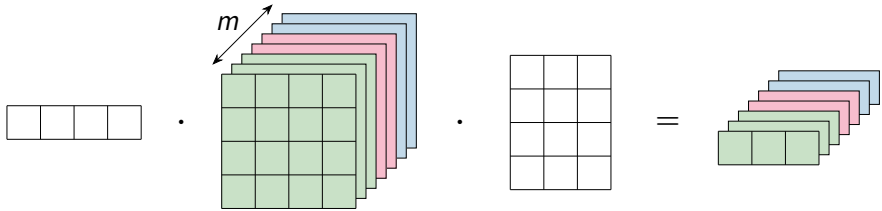
Reducing the memory consumption

One Pattern Behind All Critical Operations

$$\mathbf{A}[i,:] = \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)^\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}} \qquad \mathbf{y}[i] = \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v} \qquad i = 0, \ldots, m-1$$

One Pattern Behind All Critical Operations

$$\mathbf{A}[i,:] = \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}} \qquad \mathbf{y}[i] = \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v} \qquad i = 0, \ldots, m-1$$



$\mathbf{v}^\top$
single row vector

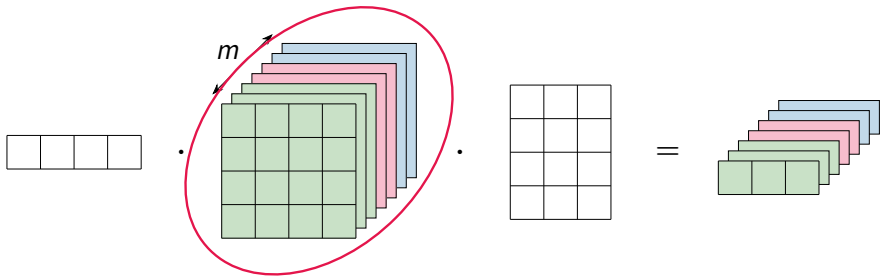
$\{\mathbf{P}_i\}_{i \in [m]}$
set of m matrices

$\bar{\mathbf{O}}$ or $\mathbf{v}$
single matrix or column vector

m results
m vectors
or m scalars

One Pattern Behind All Critical Operations

$$\mathbf{A}[i,:] = \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)^\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}} \qquad \mathbf{y}[i] = \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v} \qquad i = 0, \ldots, m-1$$



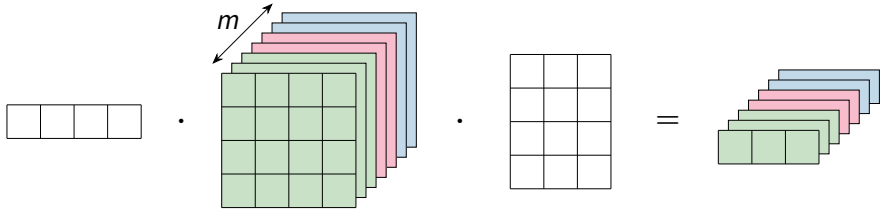
$\mathbf{v}^\top$
single row vector

$\{\mathbf{P}_i\}_{i \in [m]}$
set of m matrices

$\bar{\mathbf{O}}$ or $\mathbf{v}$
single matrix or column vector

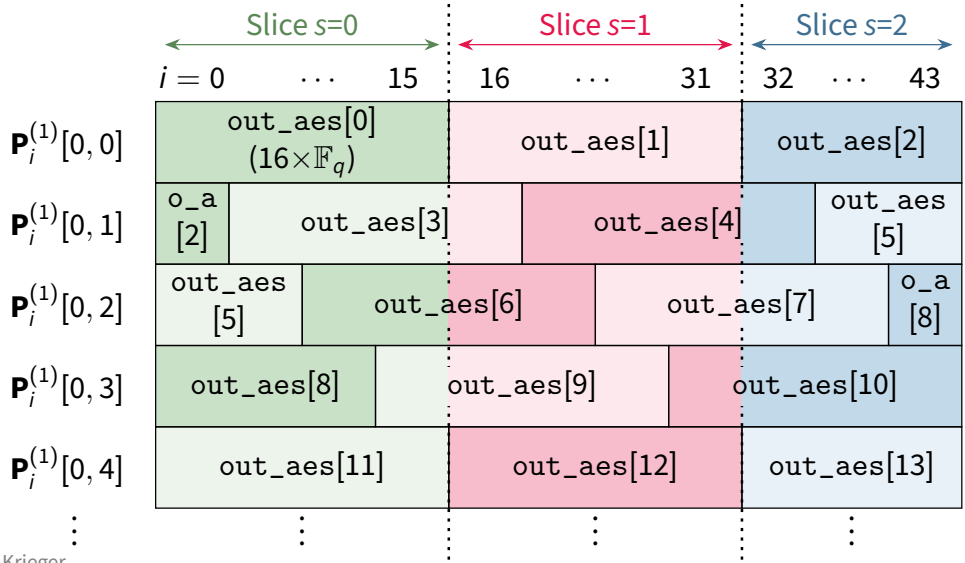
m results
m vectors
or m scalars

On-the-Fly Generation

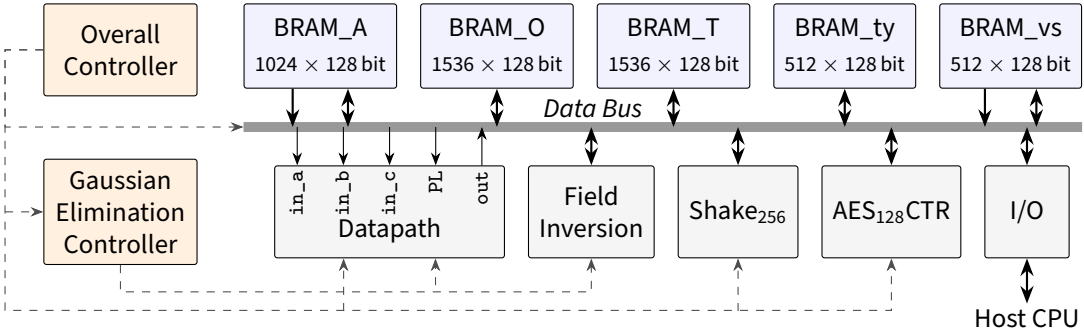


- $\mathbf{P}_i$ sampled from AES-128-CTR
- Unfavorable data layout

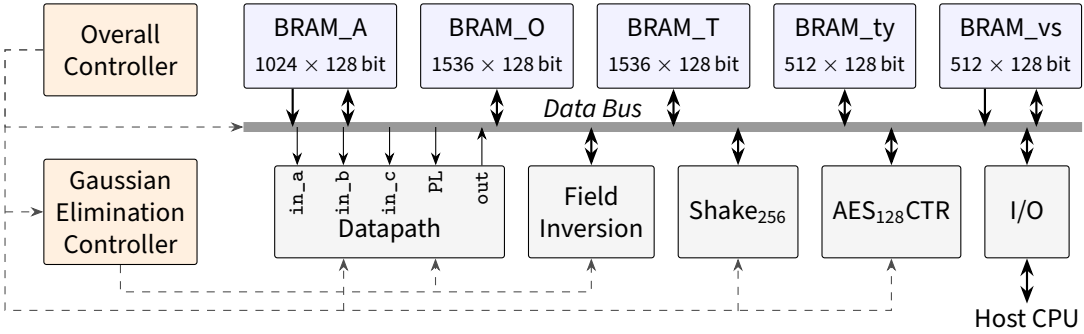
On-the-Fly Generation: Data Rearrangement



Overall Architecture



Overall Architecture



up to 16×
less on-chip memory

up to 5.1×
faster signing

up to 74×
better ATP

Best case vs. prior UOV hardware [Beu+23].

Side-Channel Security of UOV

Known Fault and SCA Attack Points of UOV

- Fault on $\mathbf{t}$ in deterministic UOV [BDK25]

UOV.Sign(csk, μ)

1: $\text{seed}_{\text{pk}}, \bar{\mathbf{O}} \leftarrow \text{Shake}_{256}(\text{csk})$
2: $\{\mathbf{P}_i^{(1)}\}, \{\mathbf{P}_i^{(2)}\} \leftarrow \text{AES}_{128}\text{CTR}(\text{seed}_{\text{pk}})$
3: $\text{salt} \xleftarrow{\$} \{0,1\}^{\text{salt\_len}}$, $\mathbf{t} \leftarrow \text{Shake}_{256}(\mu \,\|\, \text{salt})$
4: **for** ctr $= 0$ **upto** 255 **do**
5: $\quad \mathbf{v} \leftarrow \text{Shake}_{256}(\mu \| \text{salt} \| \text{seed}_{\text{sk}} \| \text{ctr})$
6: $\quad \mathbf{A} \leftarrow \mathbf{0}_{m \times m}, \quad \mathbf{y} \leftarrow \mathbf{0}_m$
7: $\quad$ **for** $i = 0$ **upto** $m - 1$ **do**
8: $\quad\quad \mathbf{A}[i,:] \leftarrow \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)^\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}}$
9: $\quad\quad \mathbf{y}[i] \leftarrow \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v}$
10: $\quad$ Solve $\mathbf{Ax} = \mathbf{t} - \mathbf{y}$ for $\mathbf{x}$ if possible, else repeat
11: $\quad \mathbf{s} \leftarrow \begin{pmatrix} \mathbf{v} \\ \mathbf{0}_m \end{pmatrix} + \bar{\mathbf{O}}\mathbf{x}$; **return** $\sigma = (\mathbf{s}, \text{salt})$

All attacks recover a vector of the oil space $\mathbf{o} \in O$

Known Fault and SCA Attack Points of UOV

■ Fault on **t** in deterministic UOV [BDK25] ■ Fixed vinegar seed [JD24]

UOV.Sign(csk, μ)

1: $\mathsf{seed}_{\mathsf{pk}}, \bar{\mathbf{O}} \leftarrow \mathsf{Shake}_{256}(\mathsf{csk})$
2: $\{\mathbf{P}_i^{(1)}\}, \{\mathbf{P}_i^{(2)}\} \leftarrow \mathsf{AES}_{128}\mathsf{CTR}(\mathsf{seed}_{\mathsf{pk}})$
3: $\mathsf{salt} \xleftarrow{\$} \{0,1\}^{\mathsf{salt\_len}}$, $\mathbf{t} \leftarrow \mathsf{Shake}_{256}(\mu \,\|\, \mathsf{salt})$
4: **for** ctr $= 0$ **upto** 255 **do**
5: $\quad \mathbf{v} \leftarrow \mathsf{Shake}_{256}(\mu \| \mathsf{salt} \| \mathsf{seed}_{\mathsf{sk}} \| \mathsf{ctr})$
6: $\quad \mathbf{A} \leftarrow \mathbf{0}_{m \times m}, \quad \mathbf{y} \leftarrow \mathbf{0}_m$
7: $\quad$ **for** $i = 0$ **upto** $m - 1$ **do**
8: $\quad\quad \mathbf{A}[i,:] \leftarrow \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)^\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}}$
9: $\quad\quad \mathbf{y}[i] \leftarrow \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v}$
10: $\quad$ Solve $\mathbf{Ax} = \mathbf{t} - \mathbf{y}$ for $\mathbf{x}$ if possible, else repeat
11: $\quad \mathbf{s} \leftarrow \begin{pmatrix} \mathbf{v} \\ \mathbf{0}_m \end{pmatrix} + \bar{\mathbf{O}}\mathbf{x}$; **return** $\sigma = (\mathbf{s}, \mathsf{salt})$

All attacks recover a vector of the oil space $\mathbf{o} \in O$

Known Fault and SCA Attack Points of UOV

Fault on $\mathbf{t}$ in deterministic UOV [BDK25] | Fixed vinegar seed [JD24] | Leaky products with $\bar{\mathbf{O}}$ [JD26]

UOV.Sign(csk, μ)

1: $\text{seed}_{\text{pk}}, \bar{\mathbf{O}} \leftarrow \text{Shake}_{256}(\text{csk})$
2: $\{\mathbf{P}_i^{(1)}\}, \{\mathbf{P}_i^{(2)}\} \leftarrow \text{AES}_{128}\text{CTR}(\text{seed}_{\text{pk}})$
3: $\text{salt} \xleftarrow{\$} \{0,1\}^{\text{salt\_len}}$, $\mathbf{t} \leftarrow \text{Shake}_{256}(\mu \,\|\, \text{salt})$
4: **for** ctr $= 0$ **upto** 255 **do**
5: $\quad \mathbf{v} \leftarrow \text{Shake}_{256}(\mu \| \text{salt} \| \text{seed}_{\text{sk}} \| \text{ctr})$
6: $\quad \mathbf{A} \leftarrow \mathbf{0}_{m \times m}, \quad \mathbf{y} \leftarrow \mathbf{0}_m$
7: $\quad$ **for** $i = 0$ **upto** $m - 1$ **do**
8: $\quad\quad \mathbf{A}[i,:] \leftarrow \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)^\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}}$
9: $\quad\quad \mathbf{y}[i] \leftarrow \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v}$
10: $\quad$ Solve $\mathbf{Ax} = \mathbf{t} - \mathbf{y}$ for $\mathbf{x}$ if possible, else repeat
11: $\quad \mathbf{s} \leftarrow \begin{pmatrix} \mathbf{v} \\ \mathbf{0}_m \end{pmatrix} + \bar{\mathbf{O}}\mathbf{x}$; $\quad$ **return** $\sigma = (\mathbf{s}, \text{salt})$

All attacks recover a vector of the oil space $\mathbf{o} \in O$

Countermeasures for UOV

- Shuffling has been proposed

Countermeasures for UOV

- Shuffling has been proposed
- Masked microcontroller implementations exist
  - [Kun+25]: 12× runtime overhead
  - [CGZ26]: 7.1× runtime overhead

Countermeasures for UOV

- Shuffling has been proposed
- Masked microcontroller implementations exist
  - [Kun+25]: 12× runtime overhead
  - [CGZ26]: 7.1× runtime overhead
- ? More lightweight SCA countermeasures

UOV's Equivalent Keys: Blinding

- $\bar{\mathbf{o}}$ is a secret basis of O

UOV's Equivalent Keys: Blinding

- $\bar{\mathbf{O}}$ is a secret basis of O
- There are many bases spanning **the same** O

UOV's Equivalent Keys: Blinding

- $\bar{\mathbf{O}}$ is a secret basis of O
- There are many bases spanning **the same** O
- Randomize basis $\bar{\mathbf{O}}_b$ for each signing

$$\bar{\mathbf{O}}_b = \bar{\mathbf{O}} \cdot \mathbf{R} \text{ with random invertible } \mathbf{R}$$

Blinded UOV

UOV.BlindedSign$(\text{seed}_{\text{pk}}, \text{seed}_{\text{sk}}, \bar{\mathbf{O}}_b, \mu)$

1: Load $\bar{\mathbf{O}}_b$ from persistent storage
2: $\{\mathbf{P}_i^{(1)}\}, \{\mathbf{P}_i^{(2)}\} \leftarrow \text{AES}_{128}\text{CTR}(\text{seed}_{\text{pk}})$
3: $\text{salt} \xleftarrow{\$} \{0,1\}^{\text{salt\_len}}$, $\mathbf{t} \leftarrow \text{Shake}_{256}(\mu \,\|\, \text{salt})$
4: **for** ctr $= 0$ **upto** 255 **do**
5: $\quad \mathbf{v} \leftarrow \text{Shake}_{256}(\mu \| \text{salt} \| \text{seed}_{\text{sk}} \| \text{ctr})$
6: $\quad \mathbf{R} \xleftarrow{\$} \text{GL}_m(\mathbb{F}_q)$; $\quad \bar{\mathbf{O}}_b \leftarrow \bar{\mathbf{O}}_b \cdot \mathbf{R}$ $\quad \triangleright$ re-randomize the basis
7: $\quad \mathbf{A} \leftarrow \mathbf{0}_{m \times m}$, $\quad \mathbf{y} \leftarrow \mathbf{0}_m$
8: $\quad$ **for** $i = 0$ **upto** $m - 1$ **do**
9: $\quad\quad \mathbf{A}[i,:] \leftarrow \mathbf{v}^\top \left(\mathbf{P}_i^{(1)} + \mathbf{P}_i^{(1)^\top} \;\middle|\; \mathbf{P}_i^{(2)} \right) \bar{\mathbf{O}}_b$
10: $\quad\quad \mathbf{y}[i] \leftarrow \mathbf{v}^\top \mathbf{P}_i^{(1)} \mathbf{v}$
11: $\quad$ Solve $\mathbf{Ax} = \mathbf{t} - \mathbf{y}$ for $\mathbf{x}$ if possible, else repeat
12: $\quad \mathbf{s} \leftarrow \begin{pmatrix} \mathbf{v} \\ \mathbf{0}_m \end{pmatrix} + \bar{\mathbf{O}}_b \mathbf{x}$; $\quad$ store $\bar{\mathbf{O}}_b$; $\quad$ **return** $\sigma = (\mathbf{s}, \text{salt})$

Blinded UOV

- Makes DPA attacks more difficult
  → Long-term secret $\bar{\mathbf{O}}$ is turned into ephemeral secret $\bar{\mathbf{O}}_b$

Blinded UOV

- Makes DPA attacks more difficult
  → Long-term secret $\bar{\mathbf{O}}$ is turned into ephemeral secret $\bar{\mathbf{O}}_b$
- Most signing steps remain the same

Blinded UOV

- Makes DPA attacks more difficult
  → Long-term secret $\bar{\mathbf{O}}$ is turned into ephemeral secret $\bar{\mathbf{O}}_b$
- Most signing steps remain the same
- The effect of blinding cancels in **s**
  → **s** is identical to unblinded case

Sampling Random Invertible Matrices

? How to efficiently sample an invertible $\mathbf{R} \xleftarrow{\$} \mathrm{GL}_m(\mathbb{F}_q)$?

Sampling Random Invertible Matrices

? How to efficiently sample an invertible $\mathbf{R} \xleftarrow{\$} \mathrm{GL}_m(\mathbb{F}_q)$?

Iterative construction

- ⊕ Uniform over $\mathrm{GL}_m(\mathbb{F}_q)$
- ⊖ Dedicated datapath
- ⊖ High constant time costs

Sampling Random Invertible Matrices

? How to efficiently sample an invertible $\mathbf{R} \xleftarrow{\$} \mathrm{GL}_m(\mathbb{F}_q)$?

Iterative construction

- ⊕ Uniform over $\mathrm{GL}_m(\mathbb{F}_q)$
- ⊖ Dedicated datapath
- ⊖ High constant time costs

Rejection sampling

- ⊕ Uniform over $\mathrm{GL}_m(\mathbb{F}_q)$
- ⊕ Reuses the Gaussian elimination datapath
- ⊖ $\approx 1.5\times$ signing latency overhead

Sampling Random Invertible Matrices

? How to efficiently sample an invertible $\mathbf{R} \xleftarrow{\$} \mathrm{GL}_m(\mathbb{F}_q)$?

Iterative construction

- ⊕ Uniform over $\mathrm{GL}_m(\mathbb{F}_q)$
- ⊖ Dedicated datapath
- ⊖ High constant time costs

Rejection sampling

- ⊕ Uniform over $\mathrm{GL}_m(\mathbb{F}_q)$
- ⊕ Reuses the Gaussian elimination datapath
- ⊖ $\approx 1.5\times$ signing latency overhead

Can we do better?

?

The LU Approach

$$\mathbf{R} = \mathbf{L} \cdot \mathbf{U} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ l_{1,0} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ l_{m-1,0} & l_{m-1,1} & \cdots & 1 \end{bmatrix} \cdot \begin{bmatrix} u_{0,0} & u_{0,1} & \cdots & u_{0,m-1} \\ 0 & u_{1,1} & \cdots & u_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{m-1,m-1} \end{bmatrix}$$

The LU Approach

$$\mathbf{R} = \mathbf{L} \cdot \mathbf{U} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ l_{1,0} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ l_{m-1,0} & l_{m-1,1} & \cdots & 1 \end{bmatrix} \cdot \begin{bmatrix} u_{0,0} & u_{0,1} & \cdots & u_{0,m-1} \\ 0 & u_{1,1} & \cdots & u_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{m-1,m-1} \end{bmatrix}$$

- **R** is invertible by construction

The LU Approach

$$\mathbf{R} = \mathbf{L} \cdot \mathbf{U} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ l_{1,0} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ l_{m-1,0} & l_{m-1,1} & \cdots & 1 \end{bmatrix} \cdot \begin{bmatrix} u_{0,0} & u_{0,1} & \cdots & u_{0,m-1} \\ 0 & u_{1,1} & \cdots & u_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{m-1,m-1} \end{bmatrix}$$

- **R** is invertible by construction
- Only needs matrix multiplication

The LU Approach

$$\mathbf{R} = \mathbf{L} \cdot \mathbf{U} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ l_{1,0} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ l_{m-1,0} & l_{m-1,1} & \cdots & 1 \end{bmatrix} \cdot \begin{bmatrix} u_{0,0} & u_{0,1} & \cdots & u_{0,m-1} \\ 0 & u_{1,1} & \cdots & u_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{m-1,m-1} \end{bmatrix}$$

- **R** is invertible by construction
- Only needs matrix multiplication

! Not uniformly random over $\mathrm{GL}_m(\mathbb{F}_q)$

The LU Approach: Statistical Analysis

- Slight bias in the diagonal elements of **R**
  - $r_{i,i}$ tend to be non-zero

The LU Approach: Statistical Analysis

- Slight bias in the diagonal elements of **R**
  - $r_{i,i}$ tend to be non-zero

$$\left(P(\mathbf{R}[i,j]=0)\right)_{i,j} = \begin{bmatrix} 0.0000 & 6.2500 & 6.2500 & 6.2500 & 6.2500 \\ 6.2500 & 5.8594 & 6.2500 & 6.2500 & 6.2500 \\ 6.2500 & 6.2500 & 6.2256 & 6.2500 & 6.2500 \\ 6.2500 & 6.2500 & 6.2500 & 6.2485 & 6.2500 \\ 6.2500 & 6.2500 & 6.2500 & 6.2500 & 6.2499 \end{bmatrix}$$

The LU Approach: Statistical Analysis

- Slight bias in the diagonal elements of **R**
  - $r_{i,i}$ tend to be non-zero

$$\big(P(\mathbf{R}[i,j]=0)\big)_{i,j} = \begin{bmatrix} 0.0000 & 6.2500 & 6.2500 & 6.2500 & 6.2500 \\ 6.2500 & 5.8594 & 6.2500 & 6.2500 & 6.2500 \\ 6.2500 & 6.2500 & 6.2256 & 6.2500 & 6.2500 \\ 6.2500 & 6.2500 & 6.2500 & 6.2485 & 6.2500 \\ 6.2500 & 6.2500 & 6.2500 & 6.2500 & 6.2499 \end{bmatrix}$$

  - Effect quickly converges for larger i

The LU Approach: Statistical Analysis

- Slight bias in the diagonal elements of **R**
  - $r_{i,i}$ tend to be non-zero

$$\big(P(\mathbf{R}[i,j]=0)\big)_{i,j} = \begin{bmatrix} 0.0000 & 6.2500 & 6.2500 & 6.2500 & 6.2500 \\ 6.2500 & 5.8594 & 6.2500 & 6.2500 & 6.2500 \\ 6.2500 & 6.2500 & 6.2256 & 6.2500 & 6.2500 \\ 6.2500 & 6.2500 & 6.2500 & 6.2485 & 6.2500 \\ 6.2500 & 6.2500 & 6.2500 & 6.2500 & 6.2499 \end{bmatrix}$$

  - Effect quickly converges for larger i
- More than $2^{15,000}$ **R** matrices possible

Sampling Random Invertible Matrices

? How to efficiently sample an invertible $\mathbf{R} \xleftarrow{\$} \mathrm{GL}_m(\mathbb{F}_q)$?

Iterative construction

- ⊕ Uniform over $\mathrm{GL}_m(\mathbb{F}_q)$
- ⊖ Dedicated datapath
- ⊖ High constant time costs

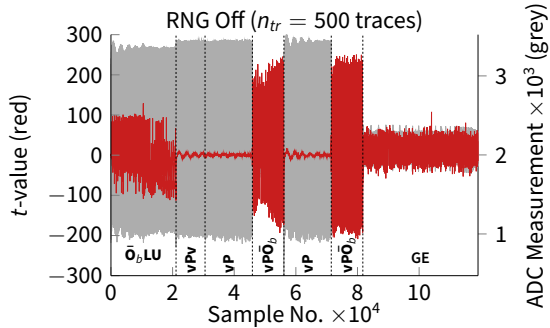
Rejection sampling

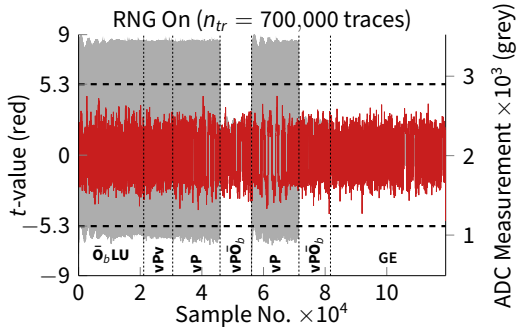
- ⊕ Uniform over $\mathrm{GL}_m(\mathbb{F}_q)$
- ⊕ Reuses the Gaussian elimination datapath
- ⊖ $\approx 1.5\times$ signing latency overhead

LU approach (ours)

- ⊕ Constant time
- ⊕ Only reuses existing datapath
- ⊕ $< 30\%$ signing latency overhead
- ⊘ Not uniform over $\mathrm{GL}_m(\mathbb{F}_q)$

TVLA


RNG Off (n_{tr} = 500 traces)
t-value (red)
ADC Measurement $\times 10^3$ (grey)
Sample No. $\times 10^4$
$\bar{O}_b$LU
vPv
vP
vP$\bar{O}_b$
vP
vP$\bar{O}_b$
GE


RNG On (n_{tr} = 700,000 traces)
t-value (red)
ADC Measurement $\times 10^3$ (grey)
Sample No. $\times 10^4$
$\bar{O}_b$LU
vPv
vP
vP$\bar{O}_b$
vP
vP$\bar{O}_b$
GE

Comparison

	vs. UOV HW [Beu+23]	
Security level	**Signing**	
1	4.7× faster	
3	4.7× faster	
5	5.1× faster	

Comparison

	vs. UOV HW [Beu+23]	
Security level	**Signing**	**Signing** (blinded)
1	4.7× faster	3.9× faster
3	4.7× faster	3.8× faster
5	5.1× faster	4.0× faster

Comparison

	vs. UOV HW [Beu+23]		
Security level	**Signing**	**Signing** (blinded)	**BRAMs**
1	4.7× faster	3.9× faster	2.2× fewer
3	4.7× faster	3.8× faster	8.4× fewer
5	5.1× faster	4.0× faster	16× fewer

Comparison

	vs. UOV HW [Beu+23]			vs. MAYO HW [Hir+24]
Security level	**Signing**	**Signing** (blinded)	**BRAMs**	**ATP**
1	4.7× faster	3.9× faster	2.2× fewer	1.25× worse
3	4.7× faster	3.8× faster	8.4× fewer	1.05× worse
5	5.1× faster	4.0× faster	16× fewer	1.6× better

Conclusion

- Low-memory UOV accelerator
- Lightweight blinding countermeasure
- Concepts also extend to other MQ schemes

ia.cr/2026/1451

Support the NIST selection process with implementation-specific insights.

TU Graz

SCIENCE
PASSION
TECHNOLOGY

Lightweight UOV Accelerator with Oil Space Blinding

Florian Krieger

Institute of Information Security, Graz University of Technology

RIGOLETTO
HIGH PERFORMANCE
RISC-V SOLUTIONS

Bibliography I

[BDK25] Sven Bauer, Fabrizio De Santis, and Kristjane Koleci. **Fault attacks against UOV-based signatures.** 2025 Workshop on Fault Detection and Tolerance in Cryptography (FDTC). 2025, pp. 52–60. DOI: 10.1109/FDTC68360.2025.00014.

[Beu+23] Ward Beullens et al. **Oil and Vinegar: Modern Parameters and Implementations.** **IACR Transactions on Cryptographic Hardware and Embedded Systems** 2023.3 (June 2023), pp. 321–365. DOI: 10.46586/tches.v2023.i3.321-365. URL: https://tches.iacr.org/index.php/TCHES/article/view/10966.

[Beu+25a] Ward Beullens et al. **MAYO Specification Round 2 Version.** NIST Post-Quantum Cryptography Standardization: Additional Digital Signature Schemes, Round 2 Submission. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/mayo-spec-round2-web.pdf. 2025.

[Beu+25b] Ward Beullens et al. **UOV: Unbalanced Oil and Vinegar – Algorithm Specifications and Supporting Documentation, Version 2.0.** NIST Post-Quantum Cryptography Standardization: Additional Digital Signature Schemes, Round 2 Submission. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/uov-spec-round2-web.pdf, Accessed in July 2026. 2025.

Bibliography II

[CGZ26] Jean-Sébastien Coron, François Gérard, and Bowen Zhang. **Masked Solving of Linear Equations System and Application to UOV Signatures.** IACR Transactions on Cryptographic Hardware and Embedded Systems 2026.2 (Apr. 2026), pp. 51–72. DOI: 10.46586/tches.v2026.i2.51-72. URL: https://tches.iacr.org/index.php/TCHES/article/view/12880.

[Hir+24] Florian Hirner et al. **Whipping the Multivariate-based MAYO Signature Scheme using Hardware Platforms.** Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. CCS '24. Salt Lake City, UT, USA: Association for Computing Machinery, 2024, pp. 3421–3435. ISBN: 9798400706363. DOI: 10.1145/3658644.3690258. URL: https://doi.org/10.1145/3658644.3690258.

[JD24] Sönke Jendral and Elena Dubrova. **MAYO Key Recovery by Fixing Vinegar Seeds.** Cryptology ePrint Archive, Paper 2024/1550. https://eprint.iacr.org/2024/1550. 2024. DOI: 10.62056/ab0ljbkrz.

[JD26] Sönke Jendral and Elena Dubrova. **Single-trace Side-Channel Attacks on MAYO Exploiting Leaky Modular Multiplication.** Proceedings of the 2025 1st Workshop on Quantum-Resistant Cryptography and Security. QRSEC '25. Association for Computing Machinery, 2026, pp. 21–30. ISBN: 9798400719080. DOI: 10.1145/3733820.3764682. URL: https://doi.org/10.1145/3733820.3764682.

Bibliography III

[Kun+25] Suparna Kundu et al. **mUOV: Masking the Unbalanced Oil and Vinegar Digital Signature Scheme at First- and Higher-Order.** Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security. CCS '25. Taipei, Taiwan: Association for Computing Machinery, 2025, pp. 1994–2008. ISBN: 9798400715259. DOI: 10.1145/3719027.3765188. URL: https://doi.org/10.1145/3719027.3765188.

[WP26] Thom Wiggers and PQShield. **NIST Signatures Zoo.** online. https://pqshield.github.io/nist-sigs-zoo/, Accessed in July 2026. June 2026.