# UOV Revisited

Jintai Ding

Tsinghua University

*Jintai.Ding@gmail.com*

NIST PQC Seminar, May 2023

# Overview

- Oil Vinegar (OV) and unbalanced Oil Vinegar Signature Schemes

# Families of Post-Quantum Cryptography

- Code-based public key cryptography
  Error correcting codes
- Hash-based public key cryptography
  Hash-tree construction
- Isogeny-based public key cryptography
- Lattice-based public key cryptography
  Shortest and nearest vector problems
- **Multivariate Public Key Cryptography**

# NIST Post-Quantum Cryptography Standardization

- NIST call for proposals of new, post-quantum cryptosystems (Dec 2016) with deadline Nov. 2017.
- Three criteria: Security, Cost, Algorithm and Implementation Characteristics
- Four selected candidate: 1 key exchange (Kyber) three signature (Dilithium, Falcon, SPHINCS+
- One more round of signature submission

# Multivariate Signature schemes

- **Public key**: $\mathcal{P}(x_1, \cdots, x_n) = (p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n))$. Here $p_i$ are multivariate polynomials over a finite field.
- **Private key** A way to compute $\mathcal{P}^{-1}$.
- **Signing a hash of a document:** $(x_1, \cdots, x_n) \in \mathcal{P}^{-1}(y_1, \cdots, y_m)$.
- **Verifying:** $(y_1, \cdots, y_m) \stackrel{?}{=} \mathcal{P}(x_1, \cdots, x_n)$

# Multivariate Signature schemes

- **Public key** $\mathcal{P}(x_1, \cdots, x_n)$ should be a surjective map – n is larger than or equal to m
- The signing and verification should be efficient
- Key sizes should not be too large.

# Theoretical Foundation

- Direct attack is to solve the set of equations:

$$\mathcal{P}(M) = \mathcal{P}(x_1, ..., x_n) = (y'_1, ..., y'_m).$$

# Theoretical Foundation

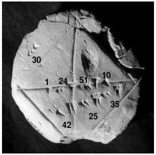
- Direct attack is to solve the set of equations:

$$\mathcal{P}(M) = \mathcal{P}(x_1, ..., x_n) = (y_1', ..., y_m').$$

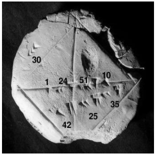
- *- Solving a set of n randomly chosen equations (nonlinear) with n variables is NP-hard, though this does not necessarily ensure the security of the systems.*

# A quick historic overview

- Single variable quadratic equation – Babylonian around 1800 to 1600 BC



- Single variable quadratic equation – Babylonian around 1800 to 1600 BC




- Cubic and quartic equation – around 1500

Tartaglia  Cardano 

# The hardness of the problem

- Single variable case – Galois's work.

  Newton method – continuous system
  Buchberger : Gröbner Basis
  Hironaka: Standard basis
  Berlekamp's algorithm – finite field and low degree

# The hardness of the problem

- Single variable case – Galois's work.

  Newton method – continuous system
  Buchberger : Gröbner Basis
  Hironaka: Standard basis
  Berlekamp's algorithm – finite field and low degree
- Hardness of Multivariate case: NP-hard the generic systems – **Finite field case**
  Numerical solvers – continuous systems

# Quadratic Constructions

- *1) Efficiency considerations lead to mainly quadratic constructions.*

$$p_l(x_1, ..x_n) = \sum_{i,j} \alpha_{lij} x_i x_j + \sum_i \beta_{li} x_i + \gamma_l.$$

# Quadratic Constructions

- *1) Efficiency considerations lead to mainly quadratic constructions.*

$$p_l(x_1, ..x_n) = \sum_{i,j} \alpha_{lij} x_i x_j + \sum_i \beta_{li} x_i + \gamma_l.$$

- *2) Mathematical structure consideration: Any set of high degree polynomial equations can be reduced to a set of quadratic equations.*

$$x_1 x_2 x_3 = 5,$$

is equivalent to

$$\begin{aligned} x_1 x_2 - y &= 0 \\ y x_3 &= 5. \end{aligned}$$

# The view from the history of Mathematics(Diffie in Paris)

- RSA – Number Theory – 18th century mathematics

# The view from the history of Mathematics(Diffie in Paris)

- RSA – Number Theory – 18th century mathematics
- ECC – Theory of Elliptic Curves – 19th century mathematics

# The view from the history of Mathematics(Diffie in Paris)

- RSA – Number Theory – 18th century mathematics
- ECC – Theory of Elliptic Curves – 19th century mathematics
- Multivariate Public key cryptosystem – Algebraic Geometry – 20th century mathematics
  Algebraic Geometry – Theory of Polynomial Rings

# Oil Vinegar Signature Scheme

- Introduced by J. Patarin, 1997
- Inspired by linearization attack to Matsumoto-Imai cryptosystem

# Oil Vinegar Signature Scheme

- Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with $q$ elements and $o, v$ be integers and the number of variables is given by $n = o + v$.
- we define the index sets $V = \{1, \ldots, v\}$ and $O = \{v + 1, \ldots, n\}$. We denote the variables $x_i$ $(i \in V)$ as Vinegar variables, the variables $x_{v+1}, \ldots, x_n$ as Oil variables.

# Oil Vinegar Signature Scheme:**Key Generation**

In order to create a key pair for the Oil and Vinegar signature scheme, Alice chooses

- an affine map $\mathcal{T} : \mathbb{F}^n \rightarrow \mathbb{F}^n$ with randomly chosen coefficients and
- an OV central map $\mathcal{F} = (f^{(1)}, \ldots, f^{(o)}) : \mathbb{F}^n \rightarrow \mathbb{F}^o$. The polynomials $f^{(1)}, \ldots, f^{(o)}$ are of the form

$$f^{(i)} = \sum_{j,k \in V} \alpha_{j,k}^{(i)} x_j x_k + \sum_{j \in V, k \in O} \beta_{j,k}^{(i)} x_j x_k + \sum_{j \in V \cup O} \gamma_j^{(i)} x_j + \delta^{(i)} \ \ (i = 1, \ldots, o)$$

  with coefficients $\alpha_{j,k}^{(i)}$, $\beta_{j,k}^{(i)}$, $\gamma_j^{(i)}$ and $\delta^{(i)}$ randomly chosen from the field $\mathbb{F}$.
- These polynomials are denoted as Oil and Vinegar polynomials.

# Key Generation

A key pair of the Oil and Vinegar signature scheme can be described as follows.

- *Private Key*: The private key of the Oil and Vinegar signature scheme consists of the two maps $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^o$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$.
- *Public Key*: The public key $\mathcal{P}$ of the Oil and Vinegar signature scheme is the composed map $\mathcal{P} = \mathcal{F} \circ \mathcal{T}$ and consists of $o$ quadratic polynomials in $n$ variables.
- In contrast to the standard construction of multivariate cryptography , we do not use a second affine map $\mathcal{S}$ in the construction of the public key of the Oil and Vinegar scheme.

# Signature Generation

To generate a signature $\mathbf{z} \in \mathbb{F}^n$ for a document $d$, one uses a hash function $\mathcal{H} : \{0,1\} \to \mathbb{F}^o$ to compute the hash value $\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}^o$ and performs the following 2 steps.

1. Find a pre-image $\mathbf{y} \in \mathbb{F}^n$ of $\mathbf{w}$ under the central map $\mathcal{F}$.
    - Choose random values for the Vinegar variables $y_1, \ldots, y_v$ and substitute them into the polynomials $f^{(1)}, \ldots, f^{(o)}$.
    - Solve the resulting linear system of $o$ equations in the $o$ Oil variables $y_{v+1}, \ldots, y_n$ by Gaussian Elimination. If the system does not have a solution, choose other values for the Vinegar variables $x_1, \ldots, x_v$ and try again.
2. Compute the signature $\mathbf{z} \in \mathbb{F}^n$ by $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$.

# How to find $\mathcal{F}^{-1}$

- Fix values for vinegar variables $x'_1, \cdots, x'_v$.
- $f_k = \sum a_{i,j,k} x_i x'_j + \sum b_{i,j,k} x'_i x'_j + \sum c_{i,k} x_i + \sum d_{i,k} x'_i + e_k$
- $\mathcal{F}$: Linear system in oil variables $x_1, \cdots, x_o$.

# Signature Verification

- To check, if $\mathbf{z} \in \mathbb{F}^n$ is indeed a valid signature for the document $d$, one uses the hash function $\mathcal{H}$ to compute $\mathbf{w} = \mathcal{H}(d) \in \mathbb{F}^o$ and computes $\mathbf{w}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^o$.
- If $\mathbf{w}' = \mathbf{w}$ holds, the signature $\mathbf{z}$ is accepted, otherwise rejected.

# A different view

- Perturbation of a linear system of equations:
  Starting from a linear system of O variables
  Then add ”noise” variable – Vinegar variable
- Guessing Vinegar variables to eliminate the ”noise” variables.
  LWE — similarity

# Key Sizes and Efficiency

- The size of the UOV public key is

$$\text{size}_{\text{pk UOV}} = o \cdot \frac{(n+1)\cdot(n+2)}{2}$$

  field elements

- The size of the private key

$$\text{size}_{\text{sk UOV}} = \underbrace{n\cdot(n+1)}_{\text{map } \mathcal{T}} + \underbrace{o \cdot \left(\frac{v\cdot(v+1)}{2} + ov + n + 1\right)}_{\text{map } \mathcal{F}}$$

  field elements.

- The signature generation process of UOV only requires the solution of a linear system, which can be efficiently done by Gaussian elimination. Therefore, the UOV signature scheme can be implemented much easily and efficiently.

# The Kipnis-Shamir Attack on balanced Oil and Vinegar and UOV

- To simplify our description, we assume that the components of the UOV central map $\mathcal{F}$ are homogeneous quadratic polynomials and that the transformation $\mathcal{T}$ is linear.
- The UOV public key $\mathcal{P} = \mathcal{F} \circ \mathcal{T}$ is homogeneous quadratic map, too.
- Let $f(\mathbf{x})$ be a central polynomial and we can write $f(\mathbf{x})$ as a quadratic form $f(\mathbf{x}) = \mathbf{x}^T \cdot F \cdot \mathbf{x}$ with an $n \times n$ matrix $F$ of the form

$$F = \begin{pmatrix} F_1 & F_2 \\ F_3 & 0_{v \times v} \end{pmatrix} \tag{1}$$

with all $F_1$, $F_2$, $F_3$ and $0_{v \times v}$ being $v \times v$ matrices with entries in $\mathbb{F}$.

# The Kipnis-Shamir Attack on balanced Oil and Vinegar and UOV

- The matrix $P$ representing the quadratic form of the corresponding public polynomial $p(\mathbf{x})$ is given as

$$P = T^T \cdot F \cdot T,$$

where $T$ is the matrix representing the linear transformation $\mathcal{T}$. For the description of the attack we need the following definition.

# The Kipnis-Shamir Attack on balanced Oil and Vinegar and UOV

For the description of the attack we need the following definition.

**Definition**

We define the Oil subspace of $\mathbb{F}^n$ as

$$\mathcal{O} = \{\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbb{F}^n : x_1 = \ldots = x_v = 0\}.$$

The Vinegar subspace is the set

$$\mathcal{V} = \{\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbb{F}^n : x_{v+1} = \ldots = x_n = 0\}.$$

Note that we have $n = 2v$.

**The key — All the corresponding quadratic forms vanishes on the Oil space!!!**

# The Kipnis-Shamir Attack on balanced Oil and Vinegar and UOV

Then we have

## Lemma

1. *For any* $\mathbf{u}_1, \mathbf{u}_2 \in \mathcal{O}$ *we have*

$$\mathbf{u}_1^T \cdot F \cdot \mathbf{u}_2 = 0.$$

2. *For any* $\mathbf{v}_1, \mathbf{v}_2 \in \mathcal{T}^{-1}(\mathcal{O})$ *we have*

$$\mathbf{v}_1^T \cdot P \cdot \mathbf{v}_2 = 0.$$

## Proof.

1. Since $\mathbf{u}_1, \mathbf{u}_2 \in \mathcal{O}$, we can write $\mathbf{u}_1 = (0, \mathbf{u}_1')^T$ and $u_2 = (0, \mathbf{u}_2')^T$.

$$\begin{aligned}
\mathbf{u}_1^T \cdot F \cdot \mathbf{u}_2 &= (0, \mathbf{u}_1') \cdot \begin{pmatrix} F_1 & F_2 \\ F_3 & 0_v \end{pmatrix} \cdot \begin{pmatrix} 0 \\ \mathbf{u}_2' \end{pmatrix} \\
&= (0, \mathbf{u}_1') \cdot \begin{pmatrix} F_2 \cdot \mathbf{u}_2' \\ 0 \end{pmatrix} = 0.
\end{aligned}$$

2. Let $\mathbf{v}_1', \mathbf{v}_2' \in \mathcal{O}$ such that $\mathbf{v}_1 = \mathcal{T}^{-1}(\mathbf{v}_1')$ and $\mathbf{v}_2 = \mathcal{T}^{-1}(\mathbf{v}_2')$.

$$\begin{aligned}
\mathbf{v}_1^T \cdot P \cdot \mathbf{v}_2 &= (T^{-1} \cdot \mathbf{v}_1')^T \cdot P \cdot (T^{-1} \cdot \mathbf{v}_2') \\
&= \mathbf{v}_1'^T \cdot (T^T)^{-1} \cdot T^T \cdot F \cdot T \cdot T^{-1} \cdot \mathbf{v}_2 \\
&= \mathbf{v}_1'^T \cdot F \cdot \mathbf{v}_2' = 0.
\end{aligned}$$

□

**The attack is to find the pre-image of the Oil subspace under the map $\mathcal{T}$.**

Let $E : \mathbb{F}^n \to \mathbb{F}^n$ be a linear transformation of the form (1). Then we have

## Lemma

*1.* $E(\mathcal{O}) \subset \mathcal{V}$*.*
*2. If E is invertible, we have* $E(\mathcal{O}) = \mathcal{V}$ *and* $E^{-1}(\mathcal{V}) = \mathcal{O}$*.*

## Proof.

1. Let $\mathbf{o} = (0, \mathbf{o}') \in \mathcal{O}$. Then we have

$$\begin{pmatrix} E_1 & E_2 \\ E_3 & 0_{v\times v} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ \mathbf{o}' \end{pmatrix} = \begin{pmatrix} E_2 \cdot \mathbf{o}' \\ 0 \end{pmatrix} \in \mathcal{V}.$$

2. If $E$ is invertible, the image space of $E(\mathcal{O})$ has dimension $\dim(\mathcal{O}) = v$, and therefore we have $E(\mathcal{O}) = \mathcal{V}$ and $E^{-1}(\mathcal{V}) = \mathcal{O}$. $\square$

- We denote by $F^{(i)}$ the matrix associated to the $i$-th component of the central map.
- We set $P^{(i)}$ to be the matrix associated to the $i$-th component of the public key. Note that we have $P^{(i)} = T^T \cdot F^{(i)} \cdot T$ for every $i \in \{1, \ldots, o\}$.
- Let $H_1$ and $H_2$ be linear combinations of the matrices $F^{(i)}$. We can assume that the matrix $H_1$ is invertible.

### Corollary

*The oil subspace $\mathcal{O}$ is a common invariant subspace of all matrices $H = H_1^{-1} \cdot H_2$.*

### Proof.

This follows directly from Lemma 3. $\square$

- Let $W_1$ and $W_2$ be linear combinations of the matrices $P^{(i)}$ ($i = 1, \ldots, o$) and assume that $W_1$ is invertible.
- $W_1$ and $W_2$ can be written as

$$W_1 = T^T \cdot \hat{F}_1 \cdot T \quad \text{and} \quad W_2 = T^T \cdot \hat{F}_2 \cdot T$$

for some matrices $\hat{F}_1$ and $\hat{F}_2$ of the form (1).

**Theorem**

*The space $\mathcal{T}^{-1}(\mathcal{O})$ is a common invariant subspace of all the matrices $W = W_1^{-1} \cdot W_2$.*

## Proof.

$$\begin{aligned} W_1^{-1} \cdot W_2(\mathcal{T}^{-1}(\mathcal{O})) &= (T^T \cdot \hat{F}_1 \cdot T)^{-1} \cdot T^T \cdot \hat{F}_2 \cdot T \cdot T^{-1}(\mathcal{O}) \\ &= T^{-1} \cdot \hat{F}_1^{-1} \cdot (T^T)^{-1} \cdot T^T \cdot \hat{F}_2 \cdot T \cdot T^{-1}(\mathcal{O}) \\ &= T^{-1} \cdot \hat{F}_1^{-1} \cdot \hat{F}_2(\mathcal{O}) \\ &= \mathcal{T}^{-1}(\mathcal{O}). \end{aligned}$$

Here, the last "=" holds due to the fact that $\mathcal{O}$ is an invariant subspace of $\hat{F}_1^{-1} \cdot \hat{F}_2$ (Corollary 4). $\square$

# Finish the attack

After having found $\mathcal{T}^{-1}(\mathcal{O})$, we know the relevant part of the transformation $\mathcal{T}$, which then can be used to compute an equivalent private key $(\tilde{\mathcal{F}}, \tilde{\mathcal{T}})$ which again can be used to generate signatures for arbitrary messages.

- There are two probabilistic polynomial time algorithms for finding the space $\mathcal{T}^{-1}(\mathcal{O})$ (for fields of odd and even characteristic respectively).
- The algorithms take a random linear combination $W_2$ of the matrices $P^{(i)}$ associated to the public key polynomials and multiply it by an invertible matrix $W_1 = \left(\sum_{i=1}^{o} \lambda_i P^{(i)}\right)^{-1}$ to obtain a matrix $W$ of the form $W = W_1^{-1} \cdot W_2$ .
- The algorithms then compute the so called minimal invariant subspaces (an invariant subspace which contains no non-trivial invariant subspaces) of this matrix.
- Each minimal invariant subspace of $W$ may or may not be a subspace of $\mathcal{T}^{-1}(\mathcal{O})$. However, by Lemma 2, we can distinguish between "correct" and "false" subspaces. We continue this process until having found $o$ linear independent basis vectors of $\mathcal{T}^{-1}(\mathcal{O})$.

# The Case of $q$ odd

- In the case of odd characteristic we can write the homogeneous quadratic part of the public polynomials $p^{(1)}(\mathbf{x}), \ldots, p^{(o)}(\mathbf{x})$ as an unique quadratic forms

$$\mathbf{x}^T \cdot \bar{Q}^{(1)} \cdot \mathbf{x}, \ldots, \mathbf{x}^T \cdot \bar{Q}^{(o)} \cdot \mathbf{x}$$

with **symmetric** matrices $\bar{Q}^{(i)}$ $(i = 1, \ldots, o)$ The entries $q_{jk}^{(i)}$ of the matrix $\bar{Q}^{(i)}$ are given as

$$q_{jk}^{(i)} = \begin{cases} \text{MonomialCoefficient}(p^{(i)}, x_j^2) & j = k, \\ \text{MonomialCoefficient}(p^{(i)}, x_j x_k)/2 & j \neq k. \end{cases}$$

# The Case of $q$ odd

- We define $\Omega = \mathrm{span}(\bar{Q}^{(1)}, \ldots, \bar{Q}^{(o)})$. Let $W_1$ and $W_2$ be elements of $\Omega$ ($W_1$ must be invertible) and set $W = W_1^{-1} \cdot W_2$.
- We compute the minimal invariant subspaces of the matrix $W$ (i.e. the invariant subspaces not containing a non-trivial invariant subspace). Each of these minimal invariant subspaces might or might not be a subspace of $\mathcal{T}^{-1}(\mathcal{O})$. This can be checked using the test provided by Lemma 2

# The attack on UOV

- Kipnis, Patarin and Goubin proposed a modified scheme called Unbalanced Oil and Vinegar signature scheme (UOV) by choosing $v > o$.
- Can the attack above applied?
  For $v \gtrsim o$, the attack works essentially the same as described above, only the spaces $\mathcal{O}$ and $\mathcal{V}$ do not have the same dimension any longer.

# The attack on UOV

- Let $E : \mathbb{F}^n \to \mathbb{F}^n$ be a linear transformation of the form

$$E = \begin{pmatrix} E_1 & E_2 \\ E_3 & 0_{o\times o} \end{pmatrix}, \tag{2}$$

where $E_1$ is a $v \times v$ matrix, $E_2$ is a $v \times o$ matrix and $E_3$ is an $o \times v$ matrix with entries randomly chosen from $\mathbb{F}$.

- We have

## Lemma

*1. $E(\mathcal{O})$ is an o-dimensional proper subspace of $\mathcal{V}$.*
*2. If E is invertible, $E^{-1}(\mathcal{V})$ is a v-dimensional subspace of $\mathbb{F}^n$, in which $\mathcal{O}$ is a proper subspace.*

- As in the attack on balanced Oil and Vinegar, we look for the space $\mathcal{T}^{-1}(\mathcal{O})$, which we will denote by $\bar{\mathcal{O}}$.
- Let the matrices $P^{(i)}$ corresponding to the components of the public key:

$$P^{(i)} = T^T \cdot F^{(i)} \cdot T,$$

**Theorem**

*Let $W_1$ and $W_2$ be randomly chosen linear combinations of the matrices $P^{(i)}$ $(i = 1, \ldots, o)$ and let $W_1$ be invertible. Then the probability that the matrix $W_1^{-1} \cdot W_2$ has a nontrivial invariant subspace (which is also a subspace of $\mathcal{T}^{-1}(\mathcal{O})$) is roughly $q^{o-v}$.*

-

- As for the balanced case we can, by computing the minimal invariant subspaces of the matrices $W_1^{-1} \cdot W_2$ and using Lemma 6 to check whether they are subspaces of $\mathcal{T}^{-1}$, recover the essential parts of the UOV linear transformation $\mathcal{T}$. From this, we can then compute an equivalent UOV private key $(\tilde{\mathcal{F}}, \tilde{\mathcal{T}})$ which can be used to sign messages.
- The complexity of the whole process can be estimated by

$$\text{complexity}_{\text{UOV attack}}(q, o, v) = q^{v-o-1} \cdot o^4. \tag{3}$$

# Broken Parameters

- $v = o$
  Defeated by Kipnis and Shamir using invariant subspace (1998).
- $v < o$
  by guessing some variables will be most likely turn into a OV system where $v = o$
- $v >> o$
  Finding a solution is generally easy. When choosing $v \approx \frac{o^2}{2}$, the complexity of a direct attack against the scheme even becomes polynomial

# Usable Parameters

- $v = 2o, 3o$
- Direct attack
- The reconciliation attack
- Collision attacks

# Reconciliation attack

- The reconciliation attack uses the structure of OV systems. Looks for equivalent maps of a special form.
- Complexity becomes solving a system of $o$ quadratic equations in $v$ variables.
  It behaves like a random system.

# Collision attack

- Guesse input and salt, then compare
- Huge memory cost

# Direct attack

- Guesse and solve
- Complexity is just like random polynomials

# UOV for standardization – what is new?

- 1. Introduction of Salt
  Randomize the signing process and signatures
- 2. Provable security
  SSH paper in 2011. Fixing Salt or Vinegar?
  The salt is essential for the security proof: which reduces the UOV problem for any vinegar vector chosen, we can always find a signature by managing Salt
  Our deign does do that? Efficiency ?
  The definition of UOV problem in [SSH11]?
- 3. Compression of the public key and private keys

- Compression of private keys
- Compression of public and private keys.
  Additional cost of signing and verification.

# UOV for standardization – what is new?

Table 1: Recommended parameter sets of UOV.

| | NIST S.L. | $n$ | $m$ | $q$ | \|pk\| (bytes) | \|sk\| (bytes) | \|cpk\| (bytes) | \|csk\| (bytes) | signature (bytes) |
|---|---|---|---|---|---|---|---|---|---|
| uov-Ip | 1 | 112 | 44 | 256 | 278 432 | 237 896 | 43 576 | 48 | 128 |
| uov-Is | 1 | 160 | 64 | 16 | 412 160 | 348 704 | 66 576 | 48 | 96 |
| uov-III | 3 | 184 | 72 | 256 | 1 225 440 | 1 044 320 | 189 232 | 48 | 200 |
| uov-V | 5 | 244 | 96 | 256 | 2 869 440 | 2 436 704 | 446 992 | 48 | 260 |

# UOV for standardization – what is new?

Table 2: Benchmarking results of AVX2 implementations of UOV.

| Schemes | Haswell | | | Skylake | | |
|---|---|---|---|---|---|---|
| | KeyGen | Sign | Verify | KeyGen | Sign | Verify |
| uov-Ip | 3 311 188 | 116 624 | 82 668 | 2 903 434 | 105 324 | 90 336 |
| uov-Ip-pkc | 3 393 872 | | 311 720 | 2 858 724 | | 224 006 |
| uov-Ip-pkc+skc | 3 287 336 | 2 251 440 | | 2 848 774 | 1 876 442 | |
| uov-Is | 4 945 376 | 123 376 | 60 832 | 4 332 050 | 109 314 | 58 274 |
| uov-Is-pkc | 5 002 756 | | 398 596 | 4 376 338 | | 276 520 |
| uov-Is-pkc+skc | 5 448 272 | 3 042 756 | | 4 450 838 | 2 473 254 | |
| uov-III | 22 046 680 | 346 424 | 275 216 | 17 603 360 | 299 316 | 241 588 |
| uov-III-pkc | 22 389 144 | | 1 280 160 | 17 534 058 | | 917 402 |
| uov-III-pkc+skc | 21 779 704 | 11 381 092 | | 17 157 802 | 9 965 110 | |
| uov-V | 58 162 124 | 690 752 | 514 100 | 48 480 444 | 591 812 | 470 886 |
| uov-V-pkc | 57 315 504 | | 2 842 416 | 46 656 796 | | 2 032 992 |
| uov-V-pkc+skc | 57 306 980 | 26 021 784 | | 45 492 216 | 22 992 816 | |
| Dilithium 2† [23] | 97 621* | 281 078* | 108 711* | 70 548 | 194 892 | 72 633 |
| Falcon-512 [30] | 19 189 801* | 792 360* | 103 281* | 26 604 000 | 948 132 | 81 036 |
| SPHINCS+‡ [17] | 1 334 220 | 33 651 546 | 2 150 290 | 1 510 712* | 50 084 397* | 2 254 495* |

† Security level II. ‡ Sphincs+-SHA2-128f-simple. * Data from SUPERCOP [6].

# UOV for standardization – what is new?

- 1. New MinRank attack

$$E = \begin{pmatrix} E_1 & E_2 \\ E_2^T & 0_{o \times o} \end{pmatrix}, \tag{4}$$

  The rows of lower half are in a subspace of dimension $V$.
- 2. Complexity very high

# UOV for standardization – what is new?

- 1. Provable Security?
- 2. A PQ problem with

$$E = n; V = \alpha n^2$$

where $\epsilon < \alpha < 1/2$

# Thanks and Any Questions?

*Jintai.Ding@gmail.com*

*Supported by Taft, NIST, NSF and ABCMint*