

“Preview Writeup”: In anticipation of a package submission to the NIST Threshold Call

Title: DUOV: A Dressing in Advance for Threshold UOV with Pre-signing

Version: Preview Writeup 1.0 (2026-08-07)¹

Team name: MASTER: (MultivariAte ThREshold Signature)

Team members: Elouan Gros, Dayane Horkos, River Moreira Ferreira, Ludovic Perret

Abstract: This document is a preview of DUOV, a submission to the NIST Multi-Party Threshold Cryptography (MPTC) process. It presents a new post-quantum threshold version of the Unbalanced Oil and Vinegar (UOV) multivariate signature scheme of Kipnis, Patarin, and Goubin, enhanced with *pre-signing*. In particular, we use a UOV variant with pre-signature proposed by Shim, Lee, and Koo [SLK22], who noted that most UOV signing is independent of the message. By precomputing the message-independent data into a *pre-signature* (dressing), we can reduce online threshold signing to a sequence of local linear operations followed by a single broadcast, achieving a one-round online phase. We also present an evaluation of DUOV on a real distributed network, deployed across up to 16 geographically distinct AWS regions and connected over the public internet with intercontinental latency. Our experiments show that the one-round online protocol remains fast even under realistic wide-area conditions.

Proposed crypto-systems:

- (I) DUOV: Threshold UOV with Pre-signing (Categories S1 and S4)

Keywords: Threshold Cryptography; NIST Threshold Call; UOV; pre-signing

Document License: Optional license (e.g., CC BY 4.0 International)

¹Preliminary version submitted to NIST-MPTC for review

Preview writeup. This document is provided to NIST for online publication, to foster public awareness and support public discussion within the scope of the NIST First Call for Multi-Party Threshold Schemes [NIST-IR8214C]. This “preview writeup” represents a good-faith plan for a subsequent “package submission”. However, until the deadline for package submission, the team may still modify its own composition and the submission plan, including possible changes to the technical scope, and/or the used techniques or achieved results.

Team members: Elouan Gros ^{i1,a3}, Dayane Horkos ^{i2,a3,a2*}, River Moreira Ferreira ^{i3,a1*}, Ludovic Perret ^{i4,a2,a1}

Open Researcher and Contributor Identifiers (ORCID):

i1 (0009-0004-9395-4619); i2 (0009-0004-9331-9359); i3 (0009-0005-1387-5724); i4 (0009-0005-7453-8705)

Affiliations:

^{a1} LIP6, Sorbonne Université @ Paris, France

^{a2} LRE, EPITA @ Le Kremlin-Bicêtre, France

^{a3} Astran @ Paris, France

Associateship clarifications:

* Ph.D. student (non-employee).

Main contacts:

- **Team mailing list:** contact-duov@astran.ai
- **Primary technical contact person:** Ludovic Perret, ludovic.perret@epita.fr
- **Secondary contact person:** Elouan Gros, elouan.gros@astran.ai

Produced by humans. The team hereby confirms that the content in this preview writeup: (i) was produced by the team members, and (ii) was not produced by generative artificial intelligence (AI), with the possible exception of AI-proposed grammar improvements, minor integrated suggestions, or some well-identified and short localized portions of auxiliary content (e.g., some illustration); and (iii) was proofread by the team members.

1. Introduction

The reasons to consider UOV [KPG99] for thresholdization are twofold. First, it is widely considered the most interesting multivariate scheme for practical deployment, as illustrated by the fact that four UOV-based schemes, modern UOV, Mayo, QR-UOV and SNOVA [BCHKPSY23; Beu21; FIKT21; WTKC22], have been selected in May 2026 for the third round of the ongoing NIST additional post-quantum signature process [Nat22]. Secondly, as shown by Cozzo and Smart [CS19], threshold UOV is relatively simple compared to other post-quantum signature schemes, as it reduces to securely solving a shared linear system.

The main starting point of DUOV is a variant of UOV with a pre-signature, proposed by Shim, Lee, and Koo [SLK22]. They observed that the *entire* message-independent computation of a UOV signature can be moved into a reusable, secret-shared *pre-signature* (Section 3), computed once in advance, as is classically done for pre-signing in threshold ECDSA [GS21]. Online threshold signing for DUOV then reduces to a sequence of purely local linear operations on shares, followed by a *single* MPC broadcast. The offline part can then be carried out independently and requires securely inverting a linear system, which can be done with state-of-the-art techniques, e.g. [CS19; NIS24]. We note that vinaigrette [NIS24], the first threshold UOV-based submission to the MPTC process, also extends the offline/online pre-computing idea to threshold UOV, and the differences are discussed in Section 7.

We also evaluate DUOV on a genuine wide-area network rather than a local network emulation: we implement DUOV in Common Lisp and deploy it across up to 16 geographically distinct AWS regions, connected over the public internet with its intercontinental latency. For networks of 2 to 16 parties and 1000 signatures per configuration. Our results show that online signing time closely tracks the maximum measured pairwise latency among participants, confirming that the one-round protocol remains fast under realistic wide-area conditions, with network delay, rather than computation, dominating its cost.

2. Specification

Organization. The specification will be organized in four independent parts. Part I recalls UOV its trapdoor, the pre-signing version, together with the shared linear-system-solving building blocks. Part II is the core technical contribution: the decomposition of a UOV signature into a message-independent *pre-signature* and a message-dependent *finishing* step, and the two associated MPC protocols, PreSign and SignFromPreSig. Part III will discuss the security, including algorithmic hardness of the chosen parameters and security proofs of MPC protocols used. Finally, Part IV will describe the distributed implementation and its evaluation on a genuine wide-area network.

System model. We consider N parties holding an additive secret sharing $[\cdot]$ of a UOV secret key, communicating over a synchronous network in which the adversary may observe, delay, or drop messages at will. The threshold structure is presently an (N, N) /dishonest-majority one and we plan to discuss (t, N) profiles in the full specification. The pre-signing split introduces two

sub-phases: an *offline pre-signing* phase, run before the message is known, which samples a shared vinegar vector, inverts the corresponding coefficient matrix using the shared-linear-system solver, and stores the resulting pre-signature; and a lightweight *online* phase, run once the message is known, that consumes exactly one pre-signature.

Security. DUOV inherits its security from the components it builds on. In the offline phase, PreSig will probably reuse a state-of-the-art shared-linear-system machinery such as in [NIS24; ABV26]. In the online phase, once a pre-signature is fixed, SignFromPreSig performs only local linear operations on shares followed by a single opening of the signature itself – a public value – so this step adds no leakage beyond that of a classical, single-party UOV signature. The current prototype targets passive security; the full specification will additionally discuss active security (e.g., via authenticated/SPDZ-style shares and a MAC-check protocol). Note that, as mentioned in [SLK22], a pre-signature must never be reused across two messages, as is standard for nonce-like threshold signatures.

3. High-Level Description of the Scheme

DUOV lifts a UOV version with pre-signature proposed by [SLK22]. We describe this version in Section 3.2, which requires recalling well-known results about UOV in Section 3.1.

3.1. Unbalanced Oil and Vinegar

MPKC [DPS20] refers to public-key schemes whose security reduces to the NP-hardness [GJ79] of solving systems of multivariate quadratic equations (MQ problem). The Matsumoto–Imai (MI) framework [MI88] gives a generic construction for such schemes from a structured non-linear inner map $\mathbf{f} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ that is easy to invert, composed with two secret invertible linear maps $\mathbf{S}$ and $\mathbf{U}$, applied to the input and output respectively, that hide this structure. The public key is then $\mathcal{P} = \mathbf{U} \circ \mathbf{f} \circ \mathbf{S}$, whose inversion is hard without knowledge of $\mathbf{S}$, $\mathbf{U}$, and the structure of $\mathbf{f}$.

Unbalanced Oil and Vinegar (UOV), proposed by A. Kipnis, L. Goubin and J. Patarin [KPG99], is a particular instantiation of the MI framework where the inner map $\mathbf{f} = (f_1, \dots, f_m) \in \mathbb{F}_q[x_1, \dots, x_n]^m$ becomes linear once a particular subset of variables, the so-called vinegar variables, are fixed. The inner non-linear system can thus be solved efficiently by randomly sampling the vinegar variables and then solving the resulting linear system for the remaining unknowns, the so-called oil variables. The public key $\mathcal{P}$ is obtained as in the MI framework, with the outer linear map $\mathbf{U}$ taken to be the identity.

In [Beu21], the author restated this traditional presentation of the UOV trapdoor in an equivalent form by introducing the vanishing subspace of a multivariate quadratic map. We shall say that a linear subspace $\mathcal{O}$ of $\mathbb{F}_q^n$ is a vanishing subspace of $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ if :

$$\forall \mathbf{o} \in \mathcal{O}, \mathcal{P}(\mathbf{o}) = \mathbf{0}_m. \quad (1)$$

In this setting, the public key remains the multivariate quadratic map $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$, but the corresponding secret key is now a vanishing subspace $\mathcal{O} \subset \mathbb{F}_q^n$ of dimension m (the oil space).

3.1.1. Key Generation

To generate the key pair $(\mathcal{P}, \mathcal{O})$ with $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ and with $\mathcal{O} \subset \mathbb{F}_q^n$ a vanishing subspace of dimension m (Definition 1), we first generate a random basis of $\mathcal{O}$ in systematic form, namely a basis of the form:

$$\begin{pmatrix} \mathbf{O}_{v \times m} \\ \mathbf{1}_m \end{pmatrix} \in \mathbb{F}_q^{n \times m}, \text{ where } \mathbf{O}_{v \times m} \in \mathbb{F}_q^{v \times m} \text{ and } v = n - m. \quad (2)$$

The components $p_1, \dots, p_m \in \mathbb{F}_q[x_1, \dots, x_n]$ of $\mathcal{P}$ are then constructed as:

$$p_i(\mathbf{x}) = \mathbf{x}^\top \mathbf{Q}_i \mathbf{x}, \quad \mathbf{Q}_i = \begin{pmatrix} \mathbf{Q}_i^{(1)} & \mathbf{Q}_i^{(2)} \\ \mathbf{0}_{m \times v} & \mathbf{Q}_i^{(3)} \end{pmatrix} \in \mathbb{F}_q^{n \times n}, \quad 1 \leq i \leq m, \quad (3)$$

with $\mathbf{x} = (x_1, \dots, x_n)$, and where $\mathbf{Q}_i^{(1)} \in \mathbb{F}_q^{v \times v}$ is upper triangular, $\mathbf{Q}_i^{(2)} \in \mathbb{F}_q^{v \times m}$ is arbitrary, and $\mathbf{Q}_i^{(3)} = \text{Upper}(-\mathbf{O}^\top \mathbf{Q}_i^{(1)} \mathbf{O} - \mathbf{O}^\top \mathbf{Q}_i^{(2)}) \in \mathbb{F}_q^{m \times m}$. The subspace $\mathcal{O}$ generated as in (2) is then a vanishing subspace of the map defined by (3).

3.1.2. Signature Generation and Verification

The UOV signature for a message $\text{msg} \in \{0, 1\}^*$ is given by a vector $\mathbf{s} \in \mathbb{F}_q^n$ and a fixed-length bit string $\text{salt} \in \{0, 1\}^{\text{len}_{\text{salt}}}$ such that

$$\mathcal{P}(\mathbf{s}) = \mathcal{H}(\text{msg} || \text{salt}),$$

where $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{F}_q^m$ is a hash function.

The UOV trapdoor is based on the result below, demonstrating that the knowledge of the vanishing subspace allows one to compute a valid signature by solving a linear system.

Lemma 1. *Let $v = n - m$, $\mathbf{O} \in \mathbb{F}_q^{v \times m}$ be a systematic basis of a vanishing subspace of dimension m as in (2), and $\mathbf{Q}_1, \dots, \mathbf{Q}_m \in \mathbb{F}_q^{n \times n}$ be the matrices defining $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ as in (3). Let $\mathbf{v} \in \mathbb{F}_q^v$, $\mathbf{x} \in \mathbb{F}_q^m$, $\bar{\mathbf{v}} = \begin{pmatrix} \mathbf{v} \\ \mathbf{0}_m \end{pmatrix} \in \mathbb{F}_q^n$, and $\mathbf{o} = \begin{pmatrix} \mathbf{O} \\ \mathbf{1}_m \end{pmatrix} \mathbf{x} \in \mathbb{F}_q^n$. Then, for all $\mathbf{h} = (h_1, \dots, h_m) \in \mathbb{F}_q^m$:*

$$\mathcal{P}(\bar{\mathbf{v}} + \mathbf{o}) = \mathbf{h} \quad \text{iff} \quad \mathbf{A}_{\mathbf{v}} \mathbf{x} = \mathbf{b},$$

where $\mathbf{A}_{\mathbf{v}} := \begin{pmatrix} \mathbf{A}_1 \\ \vdots \\ \mathbf{A}_m \end{pmatrix}$ and $\mathbf{b}^\top = (h_1 - \mathbf{v}^\top \mathbf{Q}_1^{(1)} \mathbf{v}, \dots, h_m - \mathbf{v}^\top \mathbf{Q}_m^{(1)} \mathbf{v})$, with each row vector

$\mathbf{A}_i = \mathbf{v}^\top \mathbf{S}_i \in \mathbb{F}_q^{1 \times m}$, where $\mathbf{S}_i := (\mathbf{Q}_i^{(1)} + \mathbf{Q}_i^{(1)\top}) \mathbf{O} + \mathbf{Q}_i^{(2)} \in \mathbb{F}_q^{v \times m}$, for each $1 \leq i \leq m$,

To generate a signature of $\text{msg} \in \{0, 1\}^*$, the signer samples a random pair $(\mathbf{v}, \text{salt}) \in \mathbb{F}_q^v \times \{0, 1\}^{\text{len}_{\text{salt}}}$ and solves the linear system of Lemma 1 with $\mathbf{h} = \mathcal{H}(\text{msg}||\text{salt}) \in \mathbb{F}_q^m$. If the system has no solution, the signer resamples the vinegar vector $\mathbf{v}$ (and a fresh salt) and retries until a solution exists. Finally, the signer recovers the signature $\mathbf{s} = \bar{\mathbf{v}} + \mathbf{o} \in \mathbb{F}_q^n$, with $\bar{\mathbf{v}}, \mathbf{o}$ as in Lemma 1.

3.2. UOV with Pre-Signing (Single-Party)

As discussed by [SLK22], one can do most operations in an offline phase. Let $(\mathcal{P}, \mathcal{O})$ be a UOV key pair, with $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ the public map defined by quadratic polynomials $p_1, \dots, p_m \in \mathbb{F}_q[x_1, \dots, x_n]$, $\mathcal{O} \subset \mathbb{F}_q^n$ a vanishing subspace of $\mathcal{P}$ of dimension m , and $\mathbf{Q}_1, \dots, \mathbf{Q}_m \in \mathbb{F}_q^{n \times n}$ the matrices defining $\mathcal{P}$ as in (3). Let also $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{F}_q^m$ be a hash function and $\mathbf{O}_{v \times m} \in \mathbb{F}_q^{v \times m}$ be the matrix defining a systematic basis of $\mathcal{O}$:

$$\begin{pmatrix} \mathbf{O}_{v \times m} \\ \mathbf{1}_m \end{pmatrix} \in \mathbb{F}_q^{n \times m}, \text{ with } v = n - m.$$

According to Lemma 1, a UOV signature $(\boldsymbol{\sigma}, \text{salt}) \in \mathbb{F}_q^n \times \{0, 1\}^{\text{len}_{\text{salt}}}$ of a message $\text{msg} \in \{0, 1\}^*$, with $\mathbf{h} = (h_1, \dots, h_m) = \mathcal{H}(\text{msg}||\text{salt}) \in \mathbb{F}_q^m$, satisfies $\mathcal{P}(\mathbf{s}) = \mathcal{H}(\text{msg}||\text{salt})$ and has the form:

$$\boldsymbol{\sigma} = \begin{pmatrix} \mathbf{v} + \mathbf{O}\mathbf{x} \\ \mathbf{x} \end{pmatrix}, \quad (4)$$

where $\mathbf{v} \in \mathbb{F}_q^v$ is sampled at random and $\mathbf{x} \in \mathbb{F}_q^m$ solves the linear system

$$\mathbf{A}_{\mathbf{v}}\mathbf{x} = \mathbf{b}, \quad (5)$$

of Lemma 1, instantiated with the sampled $\mathbf{v}$ and $\mathbf{h}$.

The key observation is that the right-hand side $\mathbf{b}$ can be split into a message-independent part and a message-dependent part:

$$\mathbf{b} = \mathbf{b}_{\mathbf{v}} + \mathbf{h}, \quad (6)$$

with $\mathbf{b}_{\mathbf{v}}^\top = (-\mathbf{v}^\top \mathbf{Q}_1^{(1)} \mathbf{v}, \dots, -\mathbf{v}^\top \mathbf{Q}_m^{(1)} \mathbf{v}) \in \mathbb{F}_q^m$.

Note that the vinegar vector $\mathbf{v}$ is sampled randomly and independently of the message. The usual implementation of UOV generates this vector on demand, retrying until the matrix $\mathbf{A}_{\mathbf{v}}$ of the linear system (5) is invertible. Instead, we can pre-sample one or several vinegar vectors $\mathbf{v} \in \mathbb{F}_q^v$ such that $\mathbf{A}_{\mathbf{v}}$ is invertible, and store the inverse $\mathbf{A}_{\mathbf{v}}^{-1}$ ahead of time. The solution $\mathbf{x}$ of the linear system (5) is then decomposed as

$$\mathbf{x} = \mathbf{x}_{\mathbf{v}} + \mathbf{A}_{\mathbf{v}}^{-1} \mathbf{h}, \text{ with } \mathbf{x}_{\mathbf{v}} = \mathbf{A}_{\mathbf{v}}^{-1} \mathbf{b}_{\mathbf{v}}. \quad (7)$$

Substituting (7) into (4), a UOV signature $\boldsymbol{\sigma}$ can be decomposed as $\boldsymbol{\sigma} = \boldsymbol{\sigma}_{\text{pre}} + \boldsymbol{\sigma}_{\text{post}}$, where

$$\boldsymbol{\sigma}_{\text{pre}} = \begin{pmatrix} \mathbf{v} + \mathbf{O}\mathbf{A}_{\mathbf{v}}^{-1} \mathbf{b}_{\mathbf{v}} \\ \mathbf{A}_{\mathbf{v}}^{-1} \mathbf{b}_{\mathbf{v}} \end{pmatrix}, \quad \boldsymbol{\sigma}_{\text{post}} = \begin{pmatrix} \mathbf{O}\mathbf{A}_{\mathbf{v}}^{-1} \mathbf{h} \\ \mathbf{A}_{\mathbf{v}}^{-1} \mathbf{h} \end{pmatrix}.$$

Here σ_{pre} depends only on $\mathbf{v}$ and is independent of the message, while σ_{post} is a linear function of the digest $\mathbf{h}$.

Hence, when $\mathbf{x}_{\mathbf{v}}$, $\mathbf{A}_{\mathbf{v}}^{-1}$, and $\mathbf{O}\mathbf{A}_{\mathbf{v}}^{-1}$ are all secret-shared among the N signing parties (PreSign protocol), completing it into a signature online can be done combining shares linearly (SignFromPreSig protocol).

4. Open-Source Implementation

Code structure. The current prototype is implemented in Common Lisp, chosen for its malleability, its debugging tools, and the balance it offers between high-level constructs and low-level performance control. It depends on `tiny-AES-c` (exposed through a CFFI foreign-function wrapper) for seed expansion, and on the Common Lisp libraries `CFFI`, `USOCKET` (network programming), `Bordeaux-Threads` (multithreading), `Alexandria`, and `nibbles` (reading values from octet-addressed data), managed through `Quicklisp`. It is compiled and run with `SBCL`.

Code progress and availability. The prototype currently implements and benchmarks the online signing step of SignFromPreSig (from a precomputed, secret-shared pre-signature) for MPC networks of 2 to 16 parties using additive secret sharing over $\mathbb{F}_{2^8}$, instantiated with the UOV-lp parameter set [BCHKPSY23]. It does not yet include a public repository; we plan to publish the DUOV core code, under a permissive open-source license, ahead of the package-submission deadline.

Implementation of the networking model. We tested DUOV on a locally emulated network where all participants are processes on a single machine, communicating via network sockets on the loopback interface. For our evaluation (Section 5), the 16 participants ran on distinct AWS EC2 instances located in different geographic regions, connected over the public internet through a WireGuard VPN for ease of addressing and confidentiality of the communication channel against external eavesdroppers.

5. Experimental Performance Evaluation

Performance. Figure 1 reports the mean wall-clock time to sign from a pre-signature for the UOV-lp parameter set, over 1000 signatures per party count. We compare a *control* environment, where all $N \in \{2, \dots, 16\}$ parties are emulated on a single 32-core machine (Scaleway POP2-HC-32C-64G, communicating over loopback), against a *test* environment where each party runs on its own AWS `t3.small` instance in a distinct region. Signing time grows mildly with N in the control environment, matching the fact that opening the final signature share requires an all-to-all broadcast. In the test environment, signing time is markedly higher and tracks the maximum pairwise latency among the currently-benchmarked participants (also plotted in Figure 1) rather than the number of parties: since the MPC broadcast for UOV-lp carries only $\log_2 |\mathbb{F}_{2^8}^{112}| = 896$ bits,

easily fitting one network frame, this confirms that intercontinental latency – not local computation – is the dominant cost of the online phase. This is, to our knowledge, the first demonstration that a one-round threshold multivariate signing protocol remains practical under genuine wide-area network conditions.

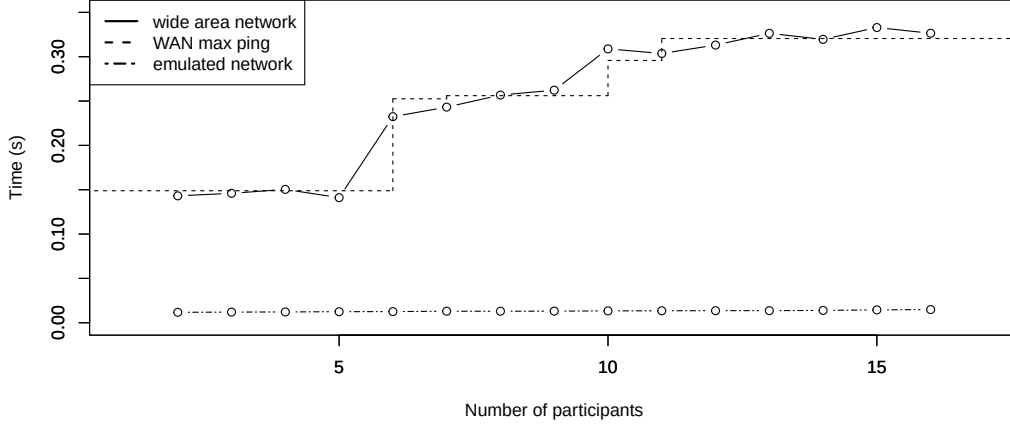


Figure 1: Mean time to sign UOV-lp from a pre-signature, by number of participants, in the control (local) and test (wide-area) environments, together with the maximum measured latency between participants in the test environment.

Platform. Our test environment (16 AWS `t3.small` instances, 2 virtual CPUs and 2 GB of RAM each, one per targeted region) intentionally departs from the single-computer baseline platform (16 cores, 64 GB of RAM) mentioned in the compilation of public comments [PubComs2PD] on the 2pd, since our goal is precisely to measure the effect of realistic wide-area latency rather than raw single-machine throughput. For comparability with other submissions, we plan to also report, in the package submission, results obtained by emulating DUOV on the NIST baseline platform itself.

6. Licensing, Patent Claims, and Funding

We intend to release the core code of DUOV under a permissive open-source license (e.g., Apache 2.0 or GPL licenses). Its external dependencies (Section 4) are themselves distributed under permissive open-source licenses. To the best of the team’s knowledge, no member holds, has applied for, or is aware of, patent claims that would cover the contents of this submission.

7. Comparison with Other Submissions

As discussed, pre-computing the message-independent part of UOV signing was first exploited in the single-party setting in [SLK22]. DUOV extends this idea to the multi-party setting. Concurrently and independently of our work ², vinaigrette [NIS24; ABCN26] bring the offline/online pre-computing idea to threshold UOV: they pre-calculate the matrix inverse and move salt generation offline. In comparison to vinaigrette, our variant absorbs the vinegar vector entirely, allowing a linear operation performed online in vinaigrette to be done offline in DUOV.

²DUOV was first presented in the master thesis of the third author in 2023 and presented at a French conference (<https://indico.math.cnrs.fr/event/9364/attachments/3984/6419/2023/ProgrammeJC2.pdf>) the same year. A paper describing DUOV is also under submission

References

- [ABCN26] Diego F. Aranha, Giacomo Borin, Sofia Celi, and Guilhem Niot. *Optimizing and Implementing Threshold MAYO*. Cryptology ePrint Archive, Paper 2026/710. 2026. URL: <https://eprint.iacr.org/2026/710>.
- [ABV26] Paco Azevedo-Oliveira, Jordan Beraud, and Pierre Varjabedian. *Shared and leakage free MAYO*. Cryptology ePrint Archive, Paper 2026/189. 2026. URL: <https://eprint.iacr.org/2026/189>.
- [BCHKPSY23] Ward Beullens, Ming-Shing Chen, Shih-Hao Hung, Matthias J. Kannwischer, Bo-Yuan Peng, Cheng-Jhih Shih, and Bo-Yin Yang. “Oil and Vinegar: Modern Parameters and Implementations”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.3 (2023), pp. 321–365. DOI: [10.46586/TCHES.V2023.I3.321-365](https://doi.org/10.46586/tches.v2023.i3.321-365). URL: <https://doi.org/10.46586/tches.v2023.i3.321-365>.
- [Beu21] Ward Beullens. “MAYO: Practical Post-quantum Signatures from Oil-and-Vinegar Maps”. In: *Selected Areas in Cryptography - 28th International Conference, SAC 2021, Virtual Event, September 29 - October 1, 2021, Revised Selected Papers*. Ed. by Riham AlTawy and Andreas Hülsing. Vol. 13203. Lecture Notes in Computer Science. Springer, 2021, pp. 355–376. DOI: [10.1007/978-3-030-99277-4_17](https://doi.org/10.1007/978-3-030-99277-4_17). URL: https://doi.org/10.1007/978-3-030-99277-4_17.
- [CS19] Daniele Cozzo and Nigel P. Smart. “Sharing the LUOV: Threshold Post-quantum Signatures”. In: *Cryptography and Coding - 17th IMA International Conference, IMACC 2019, Oxford, UK, December 16-18, 2019, Proceedings*. Ed. by Martin Albrecht. Vol. 11929. Lecture Notes in Computer Science. Springer, 2019, pp. 128–153. DOI: [10.1007/978-3-030-35199-1_7](https://doi.org/10.1007/978-3-030-35199-1_7). URL: https://doi.org/10.1007/978-3-030-35199-1_7.
- [DPS20] Jintai Ding, Albrecht Petzoldt, and Dieter S. Schmidt. *Multivariate public key cryptosystems*. eng. Second edition. Advances in information security volume 80. New York, NY: Springer, 2020.
- [FIKT21] Hiroki Furue, Yasuhiko Ikematsu, Yutaro Kiyomura, and Tsuyoshi Takagi. “A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV”. In: *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part IV*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13093. Lecture Notes in Computer Science. Springer, 2021, pp. 187–217. DOI: [10.1007/978-3-030-92068-5_7](https://doi.org/10.1007/978-3-030-92068-5_7). URL: https://doi.org/10.1007/978-3-030-92068-5_7.
- [GJ79] M. R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman, 1979.
- [GS21] Jens Groth and Victor Shoup. *On the security of ECDSA with additive key derivation and presignatures*. Cryptology ePrint Archive, Paper 2021/1330. 2021. URL: <https://eprint.iacr.org/2021/1330>.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. “Unbalanced Oil and Vinegar Signature Schemes”. In: *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*. Ed. by Jacques Stern. Vol. 1592. Lecture Notes in Computer Science. Springer, 1999, pp. 206–222. DOI: [10.1007/3-540-48910-X_15](https://doi.org/10.1007/3-540-48910-X_15). URL: https://doi.org/10.1007/3-540-48910-X_15.

[MI88] Tsutomu Matsumoto and Hideki Imai. “Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption”. In: *Advances in Cryptology - EUROCRYPT '88, Workshop on the Theory and Application of Cryptographic Techniques, Davos, Switzerland, May 25-27, 1988, Proceedings*. Ed. by Christoph G. Günther. Vol. 330. Lecture Notes in Computer Science. Springer, 1988, pp. 419–453. DOI: [10.1007/3-540-45961-8_39](https://doi.org/10.1007/3-540-45961-8_39). URL: https://doi.org/10.1007/3-540-45961-8_39.

[Nat22] National Institute of Standards and Technology (NIST). *Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process*. <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf>. Issued pursuant to the Federal Information Security Management Act (FISMA) of 2002, Public Law 107–347. Submission deadline: June 1, 2023. Accessed: 2026-02-11. September 2022.

[NIS24] NIST. *An MPC Approach for Threshold UOV and MAYO*. <https://csrc.nist.gov/csrc/media/Projects/threshold-cryptography/documents/TCall-1/Vinaigrette-PW01.pdf>. Accessed: 2026-02-19. 2024. URL: <https://csrc.nist.gov/csrc/media/Projects/threshold-cryptography/documents/TCall-1/Vinaigrette-PW01.pdf>.

[SLK22] Kyung-Ah Shim, Sangyub Lee, and Namhun Koo. “Efficient Implementations of Rainbow and UOV using AVX2”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.1 (2022), pp. 245–269. DOI: [10.46586/TCHES.V2022.I1.245-269](https://doi.org/10.46586/TCHES.V2022.I1.245-269). URL: <https://doi.org/10.46586/tches.v2022.i1.245-269>.

[WTKC22] Lih-Chung Wang, Po-En Tseng, Yen-Liang Kuan, and Chun-Yen Chou. “A Simple Non-commutative UOV Scheme”. In: *IACR Cryptol. ePrint Arch.* (2022), p. 1742. URL: <https://eprint.iacr.org/2022/1742>.

[NIST-IR8214C] Luís T. A. N. Brandão and René Peralta. *NIST First Call for Multi-Party Threshold Schemes*. (National Institute of Standards and Technology) NIST Internal Report (NISTIR) 8214C. 2026. DOI: [10.6028/NIST.IR.8214C](https://doi.org/10.6028/NIST.IR.8214C).

[PubComs2PD] NIST-MPTC. *Compilation of Public Comments on NIST IR 8214C 2pd*. National Institute of Standards and Technology (NIST), Multi-Party Threshold Cryptography. June 2025. URL: <https://csrc.nist.gov/files/pubs/ir/8214/c/2pd/docs/nistir-8214c-2pd-public-feedback.pdf>.