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

Elouan Gros Dayane Horkos River Moreira Ferreira Ludovic Perret

Astran – LRE, EPITA – LIP6, CNRS, Sorbonne Université

2026-10-06 @ NIST TCPT3











Context

Two NIST processes

- Multi-Party Threshold Cryptography (MPTC)
  - Threshold KEMs, signatures, FHE, ZK, gadgets
- Additional PQ signatures – third round (May 2026)
  - Multivariate-based
    - random MQ equations: `MQOM`
    - Unbalanced Oil and Vinegar (UOV-like) schemes: UOV, `MAYO`, `QR-UOV`, `SNOVA`

National Institute of Standards and Technology

Threshold Digital Signature Scheme (TDSS) [Desmedt, Frankel, CRYPTO '91]

N parties jointly hold the signing key; **no single party ever reconstructs it**.

- $\mathsf{DKG}(1^\lambda) \to (\mathsf{pk}, [\mathsf{sk}])$ $\quad \mathsf{ThrSign}([\mathsf{sk}], \mathsf{msg}) \to \sigma$ $\quad \mathsf{Verify}(\mathsf{pk}, \mathsf{msg}, \sigma) \to \{0,1\}$

Context

Two NIST processes

- Multi-Party Threshold Cryptography (MPTC)
  - Threshold KEMs, signatures, FHE, ZK, gadgets
- Additional PQ signatures – third round (May 2026)
  - Multivariate-based
    - random MQ equations: MQOM
    - Unbalanced Oil and Vinegar (UOV-like) schemes: UOV, MAYO, QR-UOV, SNOVA

NIST
National Institute of Standards and Technology

Threshold Digital Signature Scheme (TDSS) [Desmedt, Frankel, CRYPTO '91]

N parties jointly hold the signing key; **no single party ever reconstructs it**.

- $\mathsf{DKG}(1^\lambda) \to (\mathsf{pk}, [\mathsf{sk}])$ $\quad \mathsf{ThrSign}([\mathsf{sk}], \mathsf{msg}) \to \boldsymbol{\sigma}$ $\quad \mathsf{Verify}(\mathsf{pk}, \mathsf{msg}, \boldsymbol{\sigma}) \to \{0, 1\}$

Threshold Signatures: from Classical to Post-Quantum

Classical threshold signatures

- Efficient threshold RSA, ECDSA, Schnorr (FROST)
- **pre-signing** moves all message-independent work offline
  e.g. ECDSA presignatures [Groth, Shoup, 2021]

UOV is natural post-quantum TDSS candidate [Cozzo, Smart, IMACC 2019]

- Signing $\Leftrightarrow$ secure solving of a shared linear system
- pre-signing scheme [Shim, Lee, Koo, 2021]
- `vinaigrette`: threshold UOV and MAYO, first UOV-based MPTC submission
  [Celi, Escudero, Niot, 2024; Aranha et al., MPTS 2026]

Can pre-signing be brought to threshold UOV?

Does it remain fast over the public internet?

Threshold Signatures: from Classical to Post-Quantum

Classical threshold signatures

- Efficient threshold RSA, ECDSA, Schnorr (FROST)
- **pre-signing** moves all message-independent work offline
  e.g. ECDSA presignatures [Groth, Shoup, 2021]

UOV is natural post-quantum TDSS candidate [Cozzo, Smart, IMACC 2019]

- Signing $\Leftrightarrow$ secure solving of a shared linear system
- pre-signing scheme [Shim, Lee, Koo, 2021]
- `vinaigrette`: threshold UOV and MAYO, first UOV-based MPTC submission
  [Celi, Escudero, Niot, 2024; Aranha et al., MPTS 2026]

Can pre-signing be brought to threshold UOV?

Does it remain fast over the public internet?

Threshold Signatures: from Classical to Post-Quantum

Classical threshold signatures

- Efficient threshold RSA, ECDSA, Schnorr (FROST)
- **pre-signing** moves all message-independent work offline
  e.g. ECDSA presignatures [Groth, Shoup, 2021]

UOV is natural post-quantum TDSS candidate [Cozzo, Smart, IMACC 2019]

- Signing $\Leftrightarrow$ secure solving of a shared linear system
- pre-signing scheme [Shim, Lee, Koo, 2021]
- `vinaigrette`: threshold UOV and MAYO, first UOV-based MPTC submission
  [Celi, Escudero, Niot, 2024; Aranha et al., MPTS 2026]

Can pre-signing be brought to threshold UOV?

Does it remain fast over the public internet?

Contributions

DUOV: threshold UOV with pre-signing

- Message-independent part (incl. **vinegar vector**) absorbed in a secret-shared **pre-signature** (the "dressing")
- Online signing: **local linear operations + one broadcast**
- Agnostic to the shared-linear-system solver used offline
- Compatible with any secret sharing scheme on Fields

First evaluation on a genuine wide-area network

- Practical implementation, 2 to 16 parties
- 16 AWS instances in **distinct geographic regions**, public internet
- To appear in ACM Conference on Post-Quantum and Quantum-based Security

Contributions

DUOV: threshold UOV with pre-signing

- Message-independent part (incl. **vinegar vector**) absorbed in a secret-shared **pre-signature** (the "dressing")
- Online signing: **local linear operations + one broadcast**
- Agnostic to the shared-linear-system solver used offline
- Compatible with any secret sharing scheme on Fields

First evaluation on a genuine wide-area network

- Practical implementation, 2 to 16 parties
- 16 AWS instances in **distinct geographic regions**, public internet
- To appear in ACM Conference on Post-Quantum and Quantum-based Security

Multivariate Cryptography

Polynomial System Solving over a Finite Field $\mathbb{F}_q$ (the hard hard problem)

Inputs. MQ polynomials $\mathcal{P} = (p_1, \ldots, p_m) \in \mathbb{F}_q[x_1, \ldots, x_n]^m$
Goal. Find, if possible, a vector $\boldsymbol{z} \in \mathbb{F}_q^n$ such that:

$$\mathcal{P}(\boldsymbol{z}) = 0_m$$

Matsumoto-Imai multivariate signature scheme [Matsumoto, Imai, EUROCRYPT 1988]

Public-key. MQ polynomials $\mathcal{P} = (p_1, \ldots, p_m) \in \mathbb{F}_q[x_1, \ldots, x_n]^m$
Secret-key. A secret to efficiently invert $\mathcal{P}$.

A signature $(\sigma, \text{salt}) \in \mathbb{F}_q^n \times \{0,1\}^\ell$ of msg $\in \{0,1\}^*$ satisfies

$$\mathcal{P}(\sigma) = \mathcal{H}(\text{msg}\|\text{salt}), \text{with } \mathcal{H} \text{ a hash function.}$$

Multivariate Cryptography

Polynomial System Solving over a Finite Field $\mathbb{F}_q$ (the hard hard problem)

Inputs. MQ polynomials $\mathcal{P} = (p_1, \ldots, p_m) \in \mathbb{F}_q[x_1, \ldots, x_n]^m$
Goal. Find, if possible, a vector $\boldsymbol{z} \in \mathbb{F}_q^n$ such that:

$$\mathcal{P}(\boldsymbol{z}) = 0_m$$

Matsumoto-Imai multivariate signature scheme [Matsumoto, Imai, EUROCRYPT 1988]

Public-key. MQ polynomials $\mathcal{P} = (p_1, \ldots, p_m) \in \mathbb{F}_q[x_1, \ldots, x_n]^m$
Secret-key. A secret to efficiently invert $\mathcal{P}$.

A signature $(\boldsymbol{\sigma}, \text{salt}) \in \mathbb{F}_q^n \times \{0,1\}^\ell$ of msg $\in \{0,1\}^*$ satisfies

$$\mathcal{P}(\boldsymbol{\sigma}) = \mathcal{H}(\text{msg} \| \text{salt}), \text{with } \mathcal{H} \text{ a hash function.}$$

Unbalanced Oil and Vinegar (UOV)

[Kipnis, Patarin, Goubin, EUROCRYPT 1999, Beullens, EUROCRYPT 2021]

Let $n > m$ and $v = n - m$.

UOV key pair

Public-key. $\mathcal{P} = (p_1, \ldots, p_m)$ with $p_i(\boldsymbol{x}) = \boldsymbol{x}^\intercal \boldsymbol{Q}_i \boldsymbol{x}$, $\quad \boldsymbol{Q}_i = \begin{pmatrix} \boldsymbol{Q}_i^{(1)} & \boldsymbol{Q}_i^{(2)} \\ 0 & \boldsymbol{Q}_i^{(3)} \end{pmatrix} \in \mathbb{F}_q^{n \times n}$

Secret-key The oil space $\mathcal{O} \subset \mathbb{F}_q^n$, $\dim(\mathcal{O}) = m$, with systematic basis $\begin{pmatrix} \mathrm{O} \\ 1_m \end{pmatrix}$, $\mathrm{O} \in \mathbb{F}_q^{v \times m}$

Trapdoor. $\forall \boldsymbol{o} \in \mathcal{O},\ \mathcal{P}(\boldsymbol{o}) = 0_m$

UOV signature

$$(\boldsymbol{\sigma}, \mathsf{salt}) \text{ with } \mathcal{P}(\boldsymbol{\sigma}) = \mathcal{H}(\mathsf{msg} \| \mathsf{salt})$$

How to sign with UOV

[Kipnis, Patarin, Goubin, EUROCRYPT 1999, Beullens, EUROCRYPT 2021]

UOV Signing Procedure

Input: $\mathsf{O}, \boldsymbol{Q}$

1: $salt \leftarrow \text{Rand}\left(\{0,1\}^{\text{len_salt}}\right)$
2: $\boldsymbol{h} \leftarrow \mathcal{H}(msg||salt)$
3: $\boldsymbol{S}_{i,i\in[m]} \leftarrow \left(\left(\boldsymbol{Q}_i^{(1)} + \left(\boldsymbol{Q}_i^{(1)}\right)^T\right)\mathsf{O} + \boldsymbol{Q}_i^{(2)}\right)$
4: **repeat**
5: $\quad \boldsymbol{v} \leftarrow \text{Rand}\left(\mathbb{F}_q^v\right)$
6: $\quad \boldsymbol{A}_{i,i\in[m]} \leftarrow \boldsymbol{v}^T\boldsymbol{S}_i$
7: **until** A invertible
8: $\boldsymbol{b}_{i,i\in[m]} \leftarrow \boldsymbol{v}^T\boldsymbol{Q}_i^{(1)}\boldsymbol{v}$
9: Solve $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{h} - \boldsymbol{b}$ for x
10: $\boldsymbol{\sigma} \leftarrow \text{Open}\left(\begin{bmatrix} \boldsymbol{v} + \mathsf{O}\boldsymbol{x} \\ \boldsymbol{x} \end{bmatrix}\right)$
11: **return** $(\boldsymbol{\sigma}, salt)$

Pre-signature Separation
[Shim, Lee, Koo, 2021]

l.9 independent of msg
l.10 partially independent:

$$\sigma = \begin{bmatrix} \boldsymbol{v} + \mathsf{O}\boldsymbol{x} \\ \boldsymbol{x} \end{bmatrix} = \begin{bmatrix} \mathsf{O}\boldsymbol{A}^{-1}\boldsymbol{h} - (\boldsymbol{v} + \mathsf{O}\boldsymbol{A}^{-1}\boldsymbol{b}) \\ \boldsymbol{A}^{-1}\boldsymbol{h} - (\boldsymbol{A}^{-1}\boldsymbol{b}) \end{bmatrix}$$

pre-signatures are single use!

How to sign with UOV

[Kipnis, Patarin, Goubin, EUROCRYPT 1999, Beullens, EUROCRYPT 2021]

UOV Signing Procedure

Input: $\mathsf{O}, \boldsymbol{Q}$

1: $salt \leftarrow \text{Rand}\left(\{0,1\}^{\text{len_salt}}\right)$
2: $\boldsymbol{h} \leftarrow \mathcal{H}(msg||salt)$
3: $\boldsymbol{S}_{i,i\in[m]} \leftarrow \left(\left(\boldsymbol{Q}_i^{(1)} + \left(\boldsymbol{Q}_i^{(1)}\right)^T\right)\mathsf{O} + \boldsymbol{Q}_i^{(2)}\right)$
4: **repeat**
5: $\quad \boldsymbol{v} \leftarrow \text{Rand}\left(\mathbb{F}_q^v\right)$
6: $\quad \boldsymbol{A}_{i,i\in[m]} \leftarrow \boldsymbol{v}^T\boldsymbol{S}_i$
7: **until** A invertible
8: $\boldsymbol{b}_{i,i\in[m]} \leftarrow \boldsymbol{v}^T\boldsymbol{Q}_i^{(1)}\boldsymbol{v}$
9: Solve $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{h} - \boldsymbol{b}$ for x
10: $\boldsymbol{\sigma} \leftarrow \text{Open}\left(\begin{bmatrix} \boldsymbol{v} + \mathsf{O}\boldsymbol{x} \\ \boldsymbol{x} \end{bmatrix}\right)$
11: **return** $(\boldsymbol{\sigma}, salt)$

Pre-signature Separation

[Shim, Lee, Koo, 2021]

`l.9` independent of *msg*
`l.10` partially independent:

$$\boldsymbol{\sigma} = \begin{bmatrix} \boldsymbol{v} + \mathsf{O}\boldsymbol{x} \\ \boldsymbol{x} \end{bmatrix} = \begin{bmatrix} \mathsf{O}\boldsymbol{A}^{-1}\boldsymbol{h} - (\boldsymbol{v} + \mathsf{O}\boldsymbol{A}^{-1}\boldsymbol{b}) \\ \boldsymbol{A}^{-1}\boldsymbol{h} - (\boldsymbol{A}^{-1}\boldsymbol{b}) \end{bmatrix}$$

pre-signatures are single use!

DUOV – offline phase: PreSign

We denote $[\boldsymbol{X}] = (\boldsymbol{X}_1, \ldots, \boldsymbol{X}_N)$ the secret shares of $\boldsymbol{X} \in \mathbb{F}_q^{n \times m}$ st. party P_i holds $\boldsymbol{X}_i$

Data: $\boldsymbol{Q}_1, \ldots, \boldsymbol{Q}_m$, $[\mathrm{O}]$, $[\boldsymbol{S}_1], \ldots, [\boldsymbol{S}_m]$

1. $\mathrm{salt} \xleftarrow{\$} \{0,1\}^\ell$ salt moved offline
2. **repeat**
   $[\boldsymbol{v}] \leftarrow \mathrm{Rand}(v, 1)$
   $[\boldsymbol{A}_i] \leftarrow [\boldsymbol{v}^\intercal][\boldsymbol{S}_i], \ 1 \le i \le m$
   $[\boldsymbol{A}_{\boldsymbol{v}}^{-1}] \leftarrow \mathrm{Invert}([\boldsymbol{A}_{\boldsymbol{v}}])$
   until $[\boldsymbol{A}_{\boldsymbol{v}}^{-1}] \neq \perp$
3. $[b_{\boldsymbol{v},i}] \leftarrow -[\boldsymbol{v}^\intercal]\boldsymbol{Q}_i^{(1)}[\boldsymbol{v}]$
4. $[\boldsymbol{x}_{\boldsymbol{v}}] \leftarrow [\boldsymbol{A}_{\boldsymbol{v}}^{-1}][\boldsymbol{b}_{\boldsymbol{v}}]$
5. $[\mathrm{O}\boldsymbol{A}_{\boldsymbol{v}}^{-1}] \leftarrow [\mathrm{O}][\boldsymbol{A}_{\boldsymbol{v}}^{-1}]$
6. $[\boldsymbol{\sigma}'_{\boldsymbol{v}}] \leftarrow [\mathrm{O}][\boldsymbol{x}_{\boldsymbol{v}}] + [\boldsymbol{v}]$
7. **return** $\left(\mathrm{salt}, [\boldsymbol{x}_{\boldsymbol{v}}], [\boldsymbol{\sigma}'_{\boldsymbol{v}}], [\boldsymbol{A}_{\boldsymbol{v}}^{-1}], [\mathrm{O}\boldsymbol{A}_{\boldsymbol{v}}^{-1}]\right)$

- Ahead-of-time
- Batching
- Cost amortization

DUOV – online phase: SignFromPreSig

Data: msg and a fresh pre-signature $(\text{salt}, [\boldsymbol{x_v}], [\boldsymbol{\sigma'_v}], [\boldsymbol{A_v^{-1}}], [\mathrm{O}\boldsymbol{A_v^{-1}}])$

1. $\boldsymbol{h} \leftarrow \mathcal{H}(\text{msg} \| \text{salt})$ **public**
2. $[\boldsymbol{x}] \leftarrow [\boldsymbol{x_v}] + [\boldsymbol{A_v^{-1}}]\boldsymbol{h}$ **local**
3. $[\boldsymbol{\sigma'_v}] \leftarrow [\boldsymbol{\sigma'_v}] + [\mathrm{O}\boldsymbol{A_v^{-1}}]\boldsymbol{h}$ **local**
4. $[\boldsymbol{\sigma}] := \begin{pmatrix} [\boldsymbol{\sigma'_v}] \\ [\boldsymbol{x}] \end{pmatrix}$
5. $\boldsymbol{\sigma} \leftarrow \text{Open}([\boldsymbol{\sigma}])$ one round
6. **if** $\text{Verify}(\mathcal{P}, \text{msg}, \boldsymbol{\sigma}, \text{salt}) = 0$: abort
7. **return** $(\boldsymbol{\sigma}, \text{salt})$

online communication

Given a pre-signature, signing takes **one round**: a single broadcast of $\log_2 |\mathbb{F}_q^n|$ bits.

Caveats

- **Never reuse** a pre-signature

DUOV – online phase: SignFromPreSig

Data: msg and a fresh pre-signature $(\text{salt}, [\boldsymbol{x}_v], [\boldsymbol{\sigma}'_v], [\boldsymbol{A}_v^{-1}], [\mathrm{O}\boldsymbol{A}_v^{-1}])$

1. $\boldsymbol{h} \leftarrow \mathcal{H}(\text{msg}\|\text{salt})$ **public**
2. $[\boldsymbol{x}] \leftarrow [\boldsymbol{x}_v] + [\boldsymbol{A}_v^{-1}]\boldsymbol{h}$ **local**
3. $[\boldsymbol{\sigma}'_v] \leftarrow [\boldsymbol{\sigma}'_v] + [\mathrm{O}\boldsymbol{A}_v^{-1}]\boldsymbol{h}$ **local**
4. $[\boldsymbol{\sigma}] := \begin{pmatrix} [\boldsymbol{\sigma}'_v] \\ [\boldsymbol{x}] \end{pmatrix}$
5. $\boldsymbol{\sigma} \leftarrow \mathrm{Open}([\boldsymbol{\sigma}])$ one round
6. **if** $\mathrm{Verify}(\mathcal{P}, \text{msg}, \boldsymbol{\sigma}, \text{salt}) = 0$: abort
7. **return** $(\boldsymbol{\sigma}, \text{salt})$

online communication

Given a pre-signature, signing takes **one round**: a single broadcast of $\log_2 |\mathbb{F}_q^n|$ bits.

Caveats

- **Never reuse** a pre-signature

Shared Linear System Solving (SLiSS)

SLiSS problem [Cozzo, Smart, IMACC 2019; Azevedo-Oliveira, Beraud, Varjabedian, 2026]

Given $([\boldsymbol{A}], [\boldsymbol{b}])$, securely compute $[\boldsymbol{x}]$ such that $\boldsymbol{Ax} = \boldsymbol{b}$.

Shared linear system solvers

- D. Cozzo, N. P. Smart. *Sharing the LUOV: Threshold Post-quantum Signatures*. IMACC 2019.
- S. Celi, D. Escudero, G. Niot. *Share the MAYO: thresholdizing MAYO*. ePrint 2024/1960.
- J. Maire, D. Vergnaud. *Secure Multi-Party Linear Algebra with Perfect Correctness*. IACR CiC 2024.
- P. Azevedo-Oliveira, J. Beraud, P. Varjabedian. *Shared and leakage free MAYO*. ePrint 2026/189.
- D. F. Aranha, G. Borin, S. Celi, G. Niot. *Optimizing and Implementing Threshold MAYO*. ePrint 2026/710.

Comparison with vinaigrette [Aranha et al., MPTS 2026]

Concurrent and independent works.
DUOV first appeared in a 2023 master's thesis of the third author.
To appear in ACM PQQS'26

	vinaigrette	DUOV
Online rounds	1 (explicit-salt variant)	1
Offline	matrix inverse, salt	whole $\boldsymbol{\sigma}_{\mathrm{pre}}$: $\boldsymbol{v}$, $\boldsymbol{A}_{\boldsymbol{v}}^{-1}$, $\boldsymbol{x}_{\boldsymbol{v}}$, $\mathrm{O}\boldsymbol{A}_{\boldsymbol{v}}^{-1}$, salt
Online work	linear ops on a fixed vinegar	**only $[\boldsymbol{X}]\boldsymbol{h}$ products + 1 open**

DUOV **absorbs the vinegar vector entirely**

Comparison with vinaigrette [Aranha et al., MPTS 2026]

Concurrent and independent works.
DUOV first appeared in a 2023 master's thesis of the third author.
To appear in ACM PQQS'26

	vinaigrette	DUOV
Online rounds	1 (explicit-salt variant)	1
Offline	matrix inverse, salt	whole σ_{pre}: $\boldsymbol{v}$, $\boldsymbol{A}_{\boldsymbol{v}}^{-1}$, $\boldsymbol{x}_{\boldsymbol{v}}$, $\mathrm{O}\boldsymbol{A}_{\boldsymbol{v}}^{-1}$, salt
Online work	linear ops on a fixed vinegar	**only $[\boldsymbol{X}]\boldsymbol{h}$ products + 1 open**

DUOV **absorbs the vinegar vector entirely**

Implementation

Prototype

- **Common Lisp**: malleability, debugging tools, high-level networking + low-level performance control
- `SBCL 2.6.6`; seed expansion with `tiny-AES-c` (via `CFFI`)
- `USOCKET`, `Bordeaux-Threads`, `Alexandria`, `nibbles`, `Quicklisp`, `lev`

What is benchmarked

- SignFromPreSig (steps 2–7: local ops, Open, Verify), hashing excluded
- Additive sharing over $\mathbb{F}_{2^8}$, parameter set U0V-Ip [Beullens et al., NIST 2023]
- Pre-signatures generated and secret-shared during setup, then distributed
- 2 to 16 parties, **1000 signatures** per network size

Open-source release (permissive licence) before package submission.

Implementation

Prototype

- **Common Lisp**: malleability, debugging tools, high-level networking + low-level performance control
- SBCL `2.6.6`; seed expansion with `tiny-AES-c` (via `CFFI`)
- `USOCKET`, `Bordeaux-Threads`, `Alexandria`, `nibbles`, `Quicklisp`, `lev`

What is benchmarked

- SignFromPreSig (steps 2–7: local ops, Open, Verify), hashing excluded
- Additive sharing over $\mathbb{F}_{2^8}$, parameter set UOV-Ip [Beullens et al., NIST 2023]
- Pre-signatures generated and secret-shared during setup, then distributed
- 2 to 16 parties, **1000 signatures** per network size

Open-source release (permissive licence) before package submission.

Evaluation on a genuine wide-area network

Control environment

- One Scaleway `POP2-HC-32C-64G` (32 vCPU @ 3.2 GHz, 64 GB)
- 16 emulated parties, each `taskset` to 2 cores
- Sockets over **loopback**

Test environment

- 16 AWS `t3.small` (2 vCPU @ 2.5 GHz, 2 GB)
- One instance per **distinct AWS region**
- Public internet, WireGuard VPN

Goal: individuals in different places signing together over the internet.
Previous threshold UOV/MAYO timings: **local emulation** (function calls, single process).
NIST baseline platform (16 cores, 64 GB) results: planned for the package submission.

Evaluation on a genuine wide-area network

Control environment

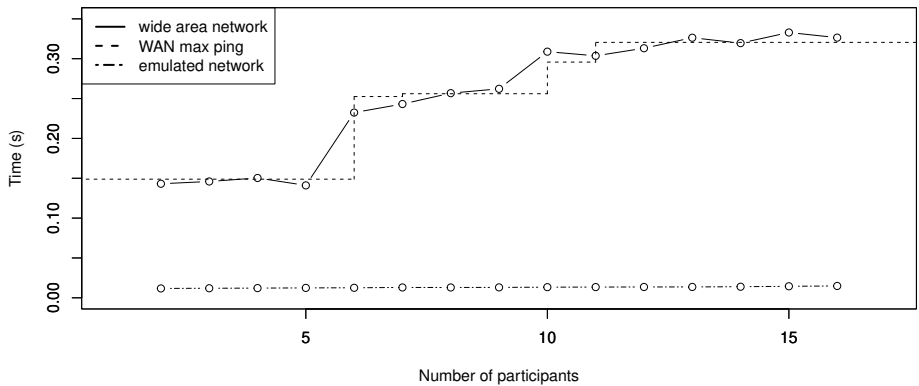
- One Scaleway `POP2-HC-32C-64G` (32 vCPU @ 3.2 GHz, 64 GB)
- 16 emulated parties, each `taskset` to 2 cores
- Sockets over **loopback**

Test environment

- 16 AWS `t3.small` (2 vCPU @ 2.5 GHz, 2 GB)
- One instance per **distinct AWS region**
- Public internet, WireGuard VPN

Goal: individuals in different places signing together over the internet.
Previous threshold UOV/MAYO timings: **local emulation** (function calls, single process).
NIST baseline platform (16 cores, 64 GB) results: planned for the package submission.

Online signing time – UOV-Ip, 1000 signatures per N



- **Emulated network:** a few ms, grows mildly with N (all-to-all Open)
- Wide-area network: $\approx$ 0.15–0.33 s, **same step pattern as the maximum pairwise ping**

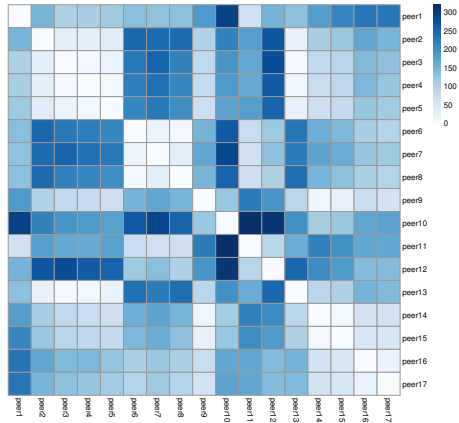
Latency, not computation, dominates

Why

- Same code in both environments
- CPU ratio (2.5 vs 3.2 GHz) far too small to explain the gap
- One broadcast of 896 bits $\Rightarrow$ fits in **one network frame**

Takeaway

- Online cost $\approx$ **latency between the farthest parties**
- First evaluation of a threshold multivariate signature on a **true WAN**



Pairwise ping between AWS regions (ms)

Conclusion

DUOV

- Threshold UOV with **pre-signing**: message-independent work moved offline
- Online: **local linear operations + one broadcast**
- Evaluated over 16 AWS regions: online time $\approx$ max. pairwise latency, not computation

Next steps

Active security · (t, N) thresholds · leakage-free offline solver · offline phase benchmarks · NIST baseline platform · open-source release · MAYO and other variants

Conclusion

DUOV

- Threshold UOV with **pre-signing**: message-independent work moved offline
- Online: **local linear operations + one broadcast**
- Evaluated over 16 AWS regions: online time $\approx$ max. pairwise latency, not computation

Next steps

Active security · (t, N) thresholds · leakage-free offline solver
offline phase benchmarks · NIST baseline platform · open-source release · MAYO and other variants

For questions or feedback,
please reach out

contact-duov@astran.ai