Universal forgery of Sequential Aggregate Signatures based on UOV

Edoardo Signorini
edoardo.signorini@telsy.it

Telsy S.p.A.

PQCifris 2022

13/10/2022

Signers

Verifier

$$\overrightarrow{\mathrm{pk}} = (\mathrm{pk}_1, \dots, \mathrm{pk}_n)$$

$$(\mathrm{sk}_i, \mathrm{pk}_i) \leftarrow \mathtt{KeyGen}$$

$$\sigma_i \leftarrow \mathtt{Sign}(\mathrm{sk}_i, M_i)$$

Signers

$\overrightarrow{\mathrm{pk}} = (\mathrm{pk}_1, \ldots, \mathrm{pk}_n)$

Verifier

$(\mathrm{sk}_i, \mathrm{pk}_i) \leftarrow \mathtt{KeyGen}$

$\sigma_i \leftarrow \mathtt{Sign}(\mathrm{sk}_i, M_i)$

$\Sigma \leftarrow \mathtt{AggSign}(\vec{M}, \vec{\sigma})$

$\vec{M}, \Sigma$

$\{✓, ✗\} \leftarrow \mathtt{AggVf}(\overrightarrow{\mathrm{pk}}, \vec{M}, \Sigma)$

Goal

Combine multiple σ_i in a single Σ such that $|\Sigma| \ll \sum_i |\sigma_i|$

Signers

$\overrightarrow{\text{pk}} = (\text{pk}_1, \dots, \text{pk}_n)$

Verifier

$(\text{sk}_i, \text{pk}_i) \leftarrow \texttt{KeyGen}$

$\sigma_i \leftarrow \texttt{Sign}(\text{sk}_i, M_i)$

$\Sigma \leftarrow \texttt{AggSign}(\vec{M}, \vec{\sigma})$

$\vec{M}, \Sigma$

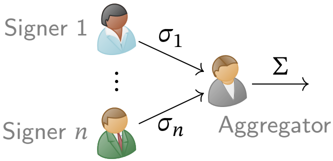
$\{✓, ✗\} \leftarrow \texttt{AggVf}(\overrightarrow{\text{pk}}, \vec{M}, \Sigma)$

Goal

Combine multiple σ_i in a single Σ such that $|\Sigma| \ll \sum_i |\sigma_i|$

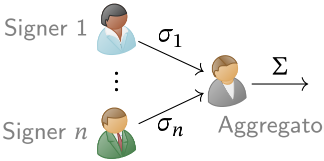
- Reduce bandwidth consumption
- Constrained devices
- Certificate chains
- Blockchains

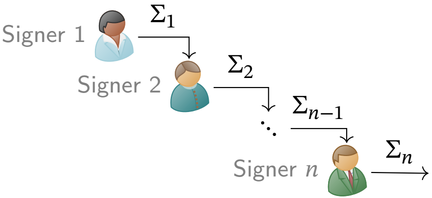
- General Aggregate Signature
  - Public aggregation by third party
  - No interaction required by signers
  - Only known construction is based on pairing [Bon+03]



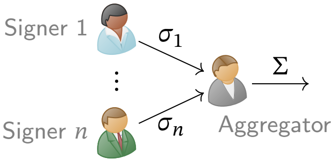
Types of Aggregate Signature

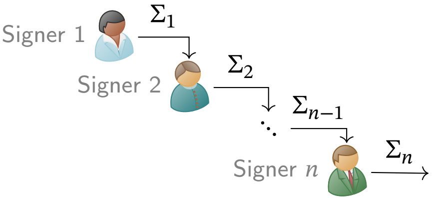
- General Aggregate Signature
  - Public aggregation by third party
  - No interaction required by signers
  - Only known construction is based on pairing [Bon+03]
- Sequential Aggregate Signature (SAS)
  - Signatures are iteratively aggregated
  - Aggregation by signers only
  - Can be built from trapdoor permutation [Lys+04; Nev08]





- General Aggregate Signature
  - Public aggregation by third party
  - No interaction required by signers
  - Only known construction is based on pairing [Bon+03]
- Sequential Aggregate Signature (SAS)
  - Signatures are iteratively aggregated
  - Aggregation by signers only
  - Can be built from trapdoor permutation [Lys+04; Nev08]





Can (S)AS be built from post-quantum assumptions?

- General Aggregate Signature
  - Public aggregation by third party
  - No interaction required by signers
  - Only known construction is based on pairing [Bon+03]
- **Sequential Aggregate Signature** (SAS)
  - Signatures are iteratively aggregated
  - Aggregation by signers only
  - Can be built from trapdoor permutation [Lys+04; Nev08]

tentative

[Dor+20; BR21]

MQ-based

Lattice-based

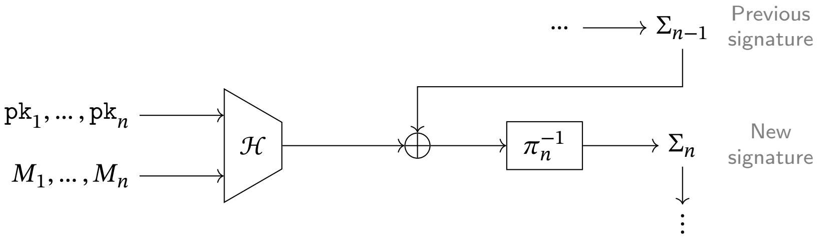
[EMP16; Che+20]

[EB14]

Can (S)AS be built from post-quantum assumptions?

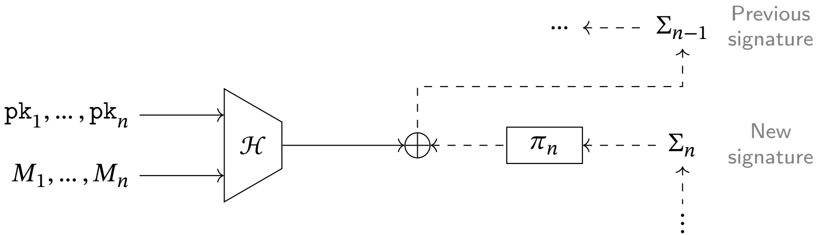
Full Domain Hash (FDH) signature from trapdoor permutation π and opportune hash function $\mathcal{H}$

Full Domain Hash (FDH) signature from trapdoor permutation π and opportune hash function $\mathcal{H}$



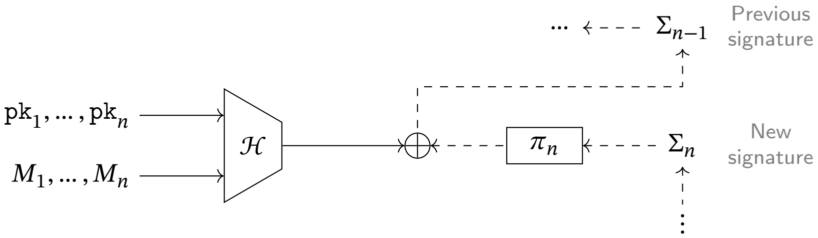
- **Aggregation** (simplified) [Lys+04; Nev08]: embed the previous aggregate signature into the new data to be signed

Full Domain Hash (FDH) signature from trapdoor permutation π and opportune hash function $\mathcal{H}$



- **Aggregation** (simplified) [Lys+04; Nev08]: embed the previous aggregate signature into the new data to be signed
- **Verification**: recover each intermediate signature. Requires n steps of verification

Full Domain Hash (FDH) signature from trapdoor permutation π and opportune hash function $\mathcal{H}$



- **Aggregation** (simplified) [Lys+04; Nev08]: embed the previous aggregate signature into the new data to be signed
- **Verification**: recover each intermediate signature. Requires n steps of verification

Rigid transposition of FDH approach to post-quantum assumptions seems impractical

MQ assumption

Solving a system of random quadratic equations over $\mathbb{F}_q$ is hard on average

- **Public key**: multivariate quadratic map $\mathcal{P}: \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$
- **Private key**: description of an hidden structure in $\mathcal{P}$ that makes it easy to find a preimage

MQ assumption

Solving a system of random quadratic equations over $\mathbb{F}_q$ is hard on average

- **Public key**: multivariate quadratic map $\mathcal{P}: \mathbb{F}_q^n \to \mathbb{F}_q^m$
- **Private key**: description of an hidden structure in $\mathcal{P}$ that makes it easy to find a preimage

Mainly used for digital signatures:

- **Signature** for message M: a preimage $\sigma \leftarrow \mathcal{P}^{-1}(\mathcal{H}(M))$, for an opportune hash function $\mathcal{H}: \{0,1\}^* \to \mathbb{F}_q^m$
- **Verification** for (M, σ): check that $\mathcal{P}(\sigma) \stackrel{?}{=} \mathcal{H}(M)$

Random salt required
for security proofs

Unbalanced Oil and Vinegar

As formalized in [Beu21]

$(\mathcal{P}, O) \in \texttt{UOV}(q, n, m)$:

- **Private key**: secret linear subspace $O \subset \mathbb{F}_q^n$ of dimension m
- **Public key**: multivariate quadratic map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ that vanishes on O

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[d, "\mathcal{P}"] & O \arrow[l, hook'] \arrow[d, "\mathcal{P}"] \\
\mathbb{F}_q^m & \{0\} \arrow[l, hook']
\end{tikzcd}$$

As formalized in [Beu21]

$(\mathcal{P}, O) \in \mathtt{UOV}(q, n, m)$:

- **Private key**: secret linear subspace $O \subset \mathbb{F}_q^n$ of dimension m
- **Public key**: multivariate quadratic map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ that vanishes on O

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[d, "\mathcal{P}"] & O \arrow[l, hook'] \arrow[d, "\mathcal{P}"] \arrow[dl, dashed, "\mathcal{P}'(x,\cdot)"] \\
\mathbb{F}_q^m & \{0\} \arrow[l, hook']
\end{tikzcd}$$

- Consider the polar form $\mathcal{P}' : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^m$ defined as

$$\mathcal{P}'(x, y) = \mathcal{P}(x + y) - \mathcal{P}(x) - \mathcal{P}(y)$$

  $\mathcal{P}'$ is a symmetric and bilinear map
- Knowing O we can find a preimage of $\mathcal{P}$ for $t \in \mathbb{F}_q^m$:
  - Randomly choose $v \in \mathbb{F}_q^n$
  - Solve $\mathcal{P}(v + o) = t$ for $o \in O$:

$$t = \mathcal{P}(v + o) = \mathcal{P}(v) + \mathcal{P}(o) + \mathcal{P}'(v, o)$$

Unbalanced Oil and Vinegar

As formalized in [Beu21]

$(\mathcal{P}, O) \in \texttt{UOV}(q, n, m)$:

- **Private key**: secret linear subspace $O \subset \mathbb{F}_q^n$ of dimension m
- **Public key**: multivariate quadratic map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ that vanishes on O

$$\begin{tikzcd} \mathbb{F}_q^n \arrow[d, "\mathcal{P}"] & O \arrow[l, hook'] \arrow[d, "\mathcal{P}"] \arrow[dl, dashed, "\mathcal{P}'(x,\cdot)"'] \\ \mathbb{F}_q^m & \{0\} \arrow[l, hook'] \end{tikzcd}$$

- Consider the polar form $\mathcal{P}' : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^m$ defined as

$$\mathcal{P}'(x, y) = \mathcal{P}(x + y) - \mathcal{P}(x) - \mathcal{P}(y)$$

  $\mathcal{P}'$ is a symmetric and bilinear map
- Knowing O we can find a preimage of $\mathcal{P}$ for $t \in \mathbb{F}_q^m$:
  - Randomly choose $v \in \mathbb{F}_q^n$
  - Solve $\mathcal{P}(v + o) = t$ for $o \in O$:

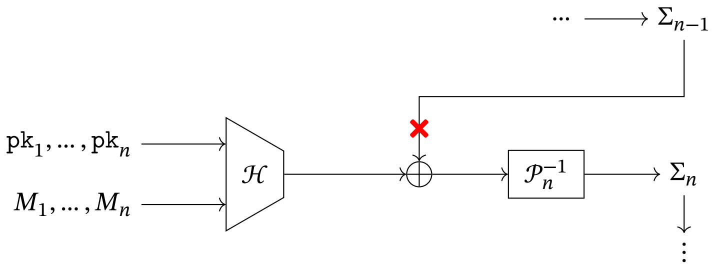
$$t = \mathcal{P}(v + o) = \mathcal{P}(v) + \cancel{\mathcal{P}(o)} + \mathcal{P}'(v, o)$$

fixed

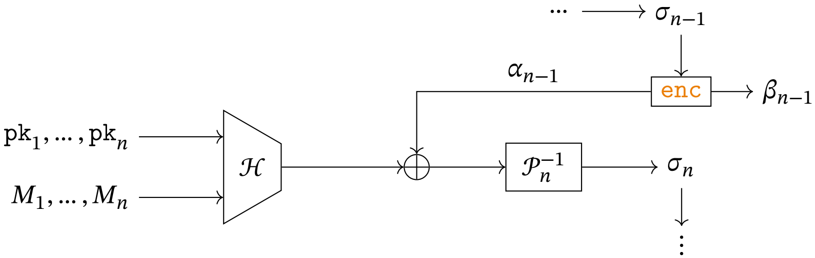
linear in o

  - This is a linear system of m equations and m variables
  - If there are no solutions choose another $v \in \mathbb{F}_q^n$

Multivariate trapdoor functions $\mathcal{P}$ are not permutation

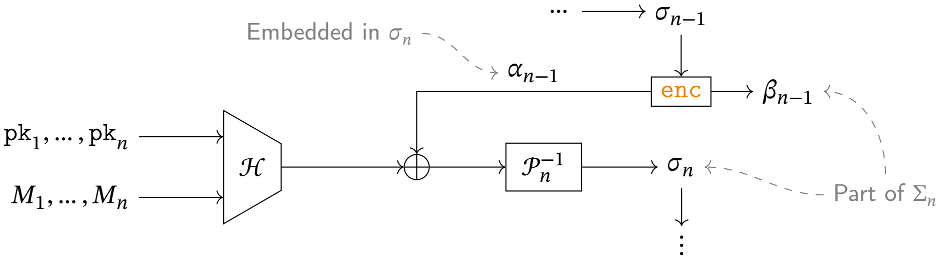


Multivariate trapdoor functions $\mathcal{P}$ are not permutation



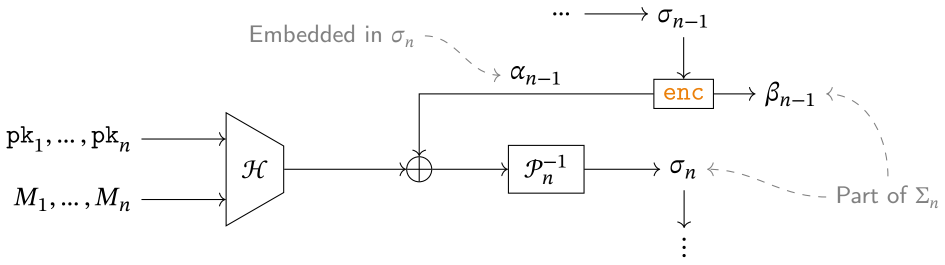
- Use an *efficient* encoding function $\texttt{enc} : \mathbb{F}_q^n \to \mathbb{F}_q^m \times \mathbb{F}_q^{n-m}$ that splits σ_i as $\texttt{enc}(\sigma_i) = (\alpha_i, \beta_i)$ [Nev08; EB14]

Multivariate trapdoor functions $\mathcal{P}$ are not permutation



- Use an *efficient* encoding function enc : $\mathbb{F}_q^n \to \mathbb{F}_q^m \times \mathbb{F}_q^{n-m}$ that splits σ_i as enc$(\sigma_i) = (\alpha_i, \beta_i)$ [Nev08; EB14]
- The aggregate signature is given by $\Sigma_n = (\beta_1, \dots, \beta_{n-1}, \sigma_n)$
- This construction can be instantiated with every multivariate signature scheme [EMP16; Che+20]

Multivariate trapdoor functions $\mathcal{P}$ are not permutation



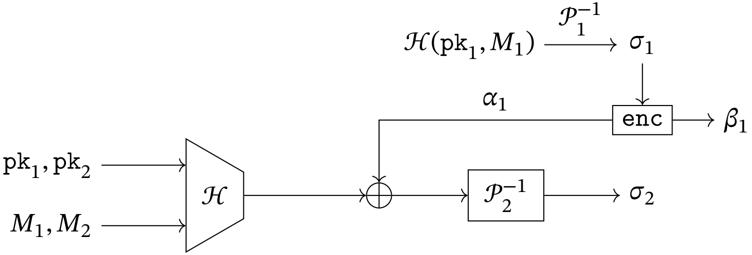
- Use an *efficient* encoding function $\mathtt{enc} : \mathbb{F}_q^n \to \mathbb{F}_q^m \times \mathbb{F}_q^{n-m}$ that splits σ_i as $\mathtt{enc}(\sigma_i) = (\alpha_i, \beta_i)$ [Nev08; EB14]
- The aggregate signature is given by $\Sigma_n = (\beta_1, \dots, \beta_{n-1}, \sigma_n)$
- This construction can be instantiated with ~~every~~ multivariate signature scheme [EMP16; Che+20]

Not with UOV!

Universal forgery of UOV-SAS

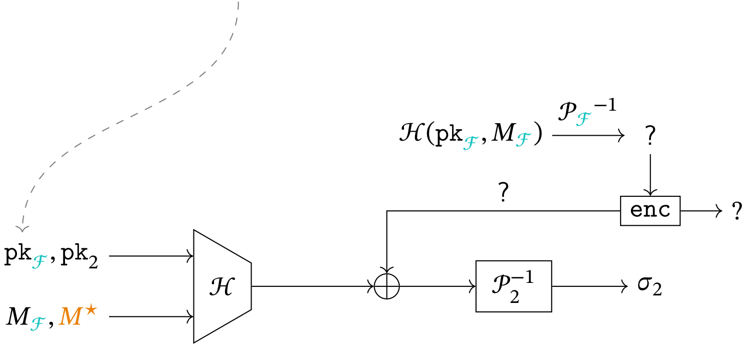
Case $n = 2$

- **Setting**: known valid aggregate signature $\Sigma = (\beta_1, \sigma_2)$ for messages M_1, M_2 under honest public keys $\mathtt{pk}_1, \mathtt{pk}_2$
- **Target**: signer 2 with public key $\mathtt{pk}_2 = \mathcal{P}_2$ and a selected message $M^\star$



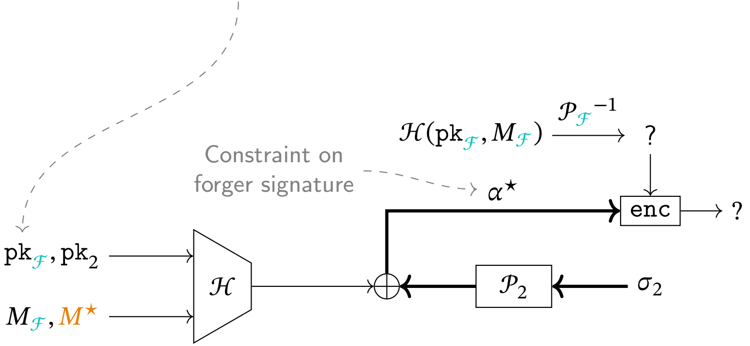
Case $n = 2$

- **Setting**: known valid aggregate signature $\Sigma = (\beta_1, \sigma_2)$ for messages M_1, M_2 under honest public keys $\mathtt{pk}_1, \mathtt{pk}_2$
- **Target**: signer 2 with public key $\mathtt{pk}_2 = \mathcal{P}_2$ and a selected message $M^\star$
- **Idea**: the forger $\mathcal{F}$ replaces the second-last signer



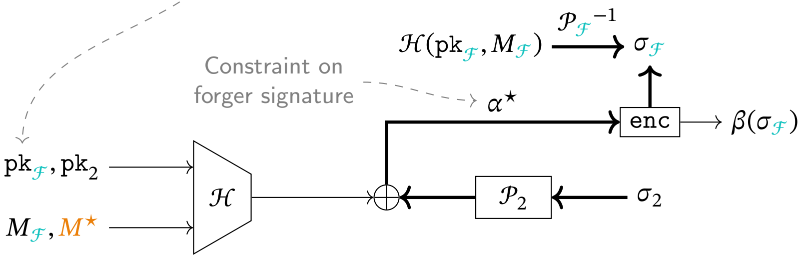
Case $n = 2$

- **Setting**: known valid aggregate signature $\Sigma = (\beta_1, \sigma_2)$ for messages M_1, M_2 under honest public keys $\mathtt{pk}_1, \mathtt{pk}_2$
- **Target**: signer 2 with public key $\mathtt{pk}_2 = \mathcal{P}_2$ and a selected message $M^\star$
- **Idea**: the forger $\mathcal{F}$ replaces the second-last signer



Case $n = 2$

- **Setting**: known valid aggregate signature $\Sigma = (\beta_1, \sigma_2)$ for messages M_1, M_2 under honest public keys $\mathtt{pk}_1, \mathtt{pk}_2$
- **Target**: signer 2 with public key $\mathtt{pk}_2 = \mathcal{P}_2$ and a selected message $M^\star$
- **Idea**: the forger $\mathcal{F}$ replaces the second-last signer



- **Result**: $\Sigma^\star = (\beta(\sigma_\mathcal{F}), \sigma_2)$ is a valid aggregate signature for messages $M_\mathcal{F}, M^\star$ under public keys $\mathcal{P}_\mathcal{F}, \mathcal{P}_2$

Partially fixed preimage

- Assume $\mathtt{enc}(x)$ to be an affine map and write $\alpha(x) = R(x) = \mathbf{A}x + b$, with $\mathbf{A} \in \mathbb{F}_q^{m \times n}, b \in \mathbb{F}_q^m$

Let $(\mathcal{P}, O) \in \mathtt{UOV}^{\star}(q, n, m)$ and $R : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ an affine map. Given $t, a \in \mathbb{F}_q^m$, find $\sigma \in \mathbb{F}_q^n$ such that $\mathcal{P}(\sigma) = t$ and $R(\sigma) = a$.

Partially fixed preimage

- Assume $\mathtt{enc}(x)$ to be an affine map and write $\alpha(x) = R(x) = \mathbf{A}x + b$, with $\mathbf{A} \in \mathbb{F}_q^{m\times n}, b \in \mathbb{F}_q^m$

Let $(\mathcal{P}, O) \in \mathtt{UOV}^\star(q, n, m)$ and $R : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ an affine map. Given $t, a \in \mathbb{F}_q^m$, find $\sigma \in \mathbb{F}_q^n$ such that $\mathcal{P}(\sigma) = t$ and $R(\sigma) = a$.

- Generate $(\mathcal{P}, O)$ by randomly choosing $O \subset \ker \mathbf{A}$ and $\mathcal{P}$ that vanishes on O.
- Use a modified UOV signing procedure to find the preimage of $\mathcal{P}$ for t:

Partially fixed preimage

- Assume $\mathtt{enc}(x)$ to be an affine map and write $\alpha(x) = R(x) = \mathbf{A}x + b$, with $\mathbf{A} \in \mathbb{F}_q^{m\times n}, b \in \mathbb{F}_q^m$

Let $(\mathcal{P}, O) \in \mathtt{UOV}^\star(q, n, m)$ and $R : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ an affine map. Given $t, a \in \mathbb{F}_q^m$, find $\sigma \in \mathbb{F}_q^n$ such that $\mathcal{P}(\sigma) = t$ and $R(\sigma) = a$.

- Generate $(\mathcal{P}, O)$ by randomly choosing $O \subset \ker \mathbf{A}$ and $\mathcal{P}$ that vanishes on O.
- Use a modified UOV signing procedure to find the preimage of $\mathcal{P}$ for t:
  - Randomly choose $v \in \ker R'$, with $R'(x) = R(x) - a = \mathbf{A}x + (b - a)$
  - Solve $\mathcal{P}(v + o) = t$ for $o \in O$ and find $\sigma = v + o$
  - Since $O \subset \ker \mathbf{A}$, then $\sigma \in \ker R'$ and $R(\sigma) = a$

Further investigations

- EUF-CMA claims of [EMP16; Che+20] are incorrect when instantiated with UOV, can it be somewhat generalized?

Future work

- Design a secure, non-centralized sequential aggregate signature scheme based on UOV

Open questions

- Is it possible to construct a general aggregate signature scheme from the MQ (or any post-quantum) assumption?

[Beu21] Ward Beullens. "Improved Cryptanalysis of UOV and Rainbow". In: *Advances in Cryptology – EUROCRYPT 2021*. Vol. 12696. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2021, pp. 348–373.

[Bon+03] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps". In: *Advances in Cryptology — EUROCRYPT 2003*. Vol. 2656. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 416–432.

[BR21] Katharina Boudgoust and Adeline Roux-Langlois. *Non-Interactive Half-Aggregate Signatures Based on Module Lattices - A First Attempt*. Cryptology ePrint Archive, Paper 2021/263. 2021.

[Che+20] Jiahui Chen, Jie Ling, Jianting Ning, Zhiniang Peng, and Yang Tan. "MQ Aggregate Signature Schemes with Exact Security Based on UOV Signature". In: *Information Security and Cryptology*. Vol. 12020. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 443–451.

[Dor+20] Yarkın Doröz, Jeffrey Hoffstein, Joseph H. Silverman, and Berk Sunar. *MMSAT: A Scheme for Multimessage Multiuser Signature Aggregation*. Cryptology ePrint Archive, Paper 2020/520. 2020.

[EB14] Rachid El Bansarkhani and Johannes Buchmann. "Towards Lattice Based Aggregate Signatures". In: *Progress in Cryptology – AFRICACRYPT 2014*. Vol. 8469. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2014, pp. 336–355.

[EMP16] Rachid El Bansarkhani, Mohamed Saied Emam Mohamed, and Albrecht Petzoldt. "MQSAS - A Multivariate Sequential Aggregate Signature Scheme". In: *Information Security*. Vol. 9866. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016, pp. 426–439.

[Lys+04] Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, and Hovav Shacham. "Sequential Aggregate Signatures from Trapdoor Permutations". In: *Advances in Cryptology - EUROCRYPT 2004*. Vol. 3027. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 74–90.

[Nev08] Gregory Neven. "Efficient Sequential Aggregate Signed Data". In: *Advances in Cryptology – EUROCRYPT 2008*. Vol. 4965. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 52–69.

Telsy

Thank you for your attention

Politecnico di Torino

1859