Threshold Structure-Preserving Signatures:

Strong and Adaptive Security under Standard Assumptions

Aikaterini Mitrokotsa, Sayantan Mukherjee, Mahdi Sedaghat, Daniel Slamanig, Jenit Tomy

University of St Gallen; Indian Institute of Technology Jammu; COSIC KU Leuven; Research Institute CODE Universität der Bundeswehr München

17th April, 2024, PKC, Sydney

Outline

Scenario

- In a structure-preserving signature scheme,
  - message consists of base group elements.
  - signature consists of base group elements.
  - verification uses group-membership check and pairing-product equation.

Scenario

- In a structure-preserving signature scheme,
  - message consists of base group elements.
  - signature consists of base group elements.
  - verification uses group-membership check and pairing-product equation only.

Scenario

- In a structure-preserving signature scheme,
  - message consists of base group elements.
  - signature consists of base group elements.
  - verification uses group-membership check and pairing-product equation only.

- In a non-interactive threshold signature scheme,
  - n parties in a system with threshold t.
  - ℓ honest parties generate partial signatures $\{\Sigma_{i_j}\}_{j\in[\ell]}$ on a message m.
  - a public algorithm combines $\{\Sigma_{i_j}\}_{j\in[\ell]}$ into a signature Σ.
  - Σ is a valid signature of m if $\ell \geq t$.

Scenario

- In a structure-preserving signature scheme,
  - message consists of base group elements.
  - signature consists of base group elements.
  - verification uses group-membership check and pairing-product equation only.

- In a non-interactive threshold signature scheme,
  - n parties in a system with threshold t.
  - ℓ honest parties generate partial signatures $\{\Sigma_{i_j}\}_{j\in[\ell]}$ on a message m.
  - a public algorithm combines $\{\Sigma_{i_j}\}_{j\in[\ell]}$ into a signature Σ.
  - Σ is a valid signature of m if $\ell \geq t$.
  - Currently receiving a lot of attention due to decentralized web.

Scenario (Simplified)

Goal. To construct a threshold structure-preserving signature

Scenario (Simplified)

Goal. To construct a threshold structure-preserving signature

1. preferably in the standard model under standard assumption,

Scenario (Simplified)

Goal. To construct a threshold structure-preserving signature

1. preferably in the standard model under standard assumption,
2. in the adaptive corruption model.

Scenario (Simplified)

Goal. To construct a threshold structure-preserving signature

1. preferably in the standard model under standard assumption,
2. in the adaptive corruption model.

- Currently, there is only one work.

Scenario (Simplified)

Goal. To construct a threshold structure-preserving signature

1. preferably in the standard model under standard assumption,
2. in the adaptive corruption model.

- Currently, there is only one work.
  - In Asiacrypt'2023, Crites et al. [CKPSS23] proposed the first

Scenario (Simplified)

Goal. To construct a threshold structure-preserving signature

1. preferably in the standard model under standard assumption,
2. in the adaptive corruption model.

- Currently, there is only one work.
  - In Asiacrypt'2023, Crites et al. [CKPSS23] proposed the first
  - for limited message space (*iDH*)

Scenario (Simplified)

Goal. To construct a threshold structure-preserving signature

1. preferably in the standard model under standard assumption,
2. in the adaptive corruption model.

- Currently, there is only one work.
  - In Asiacrypt'2023, Crites et al. [CKPSS23] proposed the first
  - for limited message space (*iDH*)
  - in algebraic group model under random oracle assumption (*AGM-ROM*)

Scenario (Simplified)

Goal. To construct a threshold structure-preserving signature

1. preferably in the standard model under standard assumption,
2. in the adaptive corruption model.

- Currently, there is only one work.
  - In Asiacrypt'2023, Crites et al. [CKPSS23] proposed the first
  - for limited message space (*iDH*)
  - in algebraic group model under random oracle assumption (*AGM-ROM*)
  - and interactive assumptions (GPS_3)

Scenario (Simplified)

Goal. To construct a threshold structure-preserving signature

1. preferably in the standard model under standard assumption,
2. in the adaptive corruption model.

- Currently, there is only one work.
  - In Asiacrypt'2023, Crites et al. [CKPSS23] proposed the first
  - for limited message space (iDH)
  - in algebraic group model under random oracle assumption (AGM-ROM)
  - and interactive assumptions (GPS_3)
  - in the weakest security model (TS-UF-0)

Notations and Hardness Assumptions

- $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$ is type-III bilinear pairing group description where
$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T.$$
- We denote g_s^a by $[\![a]\!]_s$ for any $a \in \mathbb{Z}_p$ and $s \in \{1, 2, \mathrm{T}\}$.
- We denote $\left(g_s^{u_{i,j}}\right)_{(i,j) \in I \times J}$ by $[\![\mathbf{U}]\!]_s$ for any $\mathbf{U} = (u_{i,j})_{(i,j) \in I \times J}$, $s \in \{1, 2, \mathrm{T}\}$.
- $\mathcal{D}_{\ell,k}$-matDH$_{\mathbb{G}}$: $\mathcal{A}([\![\mathbf{A}]\!], [\![\mathbf{As} + \mathbf{z}]\!] : \mathbf{A} \in \mathbb{Z}_p^{\ell \times k}$, $\mathbf{s} \hookleftarrow \mathbb{Z}_p^k$, $\mathbf{z} \hookleftarrow \mathbb{Z}_p^\ell) \to \mathbf{z} \stackrel{?}{=} \mathbf{0}$.
- $\mathcal{D}_{\ell,k}$-kerDH$_{\mathbb{G}}$: $\mathcal{A}([\![\mathbf{A}]\!] : \mathbf{A} \in \mathbb{Z}_p^{\ell \times k}) \to \mathbf{s} \in \mathbb{Z}_p^k \setminus \{\mathbf{0}\}$ s.t. $\mathbf{As} = \mathbf{0}$.

Threshold Structure-Preserving Signatures (TSPS)

- $\mathsf{Setup}(1^\kappa) \rightarrow \mathsf{pp}$.
- $\mathsf{KGen}(\mathsf{pp}, n, t) \rightarrow (\{\mathsf{sk}_i, \mathsf{pk}_i\}_{i\in[1,n]}, \mathsf{pk})$.
- $\mathsf{ParSign}(\mathsf{pp}, \mathsf{sk}_i, [m] \in \mathcal{M}) \rightarrow \Sigma_i$.
- $\mathsf{ParVerify}(\mathsf{pp}, \mathsf{pk}_i, [m] \in \mathcal{M}, \Sigma_i) \rightarrow 0/1$.
- $\mathsf{CombineSign}(\mathsf{pp}, T \subseteq [1, n], \{\Sigma_i\}_{i\in T}) \rightarrow \Sigma$.
- $\mathsf{Verify}(\mathsf{pp}, \mathsf{pk}, [m] \in \mathcal{M}, \Sigma) \rightarrow 0/1$.

Correctness

For all $\mathsf{pp} \hookleftarrow \mathsf{Setup}(1^\kappa)$,

for all $(\{\mathsf{sk}_i, \mathsf{pk}_i\}_{i\in[1,n]}, \mathsf{pk}) \hookleftarrow \mathsf{KGen}(\mathsf{pp}, n, t)$,

for all $[m] \in \mathcal{M}$,

for all $T \subseteq [1, n]$ s.t. $|T| \geq t$,

$$\mathsf{Verify}(\mathsf{pp}, \mathsf{pk}, [m], \mathsf{CombineSign}(\mathsf{pp}, T, \{\mathsf{ParSign}(\mathsf{pp}, \mathsf{sk}_i, [m])\}_{i\in T})) = 1$$

Security Definitions
Non-Adaptive Security

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.

Security Definitions
Non-Adaptive Security

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.
- $\mathcal{A}$ does not make any signature oracle queries on m^*.

Security Definitions
Non-Adaptive Security

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.
- $\mathcal{A}$ does not make any signature oracle queries on m^*.

- TS-UF-0:
  - The adversary $\mathcal{A}$ has access to O_{ParSign} oracle.
  - To show $\Pr[\mathsf{Exp}_{\mathsf{TSPS}}^{\mathsf{TS\text{-}UF\text{-}0}}(1^\lambda, \mathcal{A}) \rightarrow 1] = \mathsf{neg}(\lambda)$ in the following game:

Security Definitions
Non-Adaptive Security

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.
- $\mathcal{A}$ does not make any signature oracle queries on m^*.

- TS-UF-0:
  - The adversary $\mathcal{A}$ has access to O_{ParSign} oracle.
  - To show $\Pr[\mathsf{Exp}^{\mathsf{TS\text{-}UF\text{-}0}}_{\mathsf{TSPS}}(1^\lambda, \mathcal{A}) \to 1] = \mathsf{neg}(\lambda)$ in the following game:

$\underline{\mathsf{Exp}^{\mathsf{TS\text{-}UF\text{-}0}}_{\mathsf{TSPS}}(1^\lambda, \mathcal{A})}$
$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$
$(n, t, \mathsf{CS}) \hookleftarrow \mathcal{A}(\mathsf{pp})$ s.t. $\lvert\mathsf{CS}\rvert < t$
$\mathsf{HS} := [1, n] \setminus \mathsf{CS}$
$(\mathsf{vk}, \{\mathsf{sk}_i\}_{i\in[1,n]}, \{\mathsf{vk}_i\}_{i\in[1,n]}) \hookleftarrow \mathsf{KGen}(\mathsf{pp}, n, t)$
$([m^*], \Sigma^*) \hookleftarrow \mathcal{A}^{O_{\mathsf{ParSign}}(\cdot)}(\mathsf{vk}, \{\mathsf{sk}_i\}_{i\in\mathsf{CS}}, \{\mathsf{vk}_i\}_{i\in[1,n]})$
Return $\mathsf{Verify}(\mathsf{pp}, \mathsf{pk}, [m^*], \Sigma^*) \wedge ([m^*], \cdot) \notin Q_{\mathsf{ParSign}}$

O_{ParSign} maintains list of $([m_i], j)$ in Q_{ParSign}.

Security Definitions

Non-Adaptive Security

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.

Security Definitions

Non-Adaptive Security

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.
- $\mathcal{A}$ makes limited number of signature oracle queries on m^*.

Security Definitions
Non-Adaptive Security

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.
- $\mathcal{A}$ makes limited number of signature oracle queries on m^*.

- TS-UF-1:
  - The adversary $\mathcal{A}$ has access to O_{ParSign} oracle.
  - To show $\Pr[\mathsf{Exp}^{\text{TS-UF-1}}_{\text{TSPS}}(1^\lambda, \mathcal{A}) \to 1] = \mathsf{neg}(\lambda)$ in the following game:

Security Definitions

Non-Adaptive Security

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.
- $\mathcal{A}$ makes limited number of signature oracle queries on m^*.

- TS-UF-1:
  - The adversary $\mathcal{A}$ has access to O_{ParSign} oracle.
  - To show $\Pr[\mathsf{Exp}_{\mathsf{TSPS}}^{\mathsf{TS\text{-}UF\text{-}1}}(1^\lambda, \mathcal{A}) \to 1] = \mathsf{neg}(\lambda)$ in the following game:

$\underline{\mathsf{Exp}_{\mathsf{TSPS}}^{\mathsf{TS\text{-}UF\text{-}1}}(1^\lambda, \mathcal{A})}$
$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$
$(n, t, \mathsf{CS}) \hookleftarrow \mathcal{A}(\mathsf{pp})$ s.t. $\lvert\mathsf{CS}\rvert < t$
$\mathsf{HS} := [1, n] \setminus \mathsf{CS}$
$(\mathsf{vk}, \{\mathsf{sk}_i\}_{i \in [1,n]}, \{\mathsf{vk}_i\}_{i \in [1,n]}) \hookleftarrow \mathsf{KGen}(\mathsf{pp}, n, t)$
$([m^*], \Sigma^*) \hookleftarrow \mathcal{A}^{O_{\mathsf{ParSign}}(\cdot)}(\mathsf{vk}, \{\mathsf{sk}_i\}_{i \in \mathsf{CS}}, \{\mathsf{vk}_i\}_{i \in [1,n]})$
Return $\mathsf{Verify}(\mathsf{pp}, \mathsf{pk}, [m^*], \Sigma^*) \wedge \lvert([m^*], \cdot) \cap Q_{\mathsf{ParSign}}\rvert < t - \lvert\mathsf{CS}\rvert$

O_{ParSign} maintains list of $([m_i], j)$ in Q_{ParSign}.

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.
- $\mathcal{A}$ makes limited number of signature oracle queries on m^*

Security Definitions
Adaptive Security

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.
- $\mathcal{A}$ makes limited number of signature oracle queries on m^*
- and $\mathcal{A}$ can corrupt limited number of parties.

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.
- $\mathcal{A}$ makes limited number of signature oracle queries on m^*
- and $\mathcal{A}$ can corrupt limited number of parties.

- adp-TS-UF-1:
  - The adversary $\mathcal{A}$ has access to $O_{\mathsf{ParSign}}, O_{\mathsf{Corrupt}}$ oracle.
  - To show $\Pr[\mathsf{Exp}_{\mathsf{TSPS}}^{\text{adp-TS-UF-1}}(1^\lambda, \mathcal{A}) \to 1] = \mathsf{neg}(\lambda)$ in the following game:

- Requirement: A signature cannot be forged by any ppt adversary $\mathcal{A}$.
- $\mathcal{A}$ makes limited number of signature oracle queries on m^*
- and $\mathcal{A}$ can corrupt limited number of parties.

- adp-TS-UF-1:
  - The adversary $\mathcal{A}$ has access to $O_{\text{ParSign}}, O_{\text{Corrupt}}$ oracle.
  - To show $\Pr[\text{Exp}_{\text{TSPS}}^{\text{adp-TS-UF-1}}(1^\lambda, \mathcal{A}) \to 1] = \text{neg}(\lambda)$ in the following game:

$\underline{\text{Exp}_{\text{TSPS}}^{\text{adp-TS-UF-1}}(1^\lambda, \mathcal{A})}$
$\text{pp} \leftarrow \text{Setup}(1^\lambda)$
$(n, t, \text{CS}) \hookleftarrow \mathcal{A}(\text{pp})$ s.t. $\lvert\text{CS}\rvert < t$
$\text{HS} := [1, n] \setminus \text{CS}$
$(\text{vk}, \{\text{sk}_i\}_{i \in [1,n]}, \{\text{vk}_i\}_{i \in [1,n]}) \hookleftarrow \text{KGen}(\text{pp}, n, t)$
$([m^*], \Sigma^*) \hookleftarrow \mathcal{A}^{O_{\text{ParSign}}(\cdot), O_{\text{Corrupt}}(\cdot)}(\text{vk}, \{\text{sk}_i\}_{i \in \text{CS}}, \{\text{vk}_i\}_{i \in [1,n]})$
Return $\text{Verify}(\text{pp}, \text{pk}, [m^*], \Sigma^*) \wedge \lvert\{i : ([m^*], i) \in Q_{\text{ParSign}}\} \cup \text{CS}\rvert < t$

$O_{\text{ParSign}}, O_{\text{Corrupt}}$ maintain lists of $([m_i], j)$ and sk_j in Q_{ParSign} and CS respectively.

Scenario

Suppose. $n = 8, t = 5$.

	1	2	3	4	5	6	7	8
m_1	$\Sigma_1^{(1)}$	$\Sigma_2^{(1)}$	$\Sigma_3^{(1)}$	$\Sigma_4^{(1)}$	$\Sigma_5^{(1)}$	$\Sigma_6^{(1)}$	$\Sigma_7^{(1)}$	$\Sigma_8^{(1)}$
m_2	$\Sigma_1^{(2)}$	$\Sigma_2^{(2)}$	$\Sigma_3^{(2)}$	$\Sigma_4^{(2)}$	$\Sigma_5^{(2)}$	$\Sigma_6^{(2)}$	$\Sigma_7^{(2)}$	$\Sigma_8^{(2)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
m_i	$\Sigma_1^{(i)}$	$\Sigma_2^{(i)}$	$\Sigma_3^{(i)}$	$\Sigma_4^{(i)}$	$\Sigma_5^{(i)}$	$\Sigma_6^{(i)}$	$\Sigma_7^{(i)}$	$\Sigma_8^{(i)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
m_q	$\Sigma_1^{(q)}$	$\Sigma_2^{(q)}$	$\Sigma_3^{(q)}$	$\Sigma_4^{(q)}$	$\Sigma_5^{(q)}$	$\Sigma_6^{(q)}$	$\Sigma_7^{(q)}$	$\Sigma_8^{(q)}$

Intuition

Suppose. $n = 8, t = 5$.

- Let the adversary $\mathcal{A}$ corrupts user 7 and 8.

	1	2	3	4	5	6	7	8
m_1	$\Sigma_1^{(1)}$	$\Sigma_2^{(1)}$	$\Sigma_3^{(1)}$	$\Sigma_4^{(1)}$	$\Sigma_5^{(1)}$	$\Sigma_6^{(1)}$		
m_2	$\Sigma_1^{(2)}$	$\Sigma_2^{(2)}$	$\Sigma_3^{(2)}$	$\Sigma_4^{(2)}$	$\Sigma_5^{(2)}$	$\Sigma_6^{(2)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	sk_7	sk_8
m_i	$\Sigma_1^{(i)}$	$\Sigma_2^{(i)}$	$\Sigma_3^{(i)}$	$\Sigma_4^{(i)}$	$\Sigma_5^{(i)}$	$\Sigma_6^{(i)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
m_q	$\Sigma_1^{(q)}$	$\Sigma_2^{(q)}$	$\Sigma_3^{(q)}$	$\Sigma_4^{(q)}$	$\Sigma_5^{(q)}$	$\Sigma_6^{(q)}$		

Intuition

Suppose. $n = 8, t = 5$.

- Let the adversary $\mathcal{A}$ corrupts user 7 and 8.
- If it gets partial signatures $\Sigma_4^{(1)}$, $\Sigma_5^{(1)}$ and $\Sigma_6^{(1)}$, $\mathcal{A}$ can forge $\Sigma^{(1)}$.

	1	2	3	4	5	6	7	8
m_1	$\Sigma_1^{(1)}$	$\Sigma_2^{(1)}$	$\Sigma_3^{(1)}$	$\Sigma_4^{(1)}$	$\Sigma_5^{(1)}$	$\Sigma_6^{(1)}$		
m_2	$\Sigma_1^{(2)}$	$\Sigma_2^{(2)}$	$\Sigma_3^{(2)}$	$\Sigma_4^{(2)}$	$\Sigma_5^{(2)}$	$\Sigma_6^{(2)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	sk_7	sk_8
m_i	$\Sigma_1^{(i)}$	$\Sigma_2^{(i)}$	$\Sigma_3^{(i)}$	$\Sigma_4^{(i)}$	$\Sigma_5^{(i)}$	$\Sigma_6^{(i)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
m_q	$\Sigma_1^{(q)}$	$\Sigma_2^{(q)}$	$\Sigma_3^{(q)}$	$\Sigma_4^{(q)}$	$\Sigma_5^{(q)}$	$\Sigma_6^{(q)}$		

Intuition

Suppose. $n = 8, t = 5$.

- Let the adversary $\mathcal{A}$ corrupts user 7 and 8.
- If it gets partial signatures $\Sigma_4^{(1)}$, $\Sigma_5^{(1)}$ and $\Sigma_6^{(1)}$, $\mathcal{A}$ can forge $\Sigma^{(1)}$.
- Non-trivial goals:
  1. $m^* \notin \{m_2, \ldots, m_q\}$.
  2. $m^* \in \{m_2, \ldots, m_q\}$. Let $m^* = m_i$.
     2.1 $\mathcal{A}$ can't corrupt any more users.
     2.2 $\mathcal{A}$ can corrupt more users.

	1	2	3	4	5	6	7	8
m_1	$\Sigma_1^{(1)}$	$\Sigma_2^{(1)}$	$\Sigma_3^{(1)}$	$\Sigma_4^{(1)}$	$\Sigma_5^{(1)}$	$\Sigma_6^{(1)}$		
m_2	$\Sigma_1^{(2)}$	$\Sigma_2^{(2)}$	$\Sigma_3^{(2)}$	$\Sigma_4^{(2)}$	$\Sigma_5^{(2)}$	$\Sigma_6^{(2)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	sk_7	sk_8
m_i	$\Sigma_1^{(i)}$	$\Sigma_2^{(i)}$	$\Sigma_3^{(i)}$	$\Sigma_4^{(i)}$	$\Sigma_5^{(i)}$	$\Sigma_6^{(i)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
m_q	$\Sigma_1^{(q)}$	$\Sigma_2^{(q)}$	$\Sigma_3^{(q)}$	$\Sigma_4^{(q)}$	$\Sigma_5^{(q)}$	$\Sigma_6^{(q)}$		

Intuition (Cont.)

- Consider an Uf-CMA-secure signature Σ.

	1	2	3	4	5	6	7	8
m_1	$\Sigma_1^{(1)}$	$\Sigma_2^{(1)}$	$\Sigma_3^{(1)}$	$\Sigma_4^{(1)}$	$\Sigma_5^{(1)}$	$\Sigma_6^{(1)}$		
m_2	$\Sigma_1^{(2)}$	$\Sigma_2^{(2)}$	$\Sigma_3^{(2)}$	$\Sigma_4^{(2)}$	$\Sigma_5^{(2)}$	$\Sigma_6^{(2)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	sk_7	sk_8
m_i	$\Sigma_1^{(i)}$	$\Sigma_2^{(i)}$	$\Sigma_3^{(i)}$	$\Sigma_4^{(i)}$	$\Sigma_5^{(i)}$	$\Sigma_6^{(i)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
m_q	$\Sigma_1^{(q)}$	$\Sigma_2^{(q)}$	$\Sigma_3^{(q)}$	$\Sigma_4^{(q)}$	$\Sigma_5^{(q)}$	$\Sigma_6^{(q)}$		

Intuition (Cont.)

- Consider an Uf-CMA-secure signature Σ.
- Forging $\Sigma_6^{(i)}$ is hard for $\mathcal{A}$ even when $\left\{\Sigma_6^{(i)}\right\}_{i\in[q]\setminus\{i\}}$ are given.

	1	2	3	4	5	6	7	8
m_1	$\Sigma_1^{(1)}$	$\Sigma_2^{(1)}$	$\Sigma_3^{(1)}$	$\Sigma_4^{(1)}$	$\Sigma_5^{(1)}$	$\Sigma_6^{(1)}$		
m_2	$\Sigma_1^{(2)}$	$\Sigma_2^{(2)}$	$\Sigma_3^{(2)}$	$\Sigma_4^{(2)}$	$\Sigma_5^{(2)}$	$\Sigma_6^{(2)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	sk_7	sk_8
m_i	$\Sigma_1^{(i)}$	$\Sigma_2^{(i)}$	$\Sigma_3^{(i)}$	$\Sigma_4^{(i)}$	$\Sigma_5^{(i)}$	$\Sigma_6^{(i)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
m_q	$\Sigma_1^{(q)}$	$\Sigma_2^{(q)}$	$\Sigma_3^{(q)}$	$\Sigma_4^{(q)}$	$\Sigma_5^{(q)}$	$\Sigma_6^{(q)}$		

Intuition (Cont.)

- Consider an Uf-CMA-secure signature Σ.
- Forging $\Sigma_6^{(i)}$ is hard for $\mathcal{A}$ even when $\left\{\Sigma_6^{(i)}\right\}_{i \in [q] \setminus \{i\}}$ are given.
- Let $\mathcal{A}$ gets $\Sigma_4^{(i)}$ and $\Sigma_5^{(i)}$.

	1	2	3	4	5	6	7	8
m_1	$\Sigma_1^{(1)}$	$\Sigma_2^{(1)}$	$\Sigma_3^{(1)}$	$\Sigma_4^{(1)}$	$\Sigma_5^{(1)}$	$\Sigma_6^{(1)}$		
m_2	$\Sigma_1^{(2)}$	$\Sigma_2^{(2)}$	$\Sigma_3^{(2)}$	$\Sigma_4^{(2)}$	$\Sigma_5^{(2)}$	$\Sigma_6^{(2)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	sk_7	sk_8
m_i	$\Sigma_1^{(i)}$	$\Sigma_2^{(i)}$	$\Sigma_3^{(i)}$	$\Sigma_4^{(i)}$	$\Sigma_5^{(i)}$	$\Sigma_6^{(i)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
m_q	$\Sigma_1^{(q)}$	$\Sigma_2^{(q)}$	$\Sigma_3^{(q)}$	$\Sigma_4^{(q)}$	$\Sigma_5^{(q)}$	$\Sigma_6^{(q)}$		

Intuition (Cont.)

- Consider an Uf-CMA-secure signature Σ.
- Forging $\Sigma_6^{(i)}$ is hard for $\mathcal{A}$ even when $\left\{\Sigma_6^{(i)}\right\}_{i\in[q]\backslash\{i\}}$ are given.
- Let $\mathcal{A}$ gets $\Sigma_4^{(i)}$ and $\Sigma_5^{(i)}$.
- To prove: forging $\Sigma_6^{(i)}$ is still hard.

	1	2	3	4	5	6	7	8
m_1	$\Sigma_1^{(1)}$	$\Sigma_2^{(1)}$	$\Sigma_3^{(1)}$	$\Sigma_4^{(1)}$	$\Sigma_5^{(1)}$	$\Sigma_6^{(1)}$		
m_2	$\Sigma_1^{(2)}$	$\Sigma_2^{(2)}$	$\Sigma_3^{(2)}$	$\Sigma_4^{(2)}$	$\Sigma_5^{(2)}$	$\Sigma_6^{(2)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	sk_7	sk_8
m_i	$\Sigma_1^{(i)}$	$\Sigma_2^{(i)}$	$\Sigma_3^{(i)}$	$\Sigma_4^{(i)}$	$\Sigma_5^{(i)}$	$\Sigma_6^{(i)}$		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		
m_q	$\Sigma_1^{(q)}$	$\Sigma_2^{(q)}$	$\Sigma_3^{(q)}$	$\Sigma_4^{(q)}$	$\Sigma_5^{(q)}$	$\Sigma_6^{(q)}$		

Construction Overview

$$[\text{KPW15}]:\ (\sigma_1,\sigma_2) := \Big(\underbrace{[\![\begin{pmatrix}1 & \boldsymbol{m}^\top\end{pmatrix}]\!]_1\mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top[\![\mathbf{B}^\top(\mathbf{U}+\tau\cdot\mathbf{V})]\!]_1, [\![\mathbf{r}^\top\mathbf{B}^\top]\!]_1}^{\text{randomized PRF}}\Big)$$

Construction Overview

$$[\text{KPW15}]: \ (\sigma_1, \sigma_2) := \Big(\underbrace{[\![(1 \quad \boldsymbol{m}^\top)]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}^\top \mathbf{B}^\top]\!]_1}^{\text{randomized PRF}} \Big)$$

- [KPW15] rejects same τ for different messages.

Construction Overview

$$[\text{KPW15}]: \ (\sigma_1, \sigma_2) := \Big(\underbrace{[\![\begin{pmatrix} 1 & m^\top \end{pmatrix}]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}^\top \mathbf{B}^\top]\!]_1}^{\text{randomized PRF}} \Big)$$

- [KPW15] rejects same τ for different messages.
- [KPW15] is not strong uf-cma secure.
  - i.e. does not allow signature queries on $[\![m^*]\!]_1$.

Construction Overview (contd)

$$[\text{KPW15}]: \ (\sigma_1, \sigma_2) := \Big(\underbrace{[\![\begin{pmatrix} 1 & \mathbf{m}^\top \end{pmatrix}]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}^\top \mathbf{B}^\top]\!]_1}^{\text{randomized PRF}} \Big)$$

Construction Overview (contd)

$$[\text{KPW15}]:\ (\sigma_1, \sigma_2) := \Big(\underbrace{[\![\begin{pmatrix} 1 & m^\top \end{pmatrix}]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}^\top \mathbf{B}^\top]\!]_1}^{\text{randomized PRF}} \Big)$$

- We secret share $\mathbf{K}$ to n parties via (t, n)-Shamir Secret Sharing.
  - Each party has secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.

Construction Overview (contd)

$$[\text{KPW15}]: \ (\sigma_1, \sigma_2) := \Big(\underbrace{[\![(1 \quad m^\top)]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}^\top \mathbf{B}^\top]\!]_1}^{\text{randomized PRF}} \Big)$$

- We secret share $\mathbf{K}$ to n parties via (t, n)-Shamir Secret Sharing.
  - Each party has secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
- For each partial signature, each party can choose it's own $\mathbf{r}_j \hookleftarrow \mathbb{Z}_p^k$.

Construction Overview (contd)

$$[\text{KPW15}]: \ (\sigma_1, \sigma_2) := \Big(\underbrace{[\![\begin{pmatrix} 1 & m^\top \end{pmatrix}]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}^\top \mathbf{B}^\top]\!]_1}^{\text{randomized PRF}} \Big)$$

- We secret share $\mathbf{K}$ to n parties via (t, n)-Shamir Secret Sharing.
  - Each party has secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
- For each partial signature, each party can choose it's own $\mathbf{r}_j \hookleftarrow \mathbb{Z}_p^k$.

$$\Sigma_j^{(i)}: \ (\sigma_1, \sigma_2) := \big([\![\begin{pmatrix} 1 & m_i^\top \end{pmatrix}]\!]_1 \mathbf{K}_j + \mathbf{r}_j^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau_i \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1 \big)$$

Construction Overview (contd)

$$[\text{KPW15}]: \ (\sigma_1, \sigma_2) := \big(\underbrace{[\![(1 \quad m^\top)]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}^\top \mathbf{B}^\top]\!]_1}^{\text{randomized PRF}}\big)$$

- We secret share $\mathbf{K}$ to n parties via (t, n)-Shamir Secret Sharing.
  - Each party has secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
- For each partial signature, each party can choose it's own $\mathbf{r}_j \hookleftarrow \mathbb{Z}_p^k$.

$$\Sigma_j^{(i)}: \ (\sigma_1, \sigma_2) := ([\![(1 \quad m_i^\top)]\!]_1 \mathbf{K}_j + \mathbf{r}_j^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau_i \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1)$$

- Let $S \subseteq [1, n]$ s.t. $|S| \geq t$.

Construction Overview (contd)

$$[\text{KPW15}]: \ (\sigma_1, \sigma_2) := \Big(\underbrace{[\![(1 \quad m^\top)]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}^\top \mathbf{B}^\top]\!]_1}^{\text{randomized PRF}}\Big)$$

- We secret share $\mathbf{K}$ to n parties via (t, n)-Shamir Secret Sharing.
  - Each party has secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
- For each partial signature, each party can choose it's own $\mathbf{r}_j \hookleftarrow \mathbb{Z}_p^k$.

$$\Sigma_j^{(i)}: \ (\sigma_1, \sigma_2) := ([\![(1 \quad m_i^\top)]\!]_1 \mathbf{K}_j + \mathbf{r}_j^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau_i \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1)$$

- Let $S \subseteq [1, n]$ s.t. $|S| \geq t$.
- Let $\{\lambda_j\}_{j \in S}$ are Lagrange polynomials wrt S.

Construction Overview (contd)

$$\text{[KPW15]}: \ (\sigma_1, \sigma_2) := \Big(\underbrace{[\![(1 \quad m^\top)]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}^\top \mathbf{B}^\top]\!]_1}^{\text{randomized PRF}} \Big)$$

- We secret share $\mathbf{K}$ to n parties via (t, n)-Shamir Secret Sharing.
  - Each party has secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
- For each partial signature, each party can choose it's own $\mathbf{r}_j \hookleftarrow \mathbb{Z}_p^k$.

$$\Sigma_j^{(i)}: \ (\sigma_1, \sigma_2) := \big([\![(1 \quad m_i^\top)]\!]_1 \mathbf{K}_j + \mathbf{r}_j^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau_i \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1 \big)$$

- Let $S \subseteq [1, n]$ s.t. $|S| \geq t$.
- Let $\{\lambda_j\}_{j \in S}$ are Lagrange polynomials wrt S.
- Lin combination of $\{\Sigma_j^{(i)}\}_j$ computes $\Sigma^{(i)}$ for $\mathbf{K} = \sum_{j \in S} \lambda_j \mathbf{K}_j$, $\mathbf{r} = \sum_{j \in S} \lambda_j \mathbf{r}_j^\top$

Construction Overview (contd)

$$[\text{KPW15}]: \ (\sigma_1, \sigma_2) := \Big(\underbrace{[\![(1 \quad m^\top)]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}^\top \mathbf{B}^\top]\!]_1}^{\text{randomized PRF}} \Big)$$

- We secret share $\mathbf{K}$ to n parties via (t, n)-Shamir Secret Sharing.
  - Each party has secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
- For each partial signature, each party can choose it's own $\mathbf{r}_j \hookleftarrow \mathbb{Z}_p^k$.

$$\Sigma_j^{(i)}: \ (\sigma_1, \sigma_2) := \big([\![(1 \quad m_i^\top)]\!]_1 \mathbf{K}_j + \mathbf{r}_j^\top [\![\mathbf{B}^\top (\mathbf{U} + \tau_i \cdot \mathbf{V})]\!]_1, [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1 \big)$$

- Let $S \subseteq [1, n]$ s.t. $|S| \geq t$.
- Let $\{\lambda_j\}_{j\in S}$ are Lagrange polynomials wrt S.
- Lin combination of $\{\Sigma_j^{(i)}\}_j$ computes $\Sigma^{(i)}$ for $\mathbf{K} = \sum_{j\in S} \lambda_j \mathbf{K}_j$, $\mathbf{r} = \sum_{j\in S} \lambda_j \mathbf{r}_j^\top$
  - provided partial signatures on (j, m_i) use same τ_i,

Construction Overview (contd)

$$[\text{KPW15}]:\ (\sigma_1,\sigma_2) := \Big(\underbrace{[\![(1 \quad m^\top)]\!]_1 \mathbf{K}}_{\text{SP-OTS}} + \overbrace{\mathbf{r}^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau\cdot\mathbf{V})]\!]_1, [\![\mathbf{r}^\top\mathbf{B}^\top]\!]_1}^{\text{randomized PRF}}\Big)$$

- We secret share $\mathbf{K}$ to n parties via (t, n)-Shamir Secret Sharing.
  - Each party has secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
- For each partial signature, each party can choose it's own $\mathbf{r}_j \hookleftarrow \mathbb{Z}_p^k$.

$$\Sigma_j^{(i)}:\ (\sigma_1,\sigma_2) := ([\![(1 \quad m_i^\top)]\!]_1\mathbf{K}_j + \mathbf{r}_j^\top[\![\mathbf{B}^\top(\mathbf{U} + \tau_i\cdot\mathbf{V})]\!]_1, [\![\mathbf{r}_j^\top\mathbf{B}^\top]\!]_1)$$

- Let $S \subseteq [1, n]$ s.t. $|S| \geq t$.
- Let $\{\lambda_j\}_{j\in S}$ are Lagrange polynomials wrt S.
- Lin combination of $\{\Sigma_j^{(i)}\}_j$ computes $\Sigma^{(i)}$ for $\mathbf{K} = \sum_{j\in S}\lambda_j\mathbf{K}_j$, $\mathbf{r} = \sum_{j\in S}\lambda_j\mathbf{r}_j^\top$
  - provided partial signatures on (j, m_i) use same τ_i,
  - proof works if $\tau_t \neq \tau_i$ for all $m_t \neq m_i$.

Setup(1^λ)

$\mathbf{A}, \mathbf{B} \leftarrow \mathbb{Z}_p^{(k+1)\times k}$

$\mathbf{U}, \mathbf{V} \leftarrow \mathbb{Z}_p^{(k+1)\times(k+1)}$.

$\mathsf{pp} := ([\![\mathbf{A}]\!]_2, [\![\mathbf{UA}]\!]_2, [\![\mathbf{VA}]\!]_2, [\![\mathbf{B}]\!]_1, [\![\mathbf{B}^\top\mathbf{U}]\!]_1, [\![\mathbf{B}^\top\mathbf{V}]\!]_1)$

ParSign($\mathsf{pp}, \mathsf{sk}_i, [\![m]\!]_1$)

$\mathbf{r}_i \leftarrow \mathbb{Z}_p^k$

$\tau := \mathcal{H}([\![m]\!]_1)$

Output $\Sigma_i := (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ s.t.

$\sigma_1 := [\![(1 \quad m^\top)]\!]_1\mathbf{K}_i + \mathbf{r}_i^\top[\![\mathbf{B}^\top(\mathbf{U}+\tau\mathbf{V})]\!]_1$

$\sigma_2 := [\![\mathbf{r}_i^\top\mathbf{B}^\top]\!]_1$

$\sigma_3 := [\![\tau\mathbf{r}_i^\top\mathbf{B}^\top]\!]_1$

$\sigma_4 := [\![\tau]\!]_2$

ParVerify($\mathsf{pp}, \mathsf{pk}_i, [\![m]\!]_1, \Sigma_i$)

Let $R = e(\sigma_1, [\![\mathbf{A}]\!]_2)$

Let $S_1 = e([\![(1 \quad m^\top)]\!]_1, \mathsf{pk}_i)$

Let $S_2 = e(\sigma_2, [\![\mathbf{UA}]\!]_2) \cdot e(\sigma_3, [\![\mathbf{VA}]\!]_2)$

Check $R = S_1 \cdot S_2$

Check $e(\sigma_2, \sigma_4) = e(\sigma_3, [\![1]\!]_2)$

KGen(pp, n, t)

$\mathbf{K} \leftarrow \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.

$\mathbf{K}_1, \ldots, \mathbf{K}_n \leftarrow \mathsf{Shr}(\mathbf{K}, \mathbb{Z}_p^{(\ell+1)\times(k+1)}, n, t)$.

Set $\mathsf{pk} := [\![\mathbf{KA}]\!]_2$.

Set $(\mathsf{sk}_i, \mathsf{pk}_i) := (\mathbf{K}_i, [\![\mathbf{K}_i\mathbf{A}]\!]_2), \forall i \in [n]$.

CombineSign($\mathsf{pp}, S, \{\Sigma_i\}_{i\in S}$)

Parse $\Sigma_i = (\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_4)$ for all $i \in S$.

Let Lagrange polynomials λ_i for $i \in S$.

Output $\Sigma := (\widehat{\sigma}_1, \widehat{\sigma}_2, \widehat{\sigma}_3, \widehat{\sigma}_4)$ s.t.

$\widehat{\sigma}_1 := \prod_{i\in S} \sigma_{i,1}^{\lambda_i}$

$= [\![(1 \quad m^\top)\,\mathbf{K}]\!]_1 + \mathbf{r}^\top[\![\mathbf{B}^\top(\mathbf{U}+\tau\mathbf{V})]\!]_1$

$\widehat{\sigma}_2 := \prod_{i\in S} \sigma_{i,2}^{\lambda_i} = [\![\mathbf{r}^\top\mathbf{B}^\top]\!]_1$

$\widehat{\sigma}_3 := \prod_{i\in S} \sigma_{i,3}^{\lambda_i} = [\![\tau\mathbf{r}^\top\mathbf{B}^\top]\!]_1$

$\widehat{\sigma}_4 := \sigma_4$

Verify($\mathsf{pp}, \mathsf{pk}, [\![m]\!]_1, \Sigma$)

Let $R = e(\widehat{\sigma}_1, [\![\mathbf{A}]\!]_2)$

Let $S_1 = e([\![(1 \quad m^\top)]\!]_1, \mathsf{pk})$

Let $S_2 = e(\widehat{\sigma}_2, [\![\mathbf{UA}]\!]_2) \cdot e(\widehat{\sigma}_3, [\![\mathbf{VA}]\!]_2)$

Check $R = S_1 \cdot S_2$

Check $e(\widehat{\sigma}_2, \widehat{\sigma}_4) = e(\widehat{\sigma}_3, [\![1]\!]_2)$

Figure: Our Construction: TSPS for $k \geq 1$

Proof Intuition

- Each party has a secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
  - [KPW15] ensures $\mathbf{K}_j$ has residual entropy $\mathbf{k}_j \in \mathbb{Z}_p^{(\ell+1)}$.

Proof Intuition

- Each party has a secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
  - [KPW15] ensures $\mathbf{K}_j$ has residual entropy $\mathbf{k}_j \in \mathbb{Z}_p^{(\ell+1)}$.
  - Even after partial signatures on $[\![m_t]\!]_1 \neq [\![m^*]\!]_1$.

Proof Intuition

- Each party has a secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
  - [KPW15] ensures $\mathbf{K}_j$ has residual entropy $\mathbf{k}_j \in \mathbb{Z}_p^{(\ell+1)}$.
  - Even after partial signatures on $[\![m_t]\!]_1 \neq [\![m^*]\!]_1$.
- Shamir Secret Sharing is information-theoretically secure.
  - We focus on the effect of SSS on residual entropies.

Proof Intuition

- Each party has a secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
  - [KPW15] ensures $\mathbf{K}_j$ has residual entropy $\mathbf{k}_j \in \mathbb{Z}_p^{(\ell+1)}$.
  - Even after partial signatures on $[\![m_t]\!]_1 \neq [\![m^*]\!]_1$.
- Shamir Secret Sharing is information-theoretically secure.
  - We focus on the effect of SSS on residual entropies.
  - $\{\mathbf{k}_j\}_{j \in T}$ for $T = \{4, 5, 7, 8\}$, hides $\mathbf{k}_6$.

Proof Intuition

- Each party has a secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
  - [KPW15] ensures $\mathbf{K}_j$ has residual entropy $\mathbf{k}_j \in \mathbb{Z}_p^{(\ell+1)}$.
  - Even after partial signatures on $[\![m_t]\!]_1 \neq [\![m^*]\!]_1$.

- Shamir Secret Sharing is information-theoretically secure.
  - We focus on the effect of SSS on residual entropies.
  - $\{\mathbf{k}_j\}_{j \in T}$ for $T = \{4, 5, 7, 8\}$, hides $\mathbf{k}_6$.
  - Even when $\{\mathbf{K}_j\}_{j \in T}$ are leaked adaptively.

Proof Intuition

- Each party has a secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
  - [KPW15] ensures $\mathbf{K}_j$ has residual entropy $\mathbf{k}_j \in \mathbb{Z}_p^{(\ell+1)}$.
  - Even after partial signatures on $[\![m_t]\!]_1 \neq [\![m^*]\!]_1$.
- Shamir Secret Sharing is information-theoretically secure.
  - We focus on the effect of SSS on residual entropies.
  - $\{\mathbf{k}_j\}_{j\in T}$ for $T = \{4, 5, 7, 8\}$, hides $\mathbf{k}_6$.
  - Even when $\{\mathbf{K}_j\}_{j\in T}$ are leaked adaptively.
- [KPW15] allows the reduction to know $\mathbf{K}$.
  - We could allow the reduction to know $\{\mathbf{K}_j\}_{j\in[n]}$.

Proof Intuition

- Each party has a secret key $\mathbf{K}_j \in \mathbb{Z}_p^{(\ell+1)\times(k+1)}$.
  - [KPW15] ensures $\mathbf{K}_j$ has residual entropy $\mathbf{k}_j \in \mathbb{Z}_p^{(\ell+1)}$.
  - Even after partial signatures on $[\![m_t]\!]_1 \neq [\![m^*]\!]_1$.
- Shamir Secret Sharing is information-theoretically secure.
  - We focus on the effect of SSS on residual entropies.
  - $\left\{\mathbf{k}_j\right\}_{j\in T}$ for $T = \{4, 5, 7, 8\}$, hides $\mathbf{k}_6$.
  - Even when $\left\{\mathbf{K}_j\right\}_{j\in T}$ are leaked adaptively.
- [KPW15] allows the reduction to know $\mathbf{K}$.
  - We could allow the reduction to know $\left\{\mathbf{K}_j\right\}_{j\in[n]}$.
  - This allowed us to handle adaptive corruptions.

adp-TS-UF-1 **Security via a Hybrid Argument**

- Game_0. Real.

- Game_0. Real.

- Game_1. We change Verify to Verify* where,

Verify(pp, pk, $[\![m]\!]_1, \Sigma^*$)	Verify*(pp, vk, $[\![m^*]\!]_1, \Sigma^*$):
1: Parse Σ^* as $(\widehat{\sigma}_1, \widehat{\sigma}_2, \widehat{\sigma}_3, \widehat{\sigma}_4)$.	1: Parse Σ^* as $(\widehat{\sigma}_1, \widehat{\sigma}_2, \widehat{\sigma}_3, \widehat{\sigma}_4)$.
2: Let $R = e(\widehat{\sigma}_1, [\![\mathbf{A}]\!]_2)$	2: Let $R = e(\widehat{\sigma}_1, [\![1]\!]_2)$
3: Let $S_1 = e([\![(1 \quad m^\top)]\!]_1, \mathrm{pk})$	3: Let $S_1 = e([\![(1 \quad m^\top)]\!]_1, [\![\mathbf{K}]\!]_2)$
4: Let $S_2 = e(\widehat{\sigma}_2, [\![\mathbf{UA}]\!]_2) \cdot e(\widehat{\sigma}_3, [\![\mathbf{VA}]\!]_2)$	4: Let $S_2 = e(\widehat{\sigma}_2, [\![\mathbf{U}]\!]_2) \cdot e(\widehat{\sigma}_3, [\![\mathbf{V}]\!]_2)$
5: Check $R = S_1 \cdot S_2$	5: Check $R = S_1 \cdot S_2$
6: Check $e(\widehat{\sigma}_2, \widehat{\sigma}_4) = e(\widehat{\sigma}_3, [\![1]\!]_2)$	6: Check $e(\widehat{\sigma}_2, \widehat{\sigma}_4) = e(\widehat{\sigma}_3, [\![1]\!]_2)$

adp-TS-UF-1 **Security via a Hybrid Argument**

- Game_0. Real.

- Game_1. We change Verify to Verify* where,

$\mathsf{Verify}(\mathsf{pp}, \mathsf{pk}, [\![m]\!]_1, \Sigma^*)$	$\mathsf{Verify}^*(\mathsf{pp}, \mathsf{vk}, [\![m^*]\!]_1, \Sigma^*)$:
1: Parse Σ^* as $(\widehat{\sigma}_1, \widehat{\sigma}_2, \widehat{\sigma}_3, \widehat{\sigma}_4)$.	1: Parse Σ^* as $(\widehat{\sigma}_1, \widehat{\sigma}_2, \widehat{\sigma}_3, \widehat{\sigma}_4)$.
2: Let $R = e(\widehat{\sigma}_1, [\![\mathbf{A}]\!]_2)$	2: Let $R = e(\widehat{\sigma}_1, [\![1]\!]_2)$
3: Let $S_1 = e([\![(1 \quad m^\top)]\!]_1, \mathsf{pk})$	3: Let $S_1 = e([\![(1 \quad m^\top)]\!]_1, [\![\mathbf{K}]\!]_2)$
4: Let $S_2 = e(\widehat{\sigma}_2, [\![\mathbf{UA}]\!]_2) \cdot e(\widehat{\sigma}_3, [\![\mathbf{VA}]\!]_2)$	4: Let $S_2 = e(\widehat{\sigma}_2, [\![\mathbf{U}]\!]_2) \cdot e(\widehat{\sigma}_3, [\![\mathbf{V}]\!]_2)$
5: Check $R = S_1 \cdot S_2$	5: Check $R = S_1 \cdot S_2$
6: Check $e(\widehat{\sigma}_2, \widehat{\sigma}_4) = e(\widehat{\sigma}_3, [\![1]\!]_2)$	6: Check $e(\widehat{\sigma}_2, \widehat{\sigma}_4) = e(\widehat{\sigma}_3, [\![1]\!]_2)$

- Game_2. If two m_i, m_j queried have same hash value, we abort.

adp-TS-UF-1 **Security via a Hybrid Argument**

- Game_0. Real.

- Game_1. We change Verify to Verify* where,

$\mathsf{Verify}(\mathsf{pp}, \mathsf{pk}, [\![m]\!]_1, \Sigma^*)$	$\mathsf{Verify}^*(\mathsf{pp}, \mathsf{vk}, [\![m^*]\!]_1, \Sigma^*)$:
Parse Σ^* as $(\widehat{\sigma}_1, \widehat{\sigma}_2, \widehat{\sigma}_3, \widehat{\sigma}_4)$.	Parse Σ^* as $(\widehat{\sigma}_1, \widehat{\sigma}_2, \widehat{\sigma}_3, \widehat{\sigma}_4)$.
Let $R = e(\widehat{\sigma}_1, [\![\mathbf{A}]\!]_2)$	Let $R = e(\widehat{\sigma}_1, [\![1]\!]_2)$
Let $S_1 = e([\![(1 \quad m^\top)]\!]_1, \mathsf{pk})$	Let $S_1 = e([\![(1 \quad m^\top)]\!]_1, [\![\mathbf{K}]\!]_2)$
Let $S_2 = e(\widehat{\sigma}_2, [\![\mathbf{UA}]\!]_2) \cdot e(\widehat{\sigma}_3, [\![\mathbf{VA}]\!]_2)$	Let $S_2 = e(\widehat{\sigma}_2, [\![\mathbf{U}]\!]_2) \cdot e(\widehat{\sigma}_3, [\![\mathbf{V}]\!]_2)$
Check $R = S_1 \cdot S_2$	Check $R = S_1 \cdot S_2$
Check $e(\widehat{\sigma}_2, \widehat{\sigma}_4) = e(\widehat{\sigma}_3, [\![1]\!]_2)$	Check $e(\widehat{\sigma}_2, \widehat{\sigma}_4) = e(\widehat{\sigma}_3, [\![1]\!]_2)$

- Game_2. If two m_i, m_j queried have same hash value, we abort.

- Game_3. If our guess $[\![m^*]\!]_1$ among $[\![m_1]\!]_1, \ldots, [\![m_Q]\!]_1$ is incorrect, we abort.

- Game$_4$. We change ParSign to ParSign* where,

ParSign$(\mathsf{pp}, \mathsf{sk}_j, [\![m]\!]_1)$	ParSign$^*(\mathsf{pp}, \mathsf{sk}_j, [\![m]\!]_1)$
1: $\mathbf{r}_j \leftarrow \mathbb{Z}_p^k$	1: $\mathbf{r}_j \leftarrow \mathbb{Z}_p^k$
2: $\tau := \mathcal{H}([\![m]\!]_1)$	2: $\tau := \mathcal{H}([\![m]\!]_1)$
3: Output $\Sigma_j := (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ s.t.	3: $\boxed{\text{If } [\![m]\!]_1 = [\![m^*]\!]_1, \text{ set } \mu = 0.}$
$\sigma_1 := [\![(1 \quad m^\top)]\!]_1 \mathbf{K}_j + \mathbf{r}_j^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau\mathbf{V})]\!]_1$	4: Output $\Sigma_j := (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ s.t.
$\sigma_2 := [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$	$\sigma_1 := [\![(1 \quad m^\top)]\!]_1 \mathbf{K}_j + [\![\mu \mathbf{a}^\perp]\!]_1 + \mathbf{r}_j^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau\mathbf{V})]\!]_1$
$\sigma_3 := [\![\tau \mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$	$\sigma_2 := [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$
$\sigma_4 := [\![\tau]\!]_2$	$\sigma_3 := [\![\tau \mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$
	$\sigma_4 := [\![\tau]\!]_2$

adp-TS-UF-1 **Security via a Hybrid Argument**

- Game_4. We change $\mathsf{ParSign}$ to $\mathsf{ParSign}^*$ where,

$\underline{\mathsf{ParSign}(\mathsf{pp}, \mathsf{sk}_j, [\![m]\!]_1)}$

$\mathbf{r}_j \leftarrow \mathbb{Z}_p^k$

$\tau := \mathcal{H}([\![m]\!]_1)$

Output $\Sigma_j := (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ s.t.

$\sigma_1 := [\![(1 \quad m^\top)]\!]_1 \mathbf{K}_j + \mathbf{r}_j^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau \mathbf{V})]\!]_1$

$\sigma_2 := [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$

$\sigma_3 := [\![\tau \mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$

$\sigma_4 := [\![\tau]\!]_2$

$\underline{\mathsf{ParSign}^*(\mathsf{pp}, \mathsf{sk}_j, [\![m]\!]_1)}$

$\mathbf{r}_j \leftarrow \mathbb{Z}_p^k$

$\tau := \mathcal{H}([\![m]\!]_1)$

$\boxed{\text{If } [\![m]\!]_1 = [\![m^*]\!]_1, \text{ set } \mu = 0.}$

Output $\Sigma_j := (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ s.t.

$\sigma_1 := [\![(1 \quad m^\top)]\!]_1 \mathbf{K}_j + [\![\mu \mathbf{a}^\perp]\!]_1 + \mathbf{r}_j^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau \mathbf{V})]\!]_1$

$\sigma_2 := [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$

$\sigma_3 := [\![\tau \mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$

$\sigma_4 := [\![\tau]\!]_2$

- Game_5. Here, we sample $\widetilde{\mathbf{K}}_j \leftarrow \mathbb{Z}_p^{(\ell+1)\times(k+1)}, \mathbf{k}_j \leftarrow \mathbb{Z}_p^{\ell+1}$ for $i \in [1, n]$.
  - We set $\mathbf{K}_j = \widetilde{\mathbf{K}}_j + \mathbf{k}_j \mathbf{a}^\perp$ for $i \in [1, n]$.

adp-TS-UF-1 **Security via a Hybrid Argument**

- Game_4. We change ParSign to ParSign* where,

ParSign(pp, sk$_j$, $[\![m]\!]_1$)	ParSign*(pp, sk$_j$, $[\![m]\!]_1$)
1: $\mathbf{r}_j \hookleftarrow \mathbb{Z}_p^k$	1: $\mathbf{r}_j \hookleftarrow \mathbb{Z}_p^k$
2: $\tau := \mathcal{H}([\![m]\!]_1)$	2: $\tau := \mathcal{H}([\![m]\!]_1)$
3: Output $\Sigma_j := (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ s.t.	3: If $[\![m]\!]_1 = [\![m^*]\!]_1$, set $\mu = 0$.
$\sigma_1 := [\![(1 \quad m^\top)]\!]_1 \mathbf{K}_j + \mathbf{r}_j^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau\mathbf{V})]\!]_1$	4: Output $\Sigma_j := (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ s.t.
$\sigma_2 := [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$	$\sigma_1 := [\![(1 \quad m^\top)]\!]_1 \mathbf{K}_j + [\![\mu \mathbf{a}^\perp]\!]_1 + \mathbf{r}_j^\top [\![\mathbf{B}^\top(\mathbf{U} + \tau\mathbf{V})]\!]_1$
$\sigma_3 := [\![\tau \mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$	$\sigma_2 := [\![\mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$
$\sigma_4 := [\![\tau]\!]_2$	$\sigma_3 := [\![\tau \mathbf{r}_j^\top \mathbf{B}^\top]\!]_1$
	$\sigma_4 := [\![\tau]\!]_2$

- Game_5. Here, we sample $\widetilde{\mathbf{K}}_j \hookleftarrow \mathbb{Z}_p^{(\ell+1)\times(k+1)}, \mathbf{k}_j \hookleftarrow \mathbb{Z}_p^{\ell+1}$ for $i \in [1, n]$.
  - We set $\mathbf{K}_j = \widetilde{\mathbf{K}}_j + \mathbf{k}_j \mathbf{a}^\perp$ for $i \in [1, n]$.

- Finally, we show that Game_5 hides $\{\mathbf{k}_j\}_{j \notin T}$ information-theoretically.

Summary

- First adaptively secure TSPS construction.
- Competitive efficiency.
- First standard model construction.
- Proved it secure under standard $\mathcal{D}_k$-matDH, $\mathcal{D}_k$-kerDH assumptions.

Thanks for your attention! Any questions?

Thanks for your attention! Any questions?

Please take a look: https://ia.cr/2024/445

Thanks for your attention! Any questions?

Please take a look: https://ia.cr/2024/445

Contact: csayantan.mukherjee@gmail.com