Ordered Multi-Signatures with Public-Key Aggregation from SXDH Assumption

〇Masayuki Tezuka Keisuke Tanaka

Institute of Science Tokyo

Version 2025/11/26

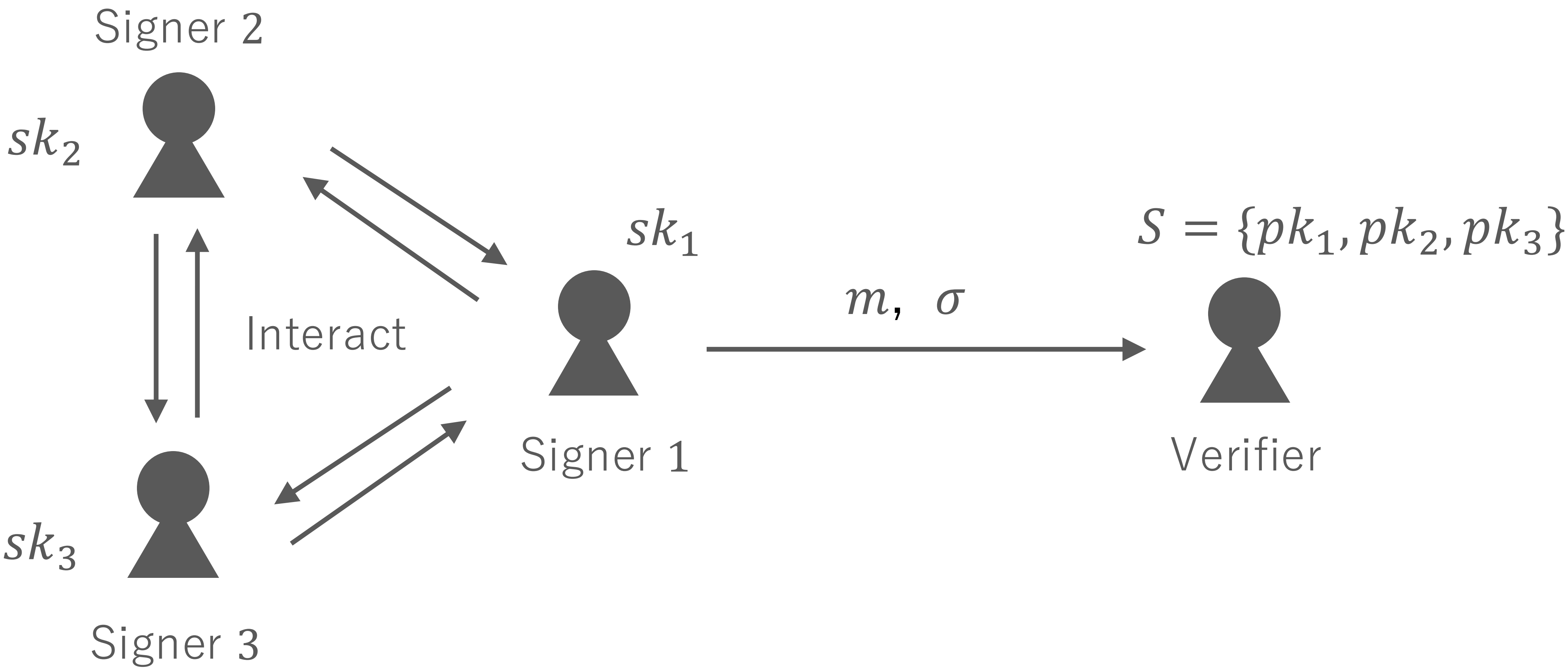
@ IWSEC 2025, Fukuoka, Japan

(Interactive) Multi-Signatures and Ordered Multi-Signatures

(Interactive) Multi-Signature (MS) [IN83]

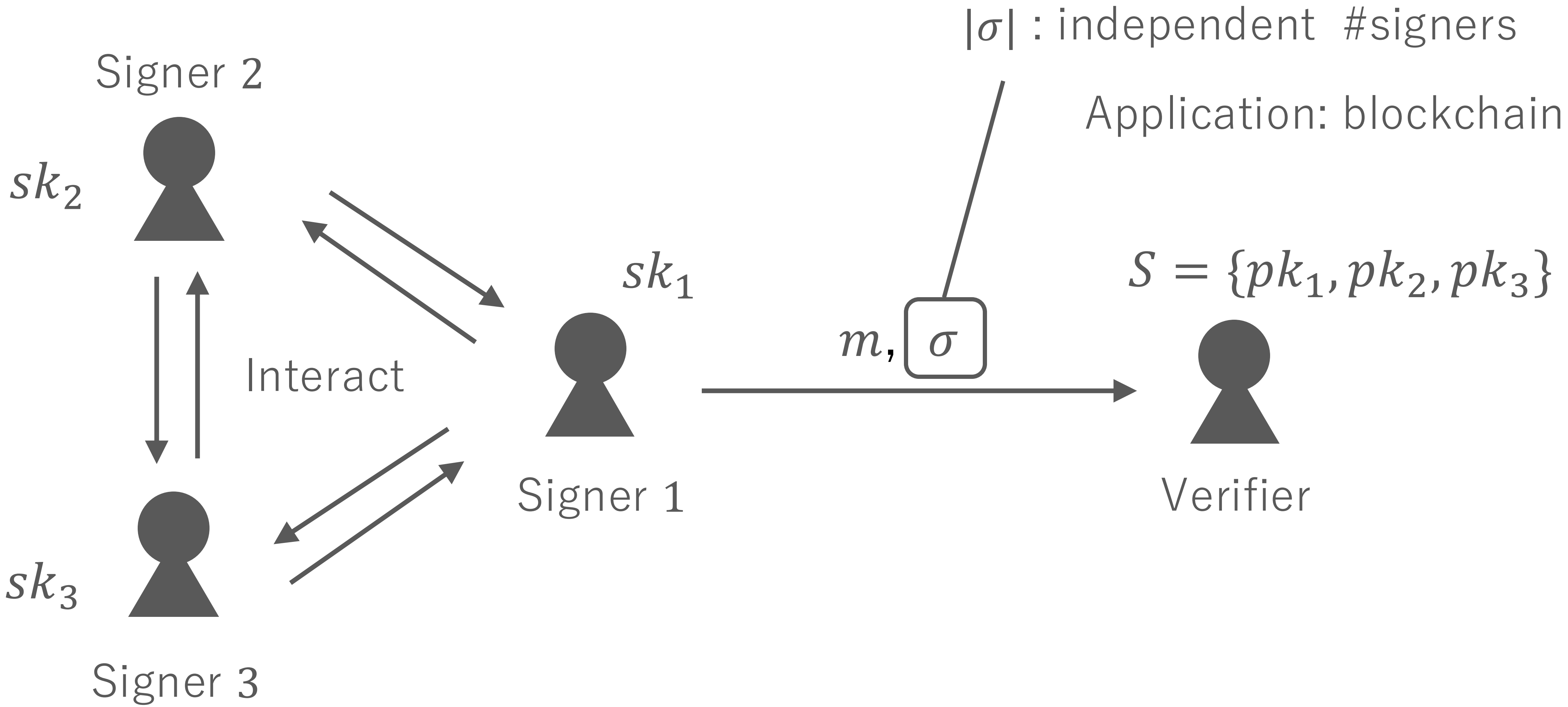
[IN83] Itakura and Nakamura. A public-key cryptosystem suitable for digital multisignatures. NEC Research & Development 1983.

(Interactive) Multi-Signature (MS) [IN83]



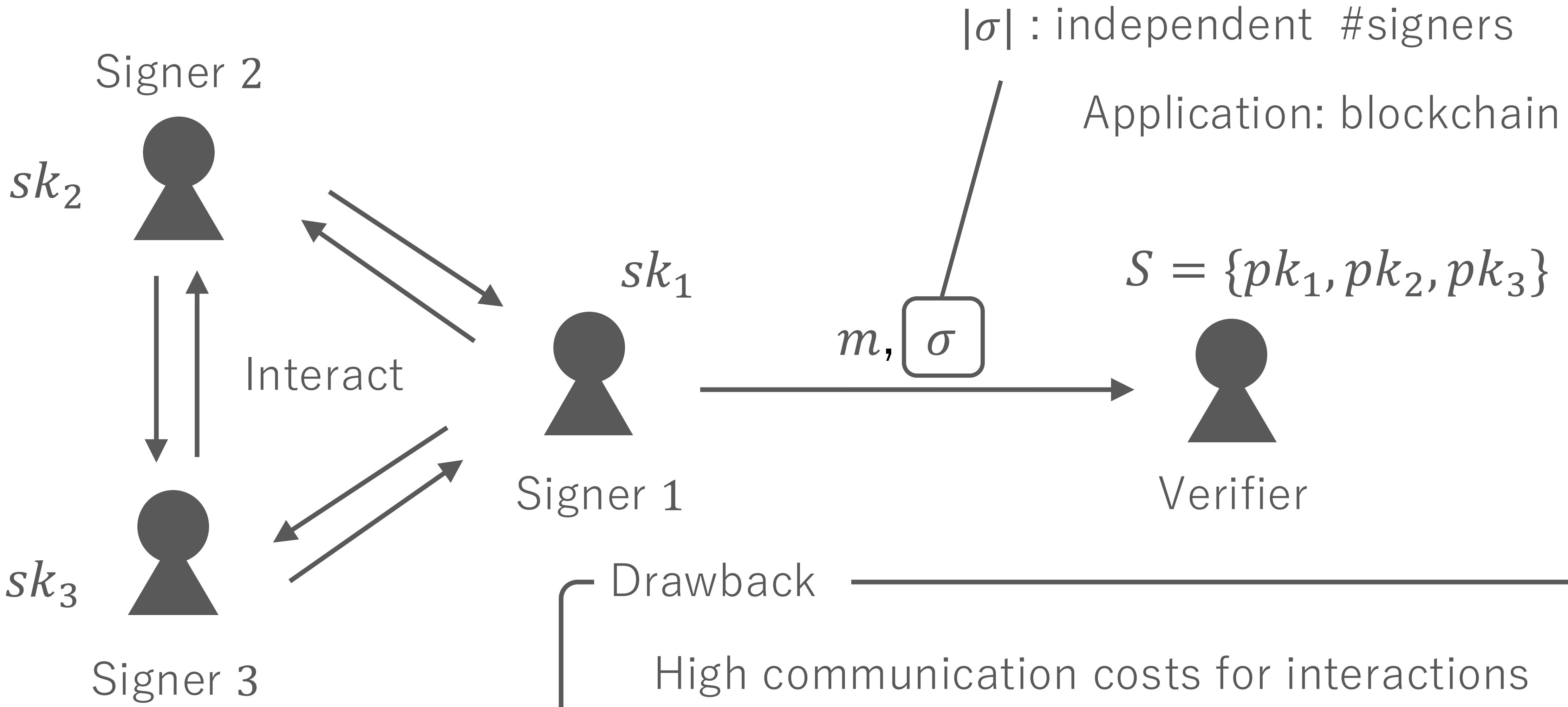
[IN83] Itakura and Nakamura. A public-key cryptosystem suitable for digital multisignatures. NEC Research & Development 1983.

(Interactive) Multi-Signature (MS) [IN83]



[IN83] Itakura and Nakamura. A public-key cryptosystem suitable for digital multisignatures. NEC Research & Development 1983.

(Interactive) Multi-Signature (MS) [IN83]



Drawback

High communication costs for interactions

[IN83] Itakura and Nakamura. A public-key cryptosystem suitable for digital multisignatures. NEC Research & Development 1983.

Ordered Multi-Signature (OMS) [BGOY07]

$$L = (pk_1, pk_2, pk_3)$$

sk_1 Signer 1

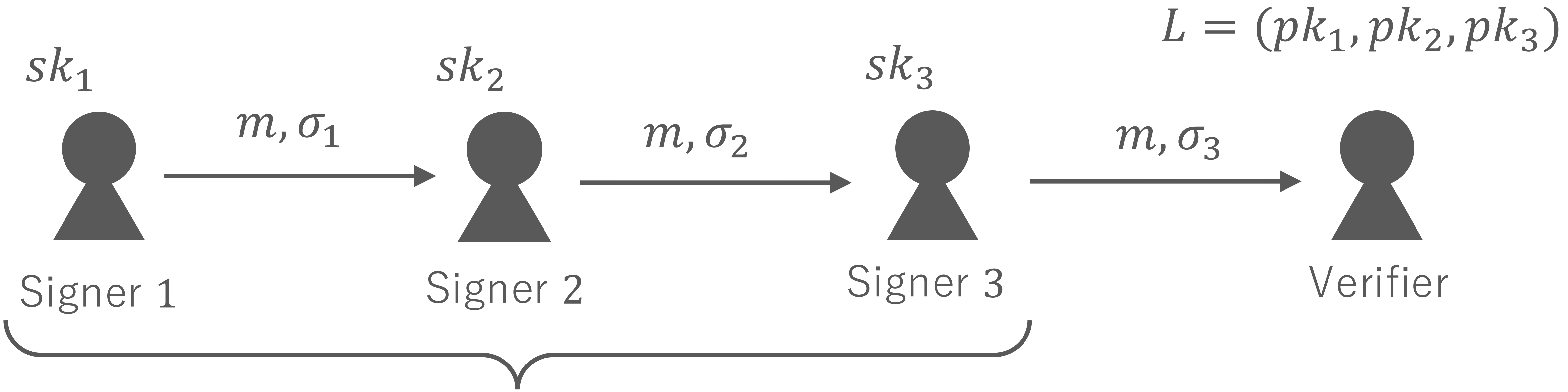
sk_2 Signer 2

sk_3 Signer 3

Verifier

[BGOY07] Boldyreva, Gentry, O'Neill, and Yum. Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing. CCS 2007

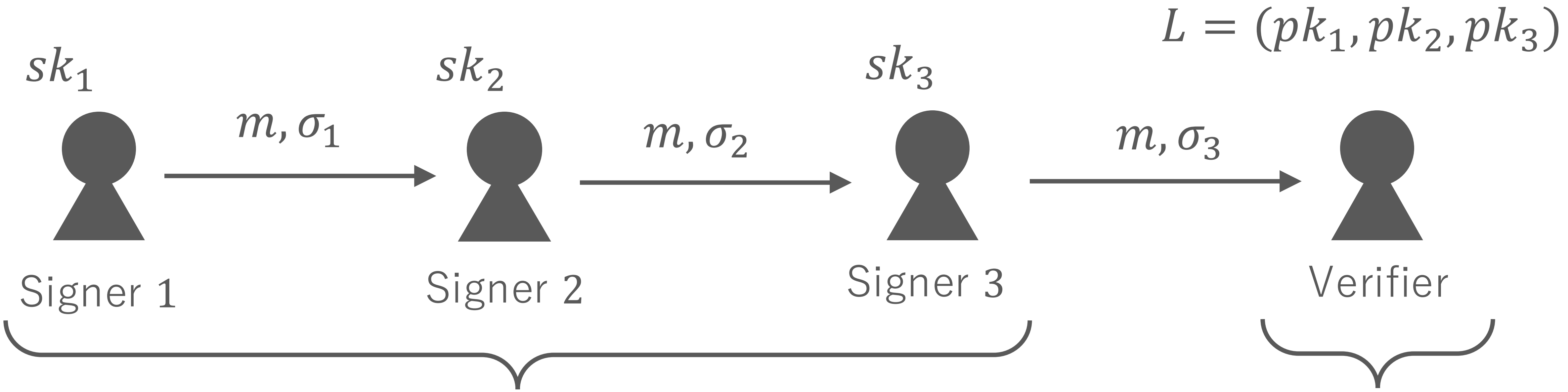
Ordered Multi-Signature (OMS) [BGOY07]



Singer i sequentially signs a common message m

[BGOY07] Boldyreva, Gentry, O'Neill, and Yum. Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing. CCS 2007

Ordered Multi-Signature (OMS) [BGOY07]



Singer i sequentially signs a common message m

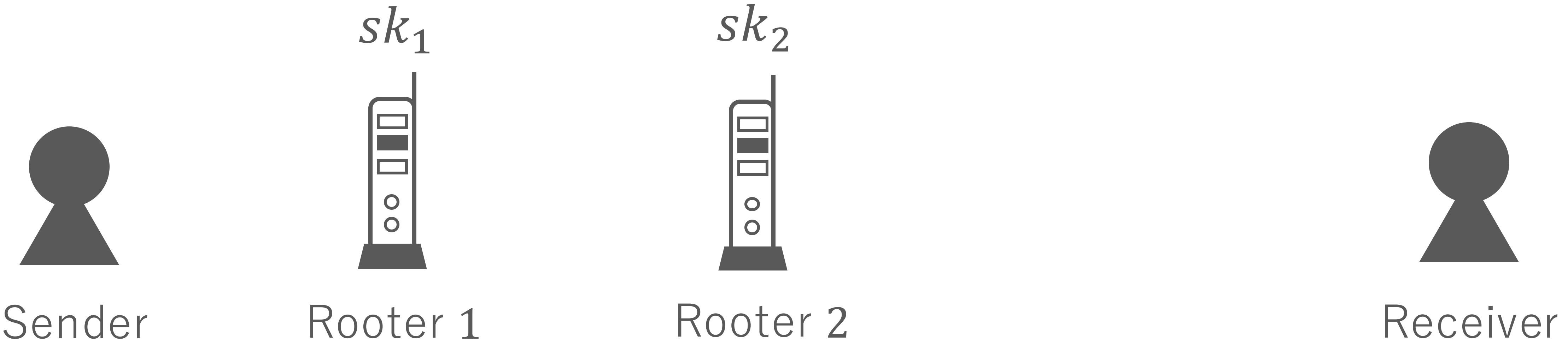
Verify signing order

Application: Network rooting

[BGOY07] Boldyreva, Gentry, O'Neill, and Yum. Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing. CCS 2007

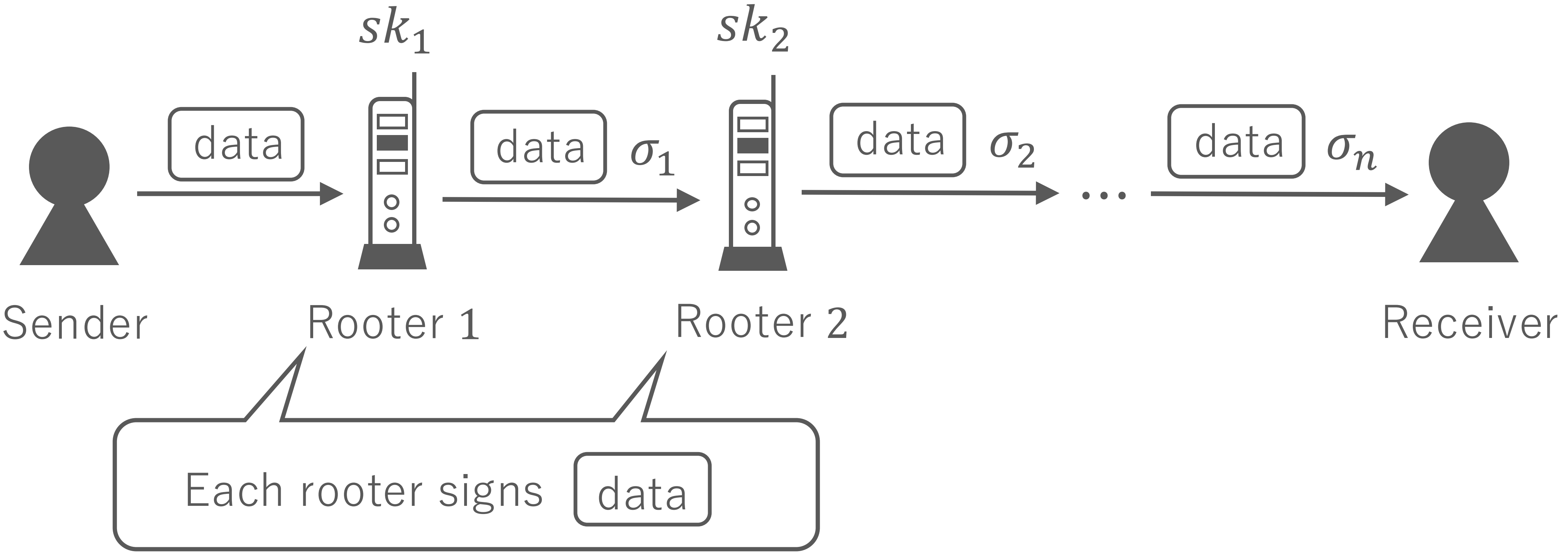
Application of OMS for Network Rooting

The sender sends the packet data $\boxed{\text{data}}$ to the receiver.



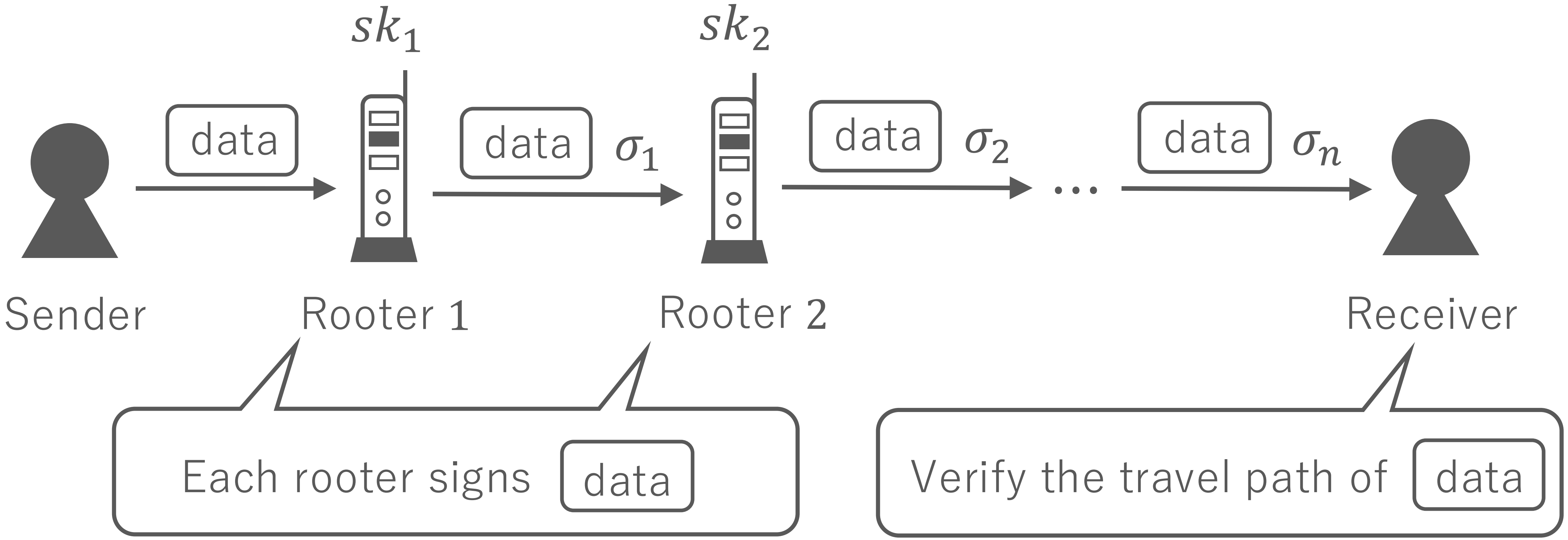
Application of OMS for Network Rooting

The sender sends the packet data $\boxed{\text{data}}$ to the receiver.



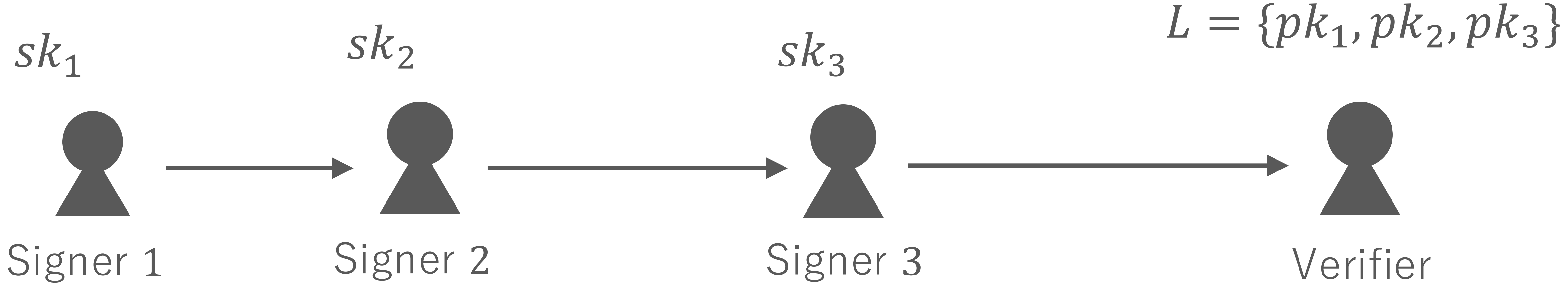
Application of OMS for Network Rooting

The sender sends the packet data $\boxed{\text{data}}$ to the receiver.



Sequential Aggregate Signatures and Ordered Multi-Signatures

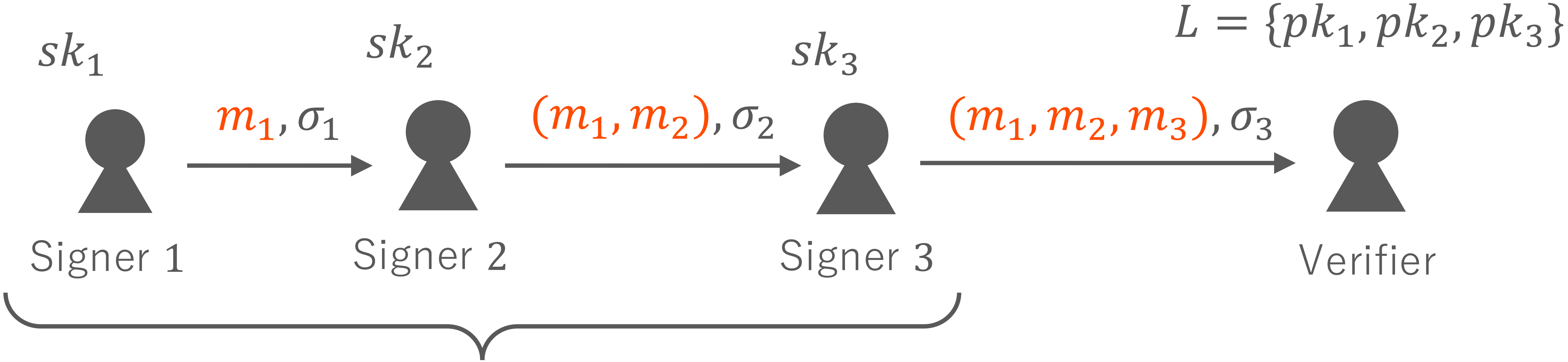
Sequential Aggregate Signature (SAS) [LMRS04]



Two main difference between SAS and OMS !

[LMRS04] Lysyanskaya, Micali, Reyzin, and Shacham. Sequential aggregate signatures from trapdoor permutations. EUROCRYPT 2004

Sequential Aggregate Signature (SAS) [LMRS04]

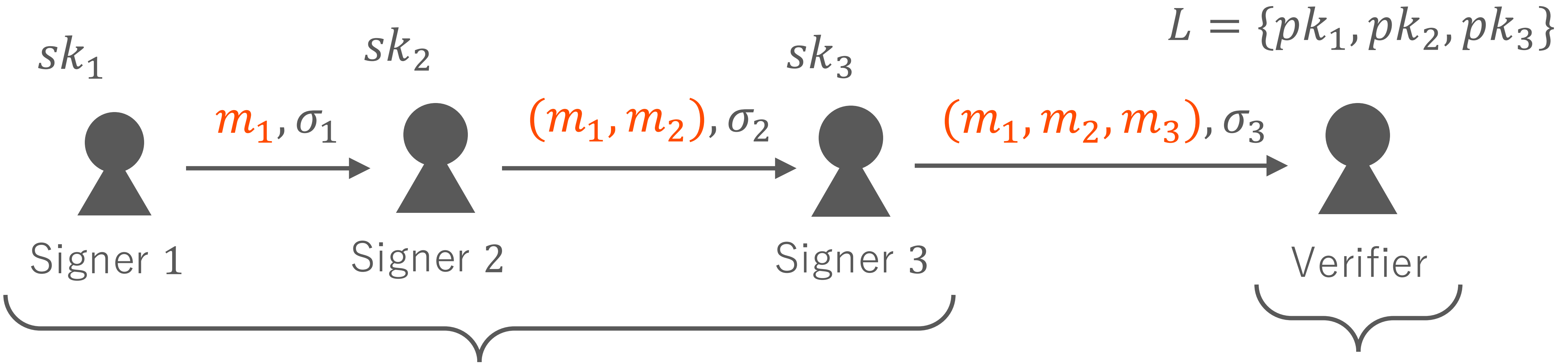


Singer i seqeuentially signs distinct message m_i

These are different from OMS.

[LMRS04] Lysyanskaya, Micali, Reyzin, and Shacham. Sequential aggregate signatures from trapdoor permutations. EUROCRYPT 2004

Sequential Aggregate Signature (SAS) [LMRS04]



Singer i seqeuentially signs distinct message m_i

Not support
signing order verification

These are different from OMS.

[LMRS04] Lysyanskaya, Micali, Reyzin, and Shacham. Sequential aggregate signatures from trapdoor permutations. EUROCRYPT 2004

Boldyreva et al.'s Transformation: From SAS to OMS

In SAS, simply signing a common message m does not yield OMS.

SAS does not support the signing order verification.

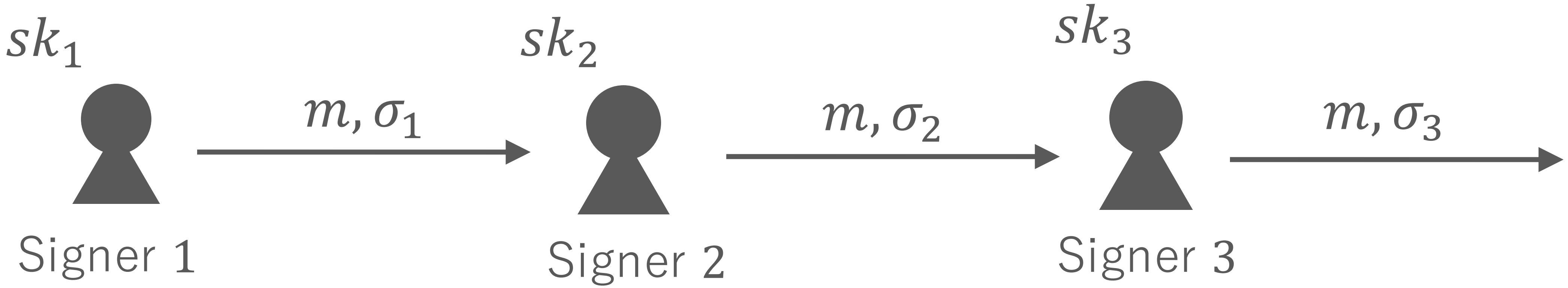
Boldyreva et al.'s Transformation: From SAS to OMS

In SAS, simply signing a common message m does not yield OMS.

SAS does not support the signing order verification.

Boldyreva et al. [BGOY07] OMS is obtained from SAS !!

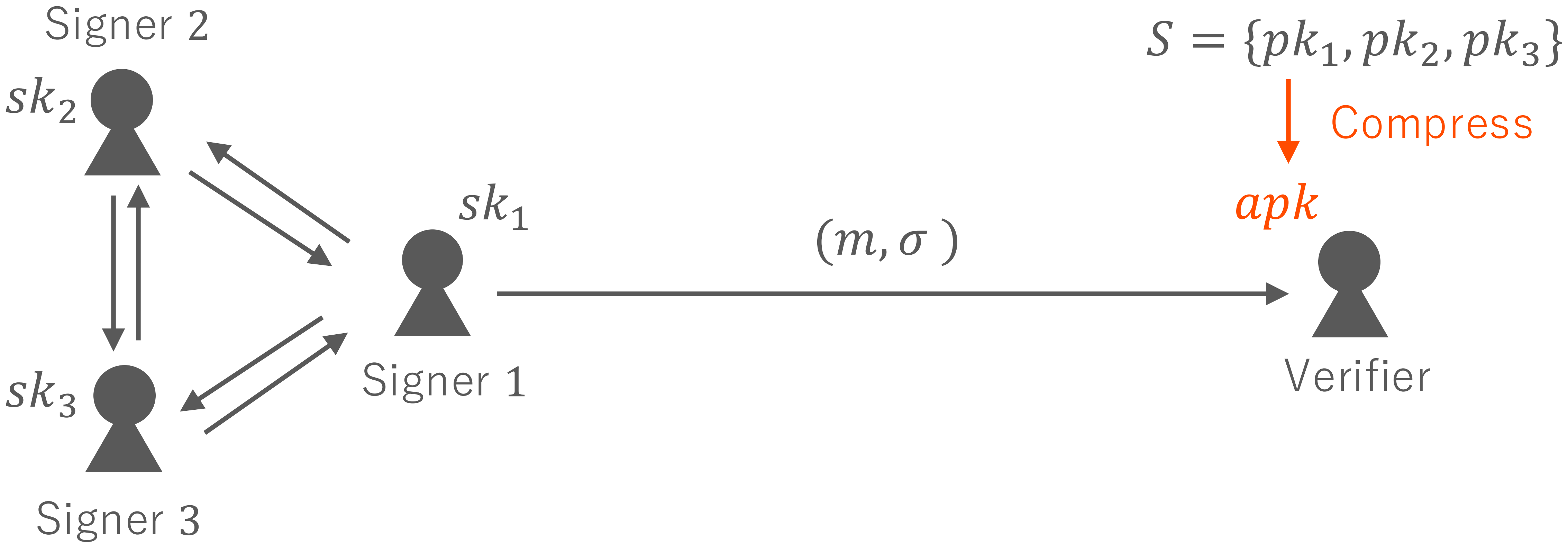
Idea：singer i signs $m_i = (m, i)$.



Sign $m_1 = (m, 1)$ Sign $m_2 = (m, 2)$ Sign $m_3 = (m, 3)$

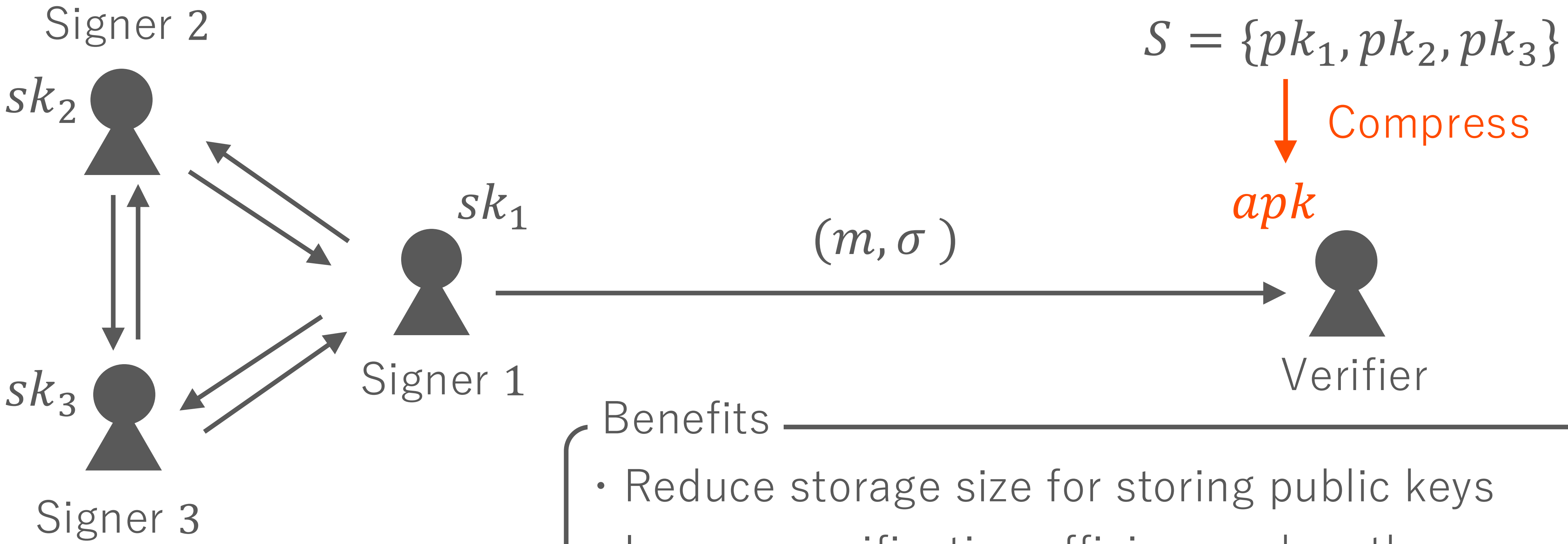
Public Key Aggregation for MS

Motivation: Public Key Aggregation in MS [MPSW19]



[MPSW19] Maxwell, Poelstra, Seurin, and Wuille. Simple schnorr multi-signatures with applications to bitcoin. Des. Codes Cryptogr. 2019

Motivation: Public Key Aggregation in MS [MPSW19]

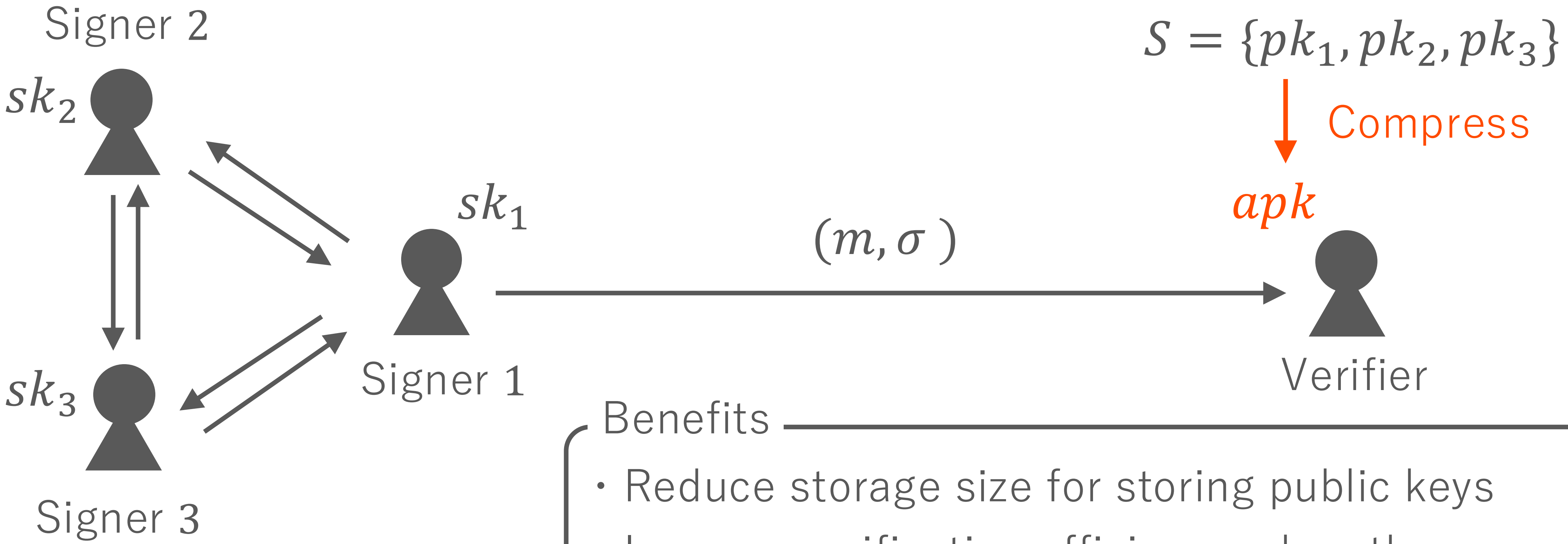


Benefits

- Reduce storage size for storing public keys
- Improve verification efficiency when the same set of signers generates multiple signatures.

[MPSW19] Maxwell, Poelstra, Seurin, and Wuille. Simple schnorr multi-signatures with applications to bitcoin. Des. Codes Cryptogr. 2019

Motivation: Public Key Aggregation in MS [MPSW19]



Benefits

- Reduce storage size for storing public keys
- Improve verification efficiency when the same set of signers generates multiple signatures.

In OMS, some schemes support public key aggregation.

[MPSW19] Maxwell, Poelstra, Seurin, and Wuille. Simple schnorr multi-signatures with applications to bitcoin. Des. Codes Cryptogr. 2019

Pairing-Based OMS (OMS from SAS via Boldyreva trans) without the ROM

Scheme	Assumption	pp size	pk size	sig size	PK Agg
OMS [YMO13]	CDH	$(\|m\|+3)\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	**YES**
SAS [LLY13]	**LRSW (Interactive)**	$2\|\mathbb{G}\|$	$\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	**No**
SAS [PS16]	**PS (Interactive)**	$2\|\mathbb{G}\|+2\|\tilde{\mathbb{G}}\|$	$\|\tilde{\mathbb{G}}\|$	$2\|\mathbb{G}\|$	**No**
SAS [McD20]	**2-PS (Interactive)**	$2\|\mathbb{G}\|+2\|\tilde{\mathbb{G}}\|$	$2\|\tilde{\mathbb{G}}\|$	$2\|\mathbb{G}\|$	**YES**
SAS [CK20]	SXDH	$4\|\mathbb{G}\|+3\|\tilde{\mathbb{G}}\|$	$\|\tilde{\mathbb{G}}\|$	$3\|\mathbb{G}\|$	**No**

[YMO13] Yanai, Mambo, and Okamoto. An ordered multisignature scheme under the CDH assumption without random oracles. ISC 2013
[LLY13] Lee, Lee, and Yung. Aggregating cl-signatures revisited: Extended functionality and better efficiency. FC 2013
[PS16] Pointcheval and Sanders. Short randomizable signatures. CT-RSA 2016
[McD20] McDonald. The landscape of pointcheval-sanders signatures: Mapping to polynomial-based signatures and beyond. IACR Cryptol. ePrint Arch. 2020
[CK20] Chatterjee and Kabaleeshwaran. From rerandomizability to sequential aggregation: Efficient signature schemes based on SXDH assumption. ACISP2020

Pairing-Based OMS (OMS from SAS via Boldyreva trans) without the ROM

Scheme	Assumption	pp size	pk size	sig size	PK Agg
OMS [YMO13]	CDH	$(\|m\| + 3)\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	**YES**
SAS [LLY13]	**LRSW (Interactive)**	$2\|\mathbb{G}\|$	$\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	**No**
SAS [PS16]	**PS (Interactive)**	$2\|\mathbb{G}\| + 2\|\tilde{\mathbb{G}}\|$	$\|\tilde{\mathbb{G}}\|$	$2\|\mathbb{G}\|$	**No**
SAS [McD20]	**2-PS (Interactive)**	$2\|\mathbb{G}\| + 2\|\tilde{\mathbb{G}}\|$	$2\|\tilde{\mathbb{G}}\|$	$2\|\mathbb{G}\|$	**YES**
SAS [CK20]	SXDH	$4\|\mathbb{G}\| + 3\|\tilde{\mathbb{G}}\|$	$\|\tilde{\mathbb{G}}\|$	$3\|\mathbb{G}\|$	**No**

The number of group element in public parameter is **linear in message bit length**.

Pairing-Based OMS (OMS from SAS via Boldyreva trans) without the ROM

Scheme	Assumption	pp size	pk size	sig size	PK Agg
OMS [YMO13]	CDH	$(\lvert m\rvert + 3)\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	**YES**
SAS [LLY13]	**LRSW (Interactive)**	$2\lvert\mathbb{G}\rvert$	$\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	**No**
SAS [PS16]	**PS (Interactive)**	$2\lvert\mathbb{G}\rvert + 2\lvert\tilde{\mathbb{G}}\rvert$	$\lvert\tilde{\mathbb{G}}\rvert$	$2\lvert\mathbb{G}\rvert$	**No**
SAS [McD20]	**2-PS (Interactive)**	$2\lvert\mathbb{G}\rvert + 2\lvert\tilde{\mathbb{G}}\rvert$	$2\lvert\tilde{\mathbb{G}}\rvert$	$2\lvert\mathbb{G}\rvert$	**YES**
SAS [CK20]	SXDH	$4\lvert\mathbb{G}\rvert + 3\lvert\tilde{\mathbb{G}}\rvert$	$\lvert\tilde{\mathbb{G}}\rvert$	$3\lvert\mathbb{G}\rvert$	**No**

The LRSW, PS, and 2-PS assumption are **interactive assumptions**.

Pairing-Based OMS (OMS from SAS via Boldyreva trans) without the ROM

Scheme	Assumption	pp size	pk size	sig size	PK Agg
OMS [YMO13]	CDH	$(\lvert m\rvert + 3)\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	**YES**
SAS [LLY13]	**LRSW (Interactive)**	$2\lvert\mathbb{G}\rvert$	$\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	**No**
SAS [PS16]	**PS (Interactive)**	$2\lvert\mathbb{G}\rvert + 2\lvert\tilde{\mathbb{G}}\rvert$	$\lvert\tilde{\mathbb{G}}\rvert$	$2\lvert\mathbb{G}\rvert$	**No**
SAS [McD20]	**2-PS (Interactive)**	$2\lvert\mathbb{G}\rvert + 2\lvert\tilde{\mathbb{G}}\rvert$	$2\lvert\tilde{\mathbb{G}}\rvert$	$2\lvert\mathbb{G}\rvert$	**YES**
SAS [CK20]	SXDH	$4\lvert\mathbb{G}\rvert + 3\lvert\tilde{\mathbb{G}}\rvert$	$\lvert\tilde{\mathbb{G}}\rvert$	$3\lvert\mathbb{G}\rvert$	**No**

Does not support public key aggregation.

Pairing-Based OMS (OMS from SAS via Boldyreva trans) without the ROM

Scheme	Assumption	pp size	pk size	sig size	PK Agg
OMS [YMO13]	CDH	**$(\|m\| + 3)$**$\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	**YES**
SAS [LLY13]	**LRSW (Interactive)**	$2\|\mathbb{G}\|$	$\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	**No**
SAS [PS16]	**PS (Interactive)**	$2\|\mathbb{G}\| + 2\|\tilde{\mathbb{G}}\|$	$\|\tilde{\mathbb{G}}\|$	$2\|\mathbb{G}\|$	**No**
SAS [McD20]	**2-PS (Interactive)**	$2\|\mathbb{G}\| + 2\|\tilde{\mathbb{G}}\|$	$2\|\tilde{\mathbb{G}}\|$	$2\|\mathbb{G}\|$	**YES**
SAS [CK20]	SXDH	$4\|\mathbb{G}\| + 3\|\tilde{\mathbb{G}}\|$	$\|\tilde{\mathbb{G}}\|$	$3\|\mathbb{G}\|$	**No**

Question

Compact pp size OMS with **PK aggregation** in the **standard assumptions**.

Our Result

Scheme	Assumption	pp size	pk size	sig size	PK Agg
OMS [YMO13]	CDH	$(\lvert m\rvert + 3)\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	YES
SAS [LLY13]	**LRSW (Interactive)**	$2\lvert\mathbb{G}\rvert$	$\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	**No**
SAS [PS16]	**PS (Interactive)**	$2\lvert\mathbb{G}\rvert + 2\lvert\tilde{\mathbb{G}}\rvert$	$\lvert\tilde{\mathbb{G}}\rvert$	$2\lvert\mathbb{G}\rvert$	**No**
SAS [McD20]	**2-PS (Interactive)**	$2\lvert\mathbb{G}\rvert + 2\lvert\tilde{\mathbb{G}}\rvert$	$2\lvert\tilde{\mathbb{G}}\rvert$	$2\lvert\mathbb{G}\rvert$	YES
SAS [CK20]	SXDH	$4\lvert\mathbb{G}\rvert + 3\lvert\tilde{\mathbb{G}}\rvert$	$\lvert\tilde{\mathbb{G}}\rvert$	$3\lvert\mathbb{G}\rvert$	**No**
Our Scheme	**SXDH**	$4\lvert\mathbb{G}\rvert + 3\lvert\tilde{\mathbb{G}}\rvert$	$2\lvert\tilde{\mathbb{G}}\rvert$	$3\lvert\mathbb{G}\rvert$	**YES**

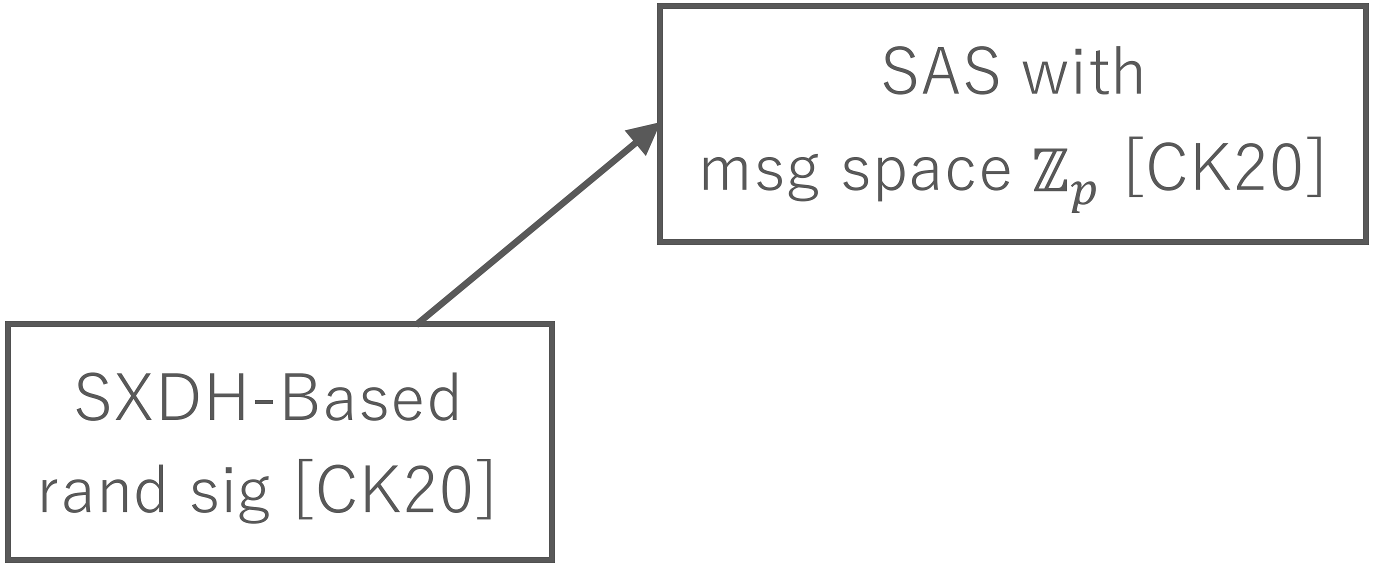
How to Obtain Scheme

SXDH-Based SAS [CK20] and OMS

SXDH-Based
rand sig [CK20]

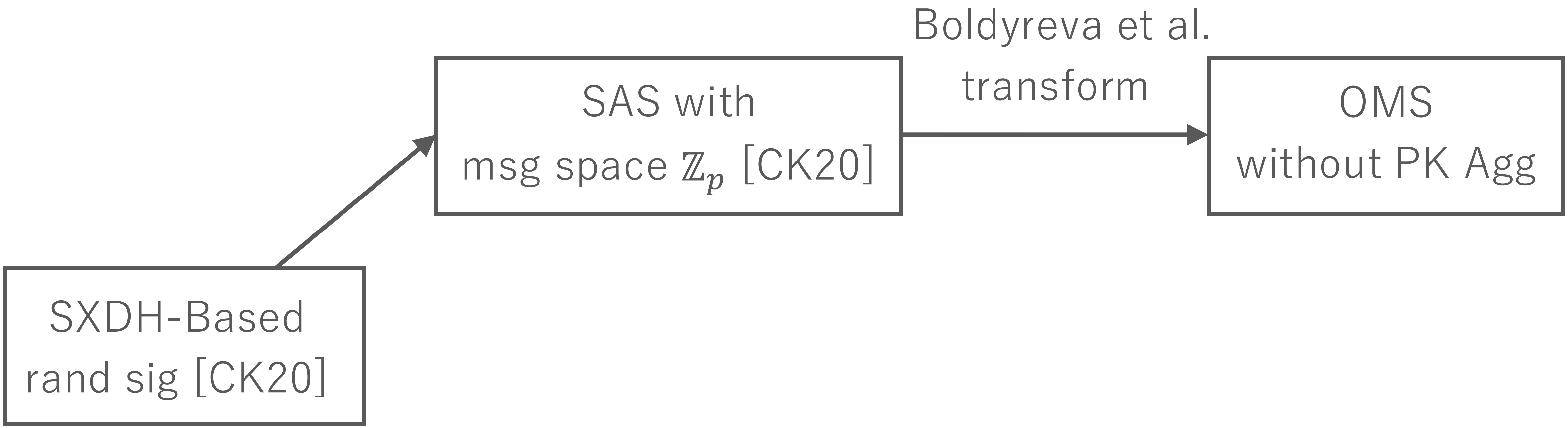
[CK20] Chatterjee and Kabaleeshwaran. From rerandomizability to sequential aggregation: Efficient signature schemes based on SXDH assumption. ACISP2020

SXDH-Based SAS [CK20] and OMS



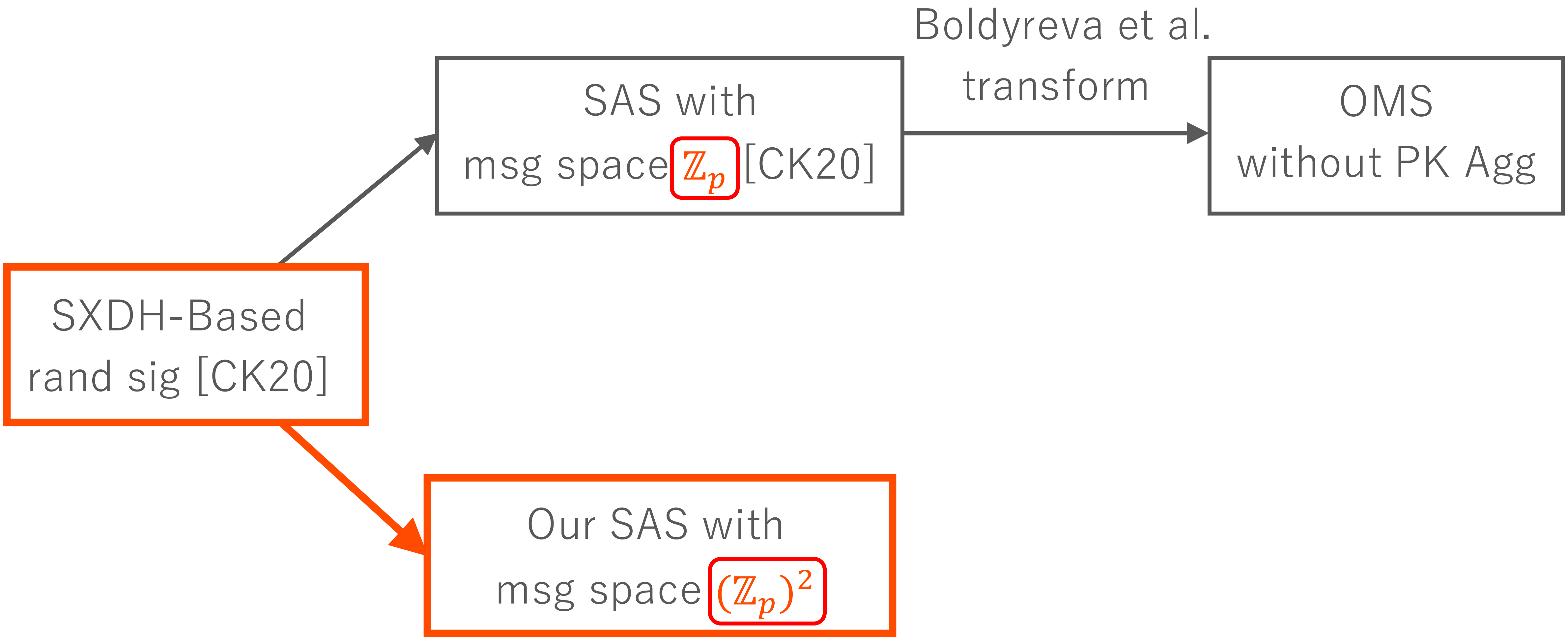
[CK20] Chatterjee and Kabaleeshwaran. From rerandomizability to sequential aggregation: Efficient signature schemes based on SXDH assumption. ACISP2020

SXDH-Based SAS [CK20] and OMS



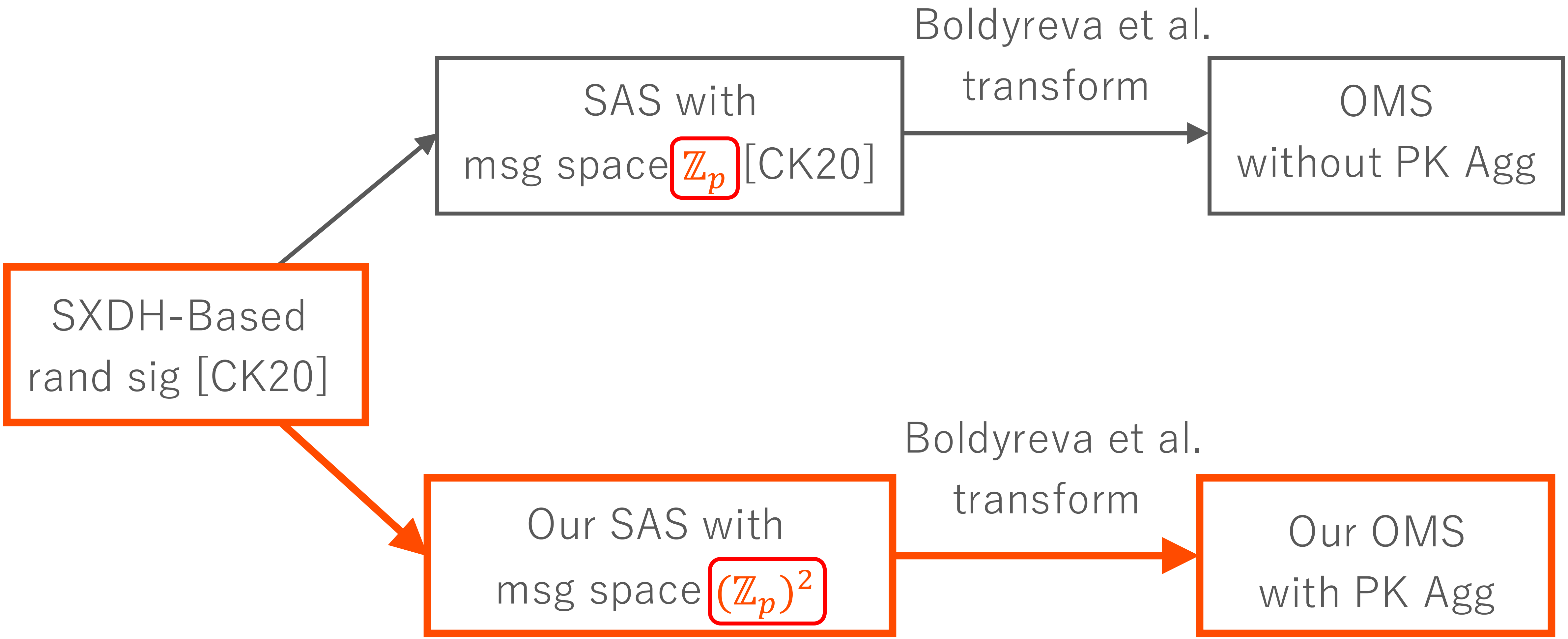
[CK20] Chatterjee and Kabaleeshwaran. From rerandomizability to sequential aggregation: Efficient signature schemes based on SXDH assumption. ACISP2020

Our Approach



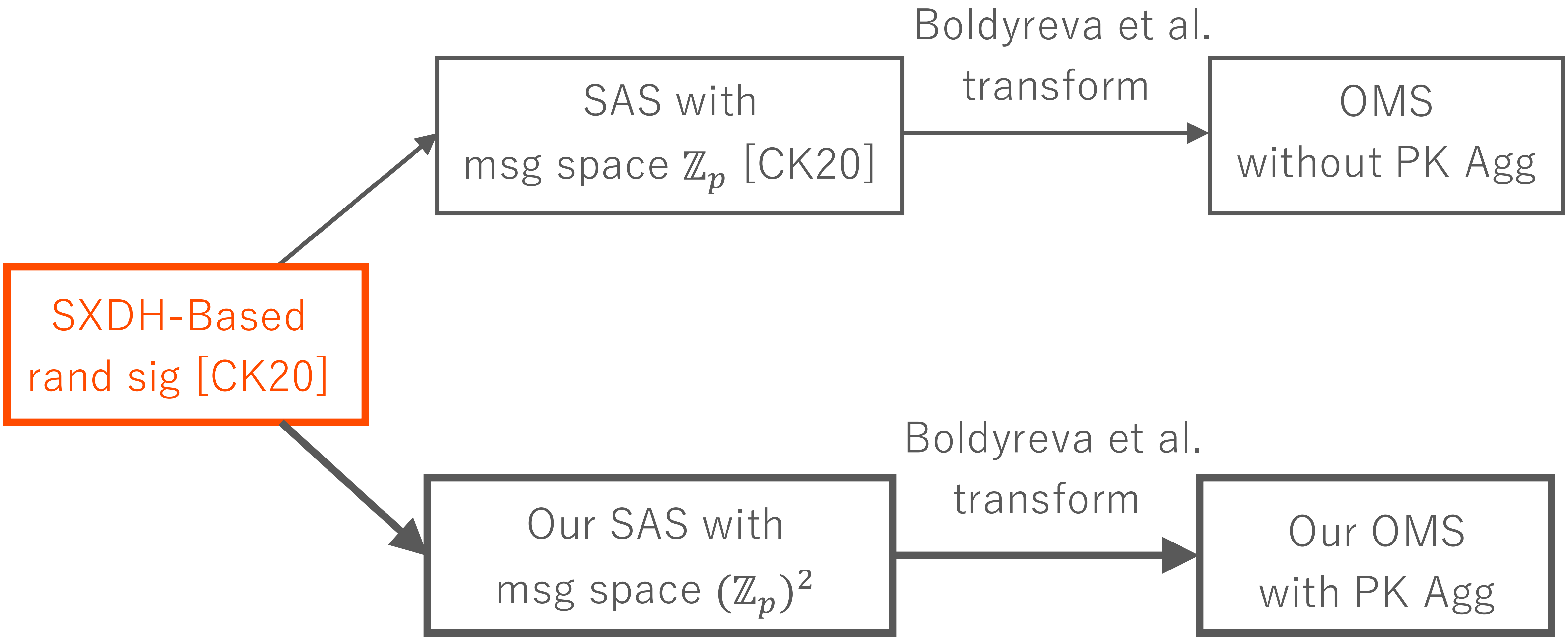
[CK20] Chatterjee and Kabaleeshwaran. From rerandomizability to sequential aggregation: Efficient signature schemes based on SXDH assumption. ACISP2020

Our Approach



[CK20] Chatterjee and Kabaleeshwaran. From rerandomizability to sequential aggregation: Efficient signature schemes based on SXDH assumption. ACISP2020

Starting Point: Based Randomizable Signature Scheme



[CK20] Chatterjee and Kabaleeshwaran. From rerandomizability to sequential aggregation: Efficient signature schemes based on SXDH assumption. ACISP2020

SXDH-Based Randomizable Signature for Msg $(\mathbb{Z}_p)^2$ [CK20]

$$pk = \left(\widetilde{H}, \widetilde{D}, \widetilde{U}, \widetilde{V}, \widetilde{W}\right) \quad sk = (x_1, x_2, y_1, y_2, z_1, z_2)$$

$$d \leftarrow \mathbb{Z}_p^*,\ \widetilde{D} = \widetilde{H}^{d}, \widetilde{U} = \widetilde{H}^{x_2 - dx_1}, \widetilde{V} = \widetilde{H}^{y_2 - dy_1}, \widetilde{W} = \widetilde{H}^{z_2 - dz_1}$$

[CK20] Chatterjee and Kabaleeshwaran. From rerandomizability to sequential aggregation: Efficient signature schemes based on SXDH assumption. ACISP2020

SXDH-Based Randomizable Signature for Msg $(\mathbb{Z}_p)^2$ [CK20]

$$pk = \left(\widetilde{H}, \widetilde{D}, \widetilde{U}, \widetilde{V}, \widetilde{W}\right) \quad sk = (x_1, x_2, y_1, y_2, z_1, z_2)$$

$$d \leftarrow \mathbb{Z}_p^*,\ \widetilde{D} = \widetilde{H}^d, \widetilde{U} = \widetilde{H}^{x_2 - d x_1}, \widetilde{V} = \widetilde{H}^{y_2 - d y_1}, \widetilde{W} = \widetilde{H}^{z_2 - d z_1}$$

Signature $\sigma = (A, B, C)$ on message (m_1, m_2)

$$r \leftarrow \mathbb{Z}_p^*,\ A \leftarrow G^r, B \leftarrow A^{x_1 + m_1 y_1 + m_2 z_1}, C \leftarrow A^{x_2 + m_1 y_2 + m_2 z_2}$$

[CK20] Chatterjee and Kabaleeshwaran. From rerandomizability to sequential aggregation: Efficient signature schemes based on SXDH assumption. ACISP2020

SXDH-Based Randomizable Signature for Msg $(\mathbb{Z}_p)^2$ [CK20]

$$pk = \left(\widetilde{H}, \widetilde{D}, \widetilde{U}, \widetilde{V}, \widetilde{W}\right) \quad sk = (x_1, x_2, y_1, y_2, z_1, z_2)$$

$$d \leftarrow \mathbb{Z}_p^*,\ \widetilde{D} = \widetilde{H}^d, \widetilde{U} = \widetilde{H}^{x_2 - dx_1}, \widetilde{V} = \widetilde{H}^{y_2 - dy_1}, \widetilde{W} = \widetilde{H}^{z_2 - dz_1}$$

Signature $\sigma = (A, B, C)$ on message (m_1, m_2)

$$r \leftarrow \mathbb{Z}_p^*,\ A \leftarrow G^r, B \leftarrow A^{x_1 + m_1 y_1 + m_2 z_1}, C \leftarrow A^{x_2 + m_1 y_2 + m_2 z_2}$$

Verification of $\sigma = (A, B, C)$ on message (m_1, m_2)

$$e\left(A, \widetilde{U}\widetilde{V}^{m_1}\widetilde{W}^{m_2}\right) \cdot e\left(B, \widetilde{D}\right) = e\left(C, \widetilde{H}\right)?$$

[CK20] Chatterjee and Kabaleeshwaran. From rerandomizability to sequential aggregation: Efficient signature schemes based on SXDH assumption. ACISP2020

Randomizable Property

A signature $\sigma = (A, B, C)$ on message (m_1, m_2) is refreshed without a signing key sk.

Signature $\sigma = (A, B, C)$ on message (m_1, m_2)

Randomizable Property

A signature $\sigma = (A, B, C)$ on message (m_1, m_2) is refreshed without a signing key sk.

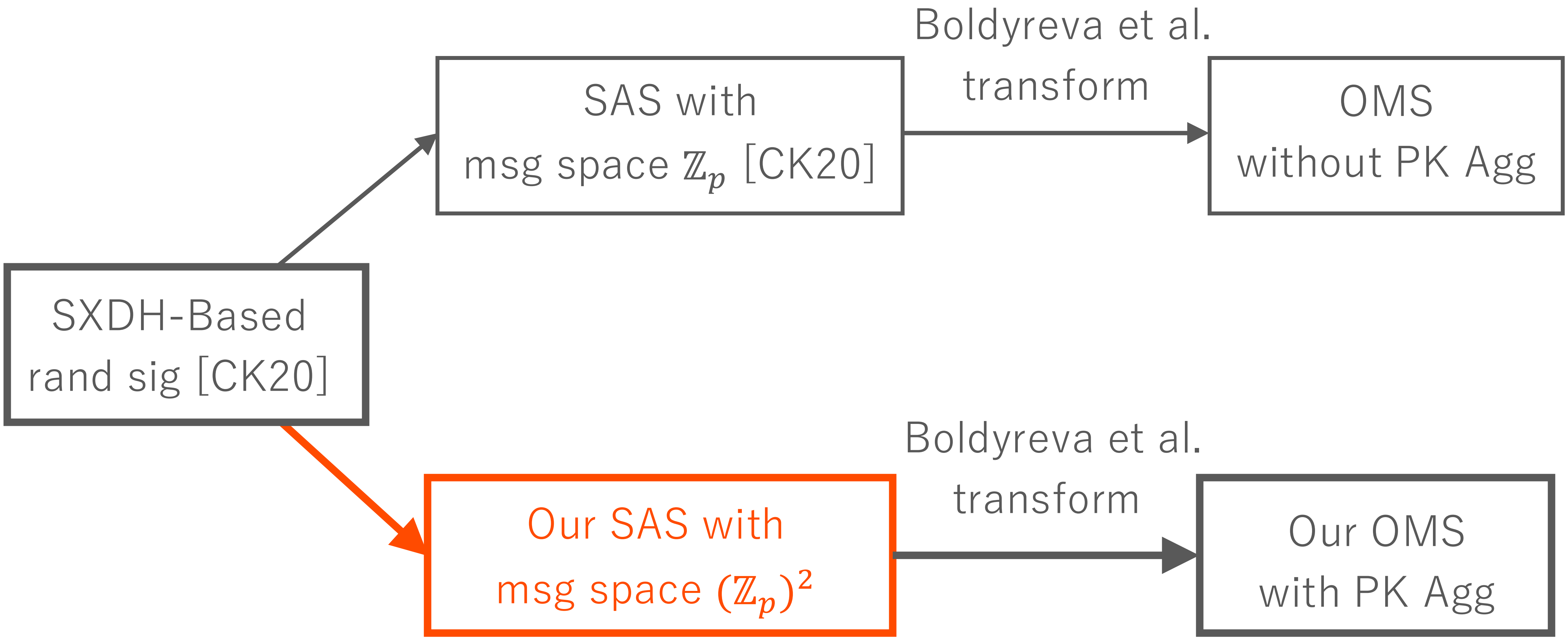
Signature $\sigma = (A, B, C)$ on message (m_1, m_2)

Randomizable property

$$r' \leftarrow \mathbb{Z}_p^*,\ A' \leftarrow A^{r'}, B' \leftarrow B^{r'}, C' \leftarrow C^{r'}$$

Refreshed signature $\sigma' = (A', B', C')$ on message (m_1, m_2)

From Based Signature Scheme to Our SAS



How to Derive SAS with msg space $(\mathbb{Z}_p)^2$

Randomizable Signature [CK20] for Msg $(\mathbb{Z}_p)^2$

$\Downarrow$

- PK sharing technique
- Modify signing algorithm

Our SAS for Msg $(\mathbb{Z}_p)^2$

PK Sharing Technique

$$pk = (\quad \tilde{H}, \tilde{D}, \tilde{U}, \quad \tilde{V}, \tilde{W}) \qquad sk = (\quad x_1, x_2, \quad y_1, y_2, z_1, z_2)$$

PK Sharing Technique

$$pk = \left(\boxed{\widetilde{H}, \widetilde{D}, \widetilde{U},}\ \widetilde{V}, \widetilde{W} \right) \quad sk = \left(\cancel{x_1, x_2,}\ y_1, y_2, z_1, z_2 \right)$$

pp

G^{x_1}, G^{x_2}

PK Sharing Technique

$$pk = (\boxed{\widetilde{H}, \widetilde{D}, \widetilde{U},}\ \widetilde{V}, \widetilde{W}) \quad sk = (\cancel{x_1, x_2,}\ y_1, y_2, z_1, z_2)$$

pp $\qquad G^{x_1}, G^{x_2}$

PK sharing technique

$$pp = (G, \widetilde{H}, \widetilde{D}, \widetilde{U}, X_1 = G^{x_1}, X_2 = G^{x_2})$$

Singer i's pk_i and sk_i

$$pk_i = (\widetilde{V}_i, \widetilde{W}_i) \quad sk_i = (y_{i,1}, y_{i,2}, z_{i,1}, z_{i,2})$$

Modifying Signing for Signer 1

Singer 1 signs $(m_{1,1}, m_{1,2})$ with $sk_1 = (y_{1,1}, y_{1,2}, z_{1,1}, z_{1,2})$

$r_1 \leftarrow \mathbb{Z}_p^*, A_1 \leftarrow G^{r_1},$

$B_1 \leftarrow (X_1 G^{m_{1,1}y_{1,1}+m_{1,2}z_{1,1}})^{r_1}$, $C_1 \leftarrow (X_2 G^{m_{1,1}y_{1,2}+m_{1,2}z_{1,2}})^{r_1}$

Generated signature $\sigma_1 = (A_1, B_1, C_1)$

$$A_1 = G^{r_1}$$
$$B_1 = A_1{}^{x+m_{1,1}y_{1,1}+m_{1,2}z_{1,1}}$$
$$C_1 = A_1{}^{x+m_{1,1}y_{1,2}+m_{1,2}z_{1,2}}$$

hold.

Modifying Signing for Signer $i \geq 2$

Singer i signs $(m_{i,1}, m_{i,2})$ with $sk_i = (y_{i,1}, y_{i,2}, z_{i,1}, z_{i,2})$

and updates $\sigma_{i-1} = (A_{i-1}, B_{i-1}, C_{i-1})$.

$$r_i \leftarrow \mathbb{Z}_p^*, A_i \leftarrow {A_{i-1}}^{r_i} \ ,$$

$$B_i \leftarrow ({A_{i-1}}^{m_{i,1}y_{i,1}+m_{i,2}z_{i,1}})^{r_i} \cdot {B_{i-1}}^{r_i}$$

$$C_i \leftarrow ({A_{i-1}}^{m_{i,1}y_{i,2}+m_{i,2}z_{i,2}})^{r_i} \cdot \ {C_{i-1}}^{r_i}$$

Updated signature $\sigma_i = (A_i, B_i, C_i)$

$$A_i = G^{\prod r_k}, \ B_i = {A_i}^{x+\sum m_{k,1}y_{k,1}+\sum m_{k,1}z_{k,1}}$$

$$C_i = {A_i}^{x+\sum m_{k,1}y_{k,2}+\sum m_{k,1}z_{k,2}}$$

hold.

Modifying Signing for Signer $i \geq 2$

Singer i signs $(m_{i,1}, m_{i,2})$ with $sk_i = (y_{i,1}, y_{i,2}, z_{i,1}, z_{i,2})$

and updates $\sigma_{i-1} = (A_{i-1}, B_{i-1}, C_{i-1})$.

$$r_i \leftarrow \mathbb{Z}_p^*, A_i \leftarrow \boxed{{A_{i-1}}^{r_i}},$$

$$B_i \leftarrow ({A_{i-1}}^{m_{i,1}y_{i,1}+m_{i,2}z_{i,1}})^{r_i} \cdot \boxed{{B_{i-1}}^{r_i}}$$

$$C_i \leftarrow ({A_{i-1}}^{m_{i,1}y_{i,2}+m_{i,2}z_{i,2}})^{r_i} \cdot \boxed{{C_{i-1}}^{r_i}}$$

Randomization of σ_{i-1}

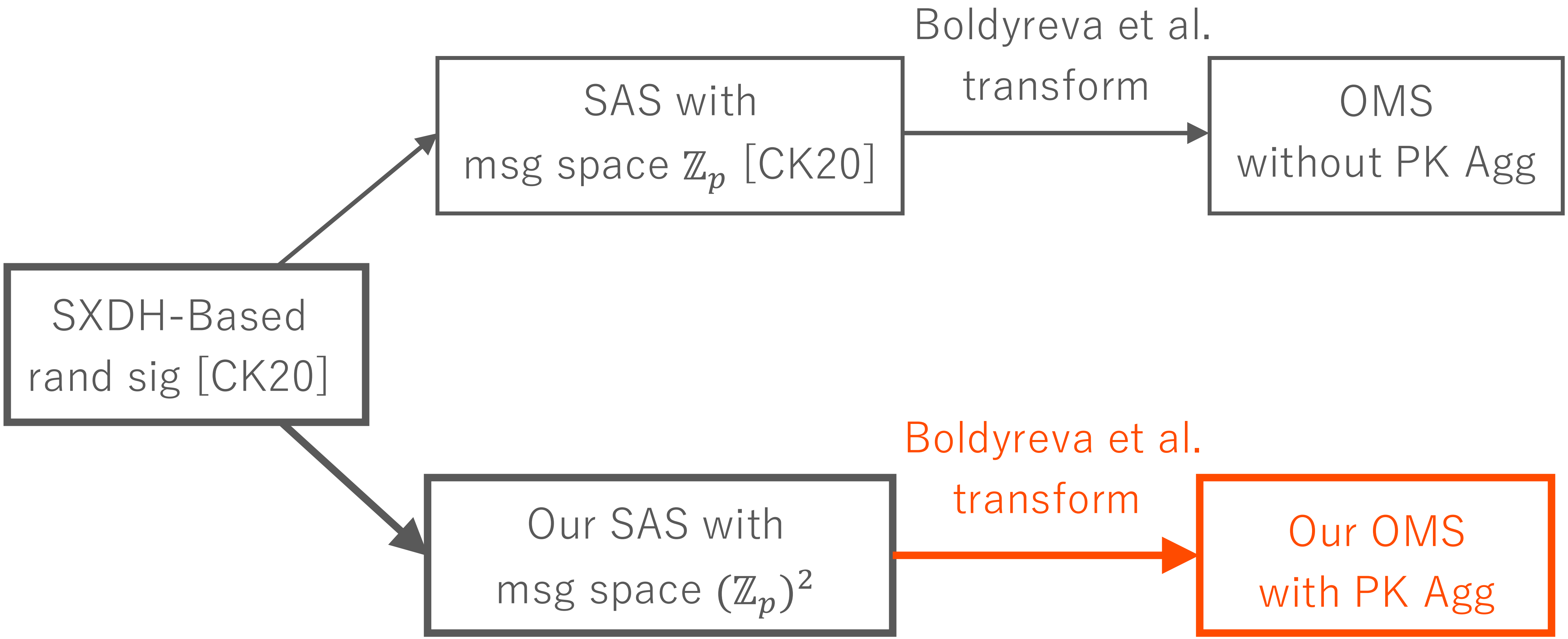
Updated signature $\sigma_i = (A_i, B_i, C_i)$

$$A_i = G^{\prod r_k}, \ B_i = {A_i}^{x+\sum m_{k,1}y_{k,1}+\sum m_{k,1}z_{k,1}}$$

$$C_i = {A_i}^{x+\sum m_{k,1}y_{k,2}+\sum m_{k,1}z_{k,2}}$$

hold.

Our SAS to Our OMS with PK Agg



Boldyreva et al. Transformation

Singer i signs (m, i) with $sk_i = \left(y_{i,1}, y_{i,2}, z_{i,1}, z_{i,2}\right)$

and updates $\sigma_{i-1} = (A_{i-1}, B_{i-1}, C_{i-1})$.

Updated signature $\sigma_i = (A_i, B_i, C_i)$

$$A_i = G^{\prod r_k}$$

$$B_i = A_i^{\,x + \sum m y_{k,1} + \sum k z_{k,1}}$$

$$C_i = A_i^{\,x + \sum m y_{k,2} + \sum k z_{k,2}}$$

hold.

PK Aggregation

$$pk_i = \left(\tilde{V}_i, \widetilde{W}_i\right) \quad \sigma_i = (A_i, B_i, C_i)$$

$$A_i = G^{\prod r_k} \quad B_i = A_i^{x+\sum m y_{k,1} + \sum k z_{k,1}} \quad C_i = A_i^{x+\sum m y_{k,2} + \sum k z_{k,2}}$$

Verification of σ_i

$$e\left(A_i, \widetilde{U} \cdot \left(\prod \tilde{V}_k\right)^m \cdot \prod \widetilde{W}_k{}^k\right) \cdot e\left(B_i, \widetilde{D}\right) = e\left(C_i, \widetilde{H}\right)\ ?$$

PK Aggregation

$$pk_i = (\tilde{V}_i, \widetilde{W}_i) \quad \sigma_i = (A_i, B_i, C_i)$$

$$A_i = G^{\prod r_k} \quad B_i = A_i^{\,x+\sum m y_{k,1} + \sum k z_{k,1}} \quad C_i = A_i^{\,x+\sum m y_{k,2} + \sum k z_{k,2}}$$

Verification of σ_i

$$e\left(A_i, \widetilde{U} \cdot \boxed{\left(\prod \tilde{V}_k\right)}^{m} \cdot \boxed{\prod \widetilde{W}_k^{\;k}}\right) \cdot e(B_i, \widetilde{D}) = e(C_i, \widetilde{H})\ ?$$

PK Aggregation

$$pk_i = \left(\tilde{V}_i, \tilde{W}_i\right) \qquad \sigma_i = (A_i, B_i, C_i)$$

$$A_i = G^{\prod r_k} \qquad B_i = A_i^{x+\sum m y_{k,1}+\sum k z_{k,1}} \qquad C_i = A_i^{x+\sum m y_{k,2}+\sum k z_{k,2}}$$

Verification of $\boldsymbol{\sigma_i}$

$$e\left(A_i, \tilde{U} \cdot \boxed{\left(\prod \tilde{V}_k\right)}^{m} \cdot \boxed{\prod \tilde{W}_k{}^{k}}\right) \cdot e\left(B_i, \tilde{D}\right) = e\left(C_i, \tilde{H}\right)\ ?$$

$$apk = \left(\prod \tilde{V}_k, \prod \tilde{W}_k{}^{k}\right)$$

Conclusion

We construct the ordered multi-signature scheme with key-aggregation.

Our scheme offers compact pp, pk, and σ.

The security is proven under the SXDH assumption without the ROM.

Future work

Tightly secure OMS with PK agg in the standard model.

Thank you for listening !