Improved Security Proof for the Camenisch-Lysyanskaya Signature-Based Synchronized Aggregate Signature Scheme

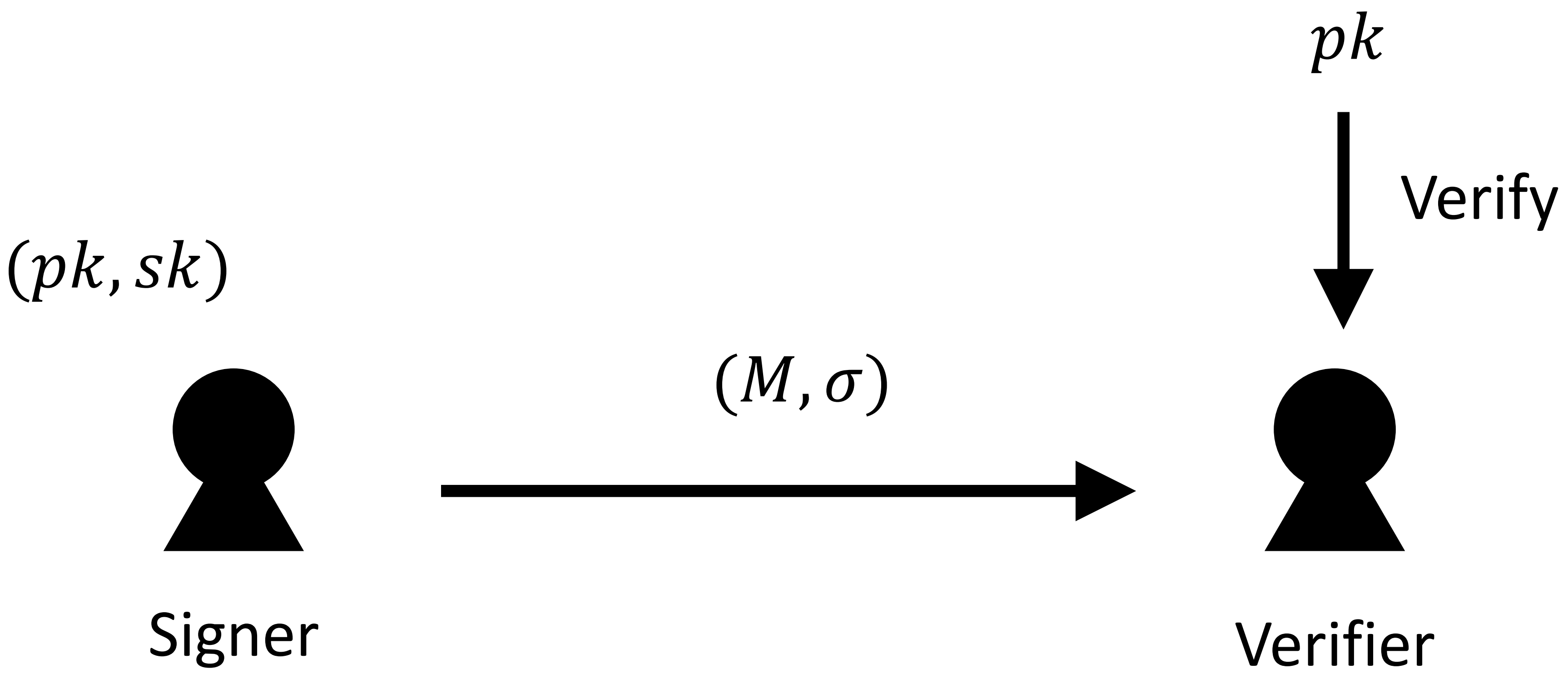
Masayuki Tezuka   Keisuke Tanaka

Tokyo Institute of Technology

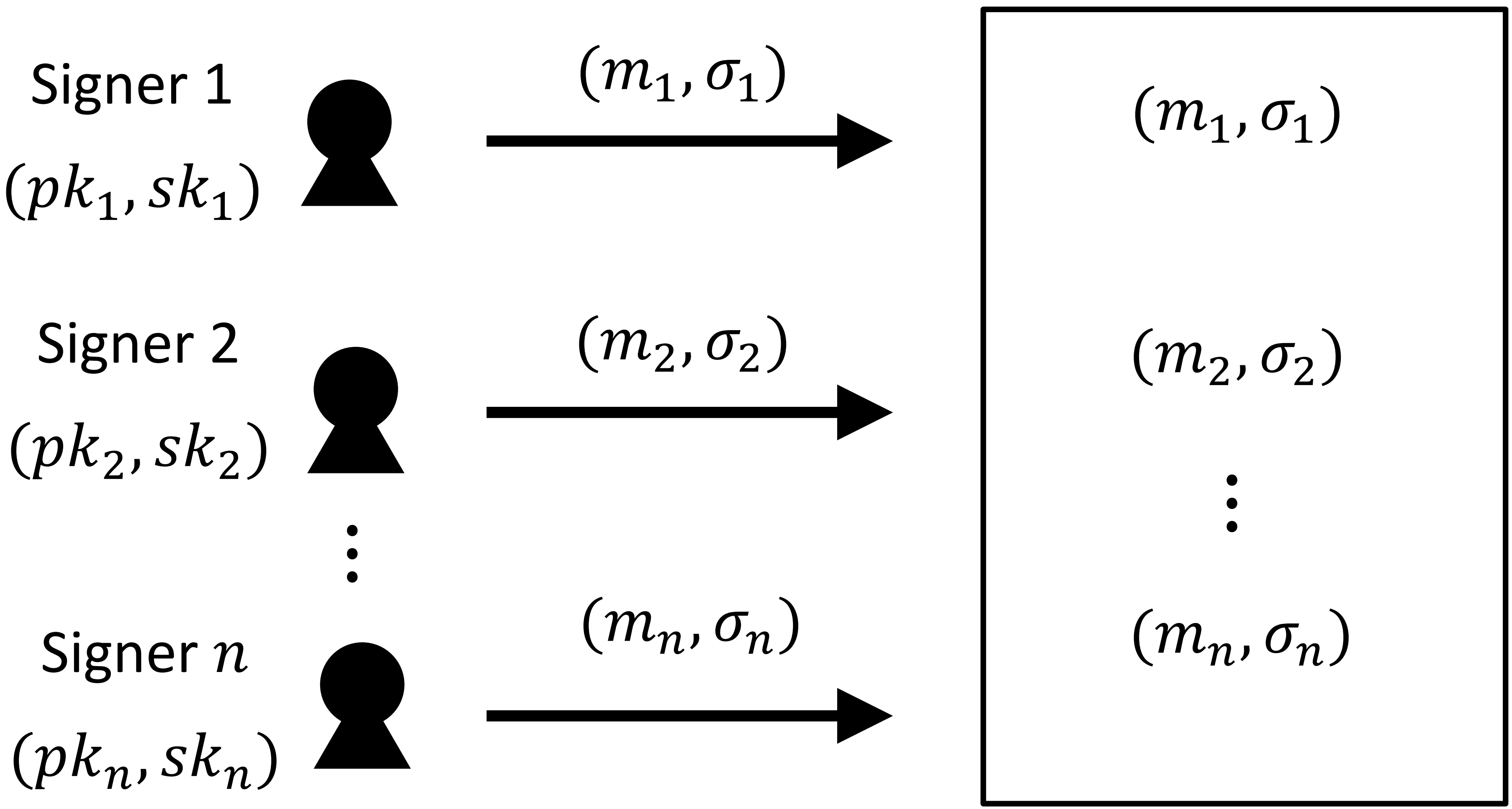
Version: 2020/12/23

ACISP 2020 Full presentation slide

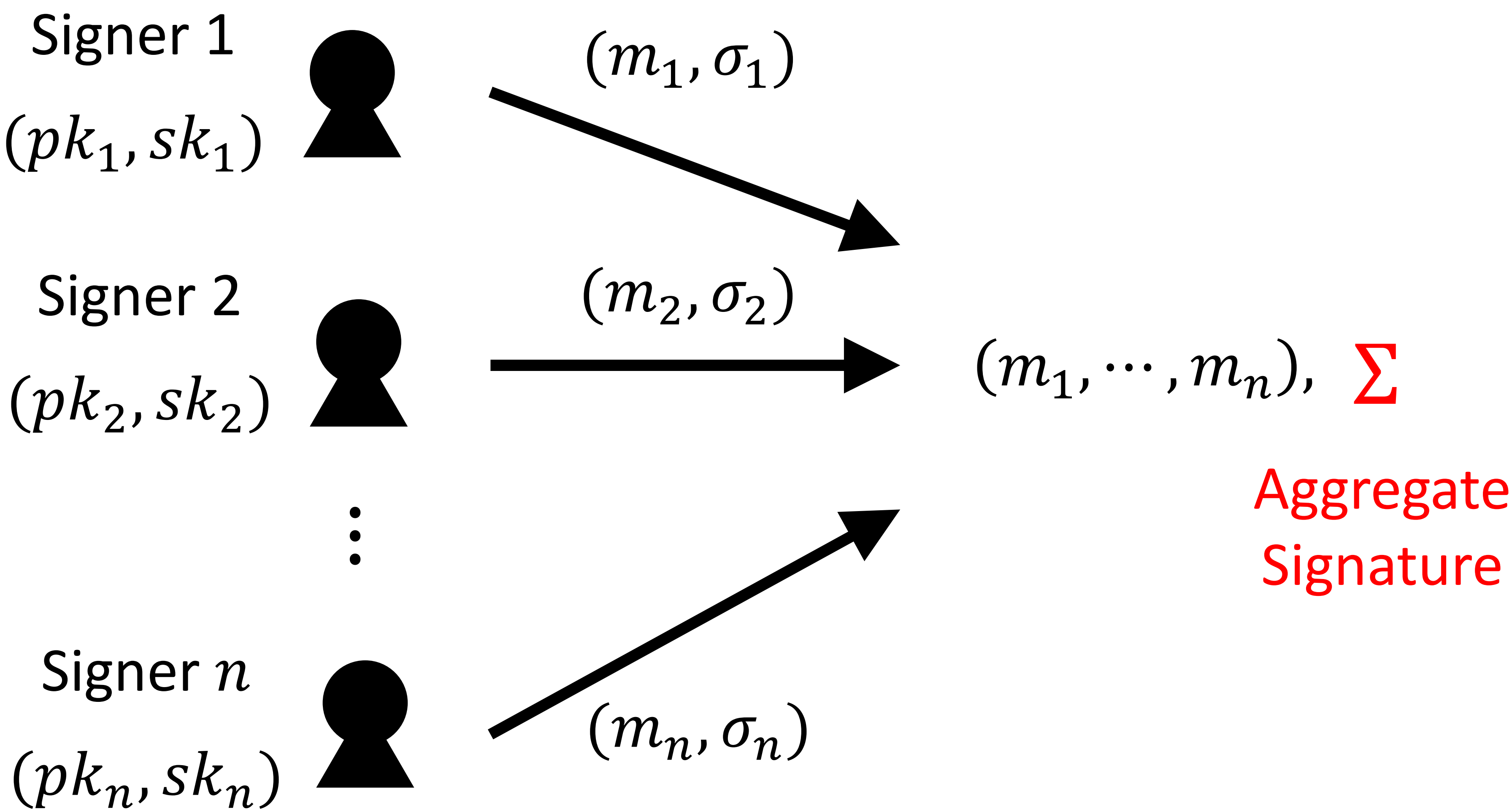
Digital Signature



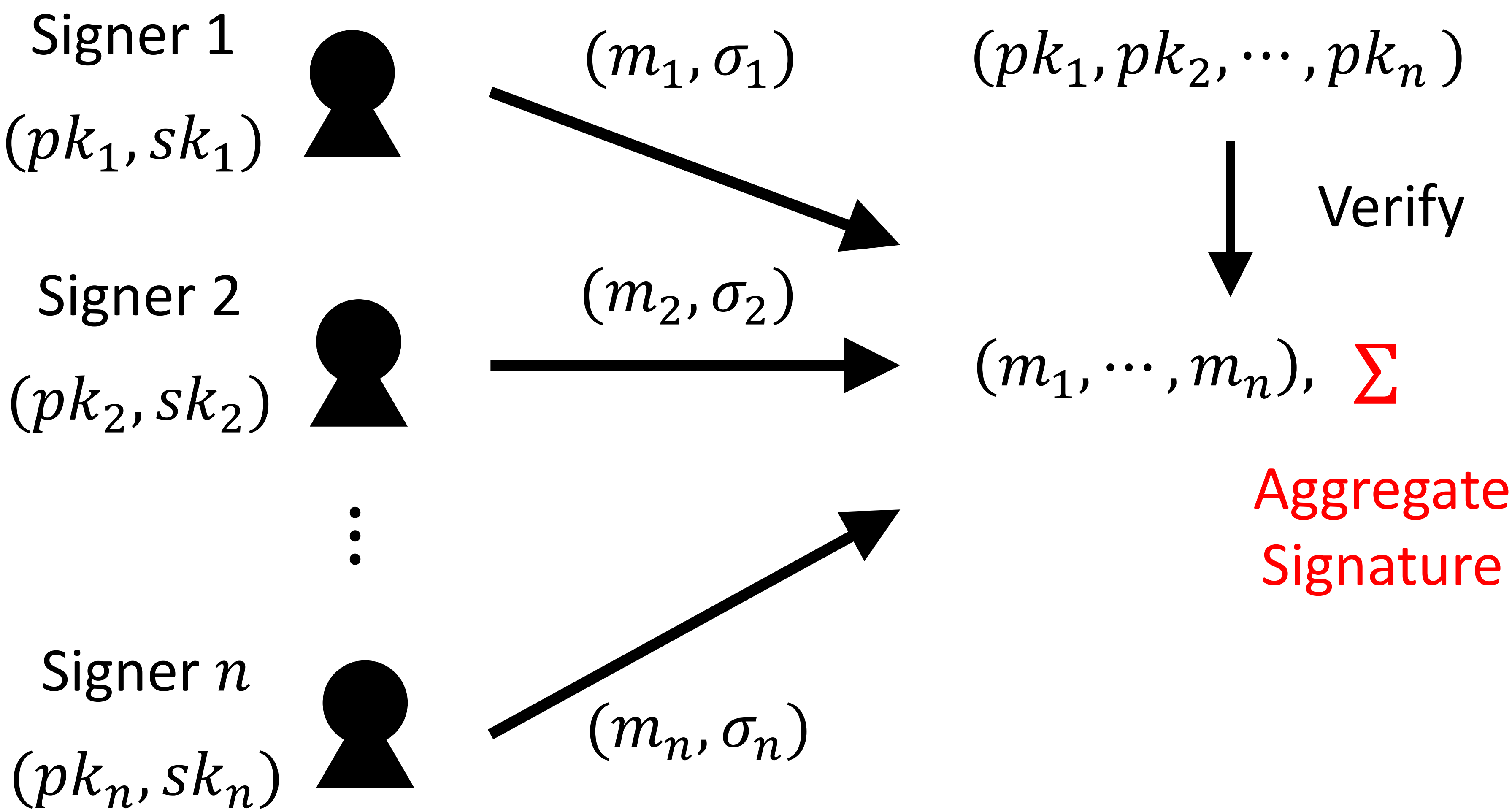
Aggregate Signature



Aggregate Signature



Aggregate Signature

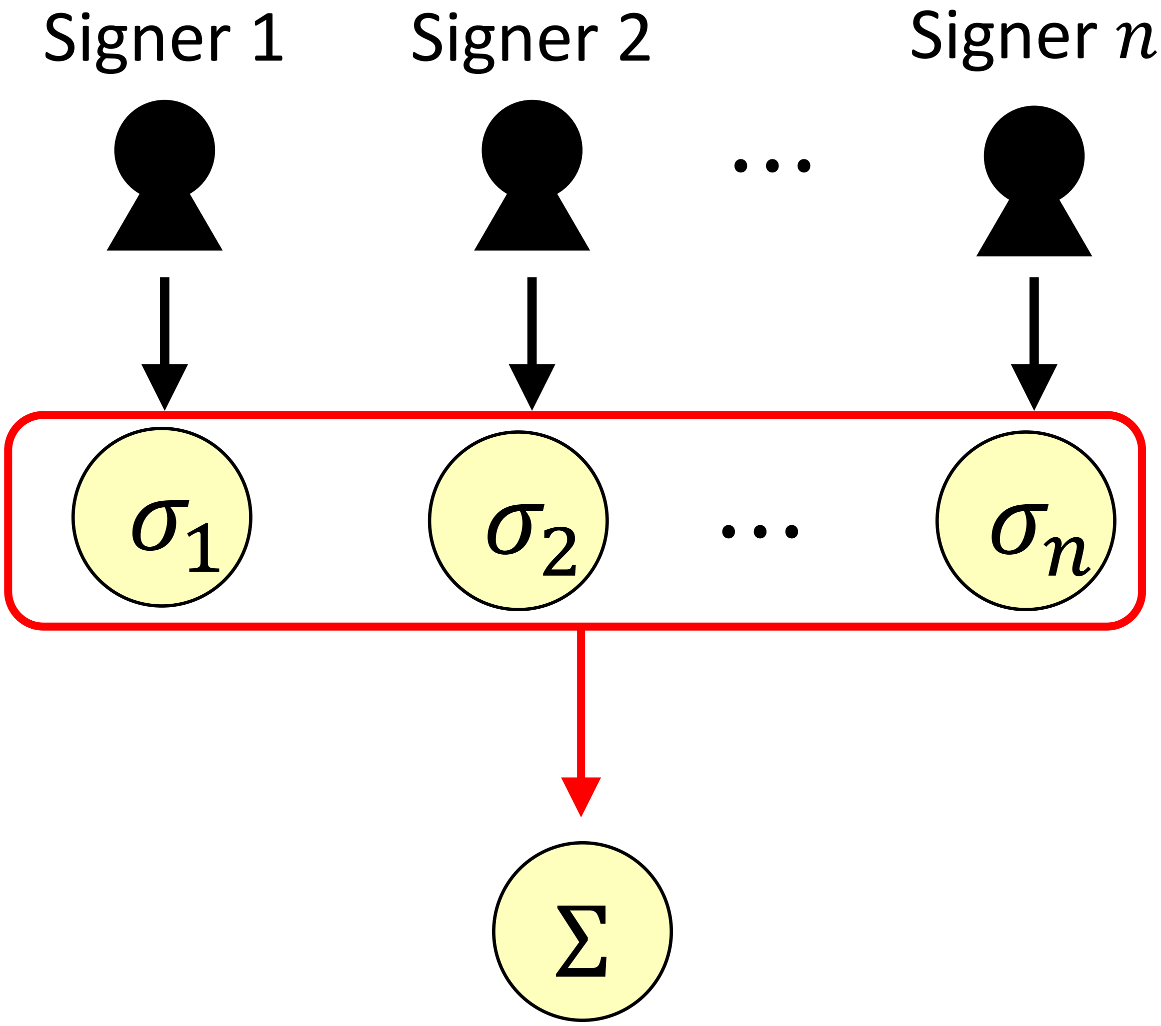


Types of Aggregate Signature

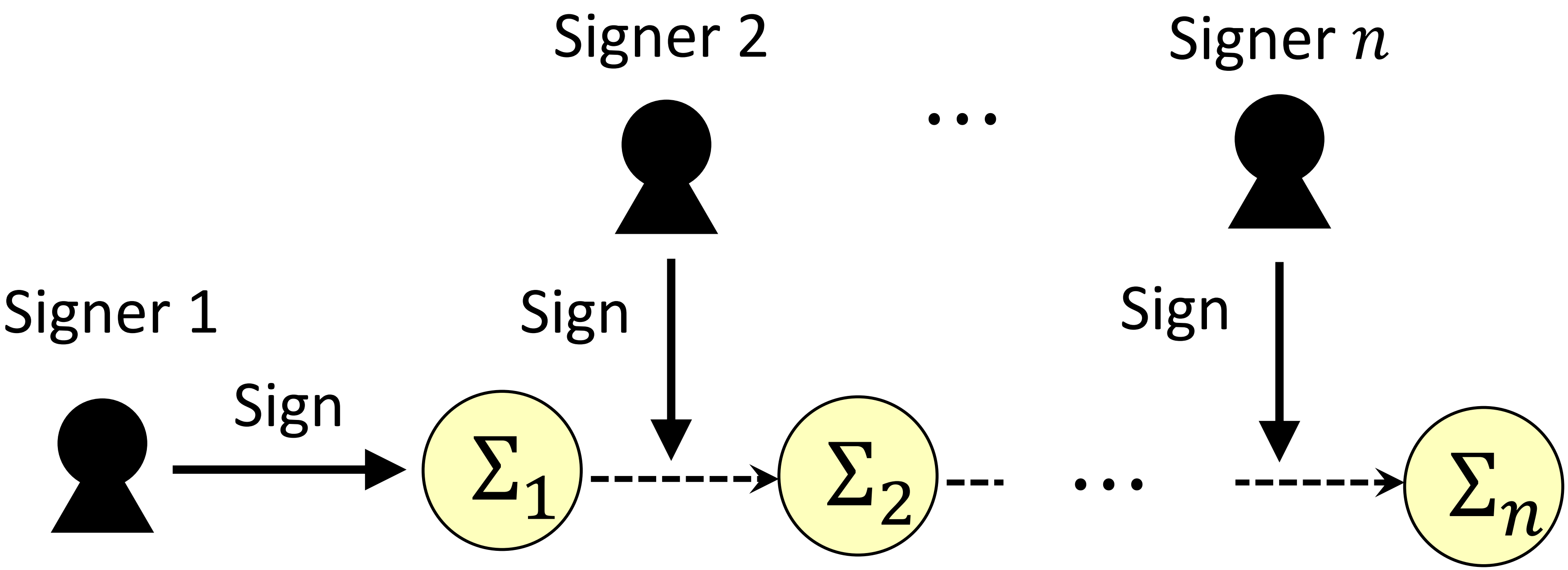
- Full aggregate signature [BGLS03]
- Sequential aggregate signature (SeqAS) [LMRS04]
- Synchronized aggregate signature (SyncAS) [GR06,AGH10]

etc…

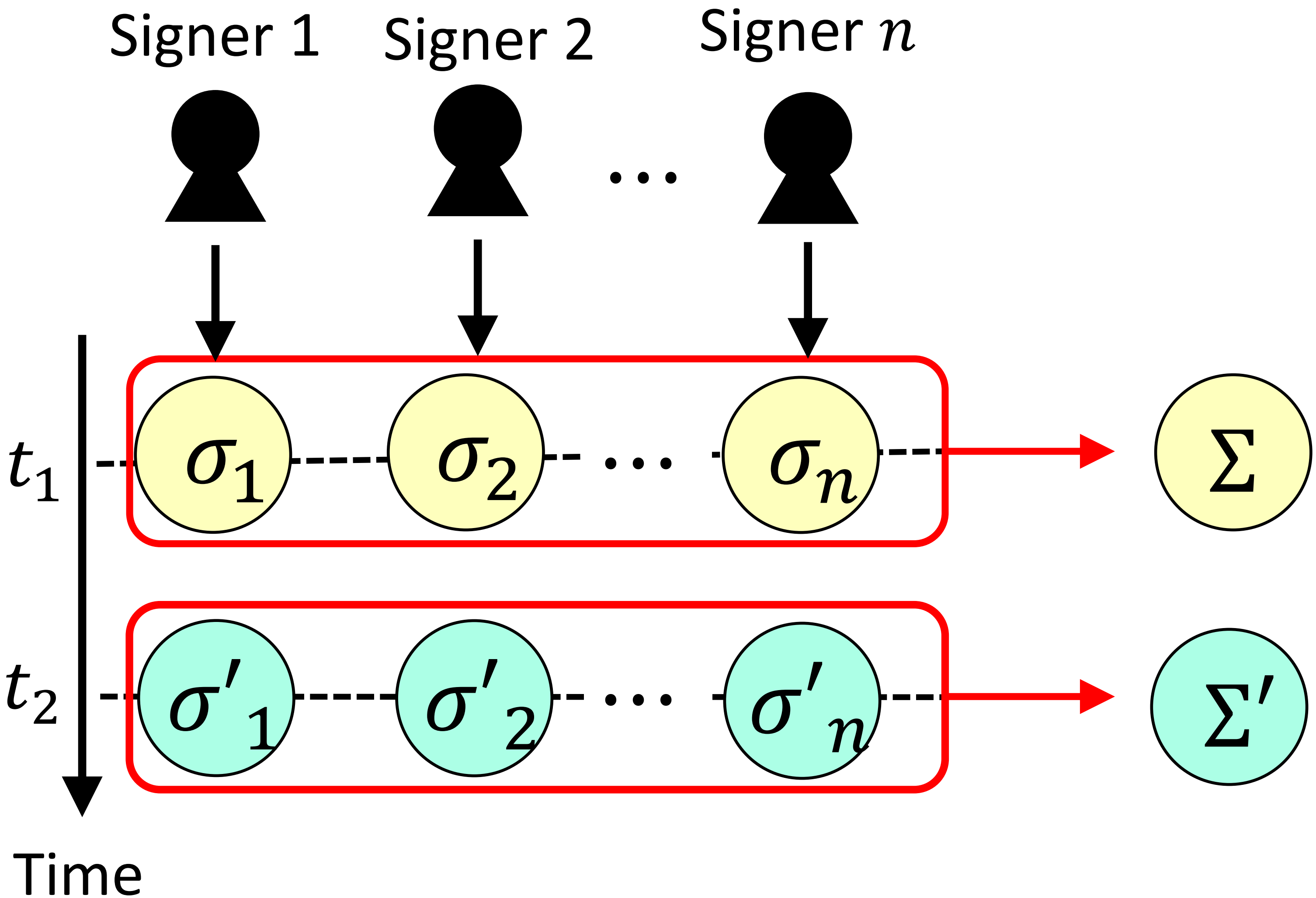
Full Aggregate Signature [BGLS03]



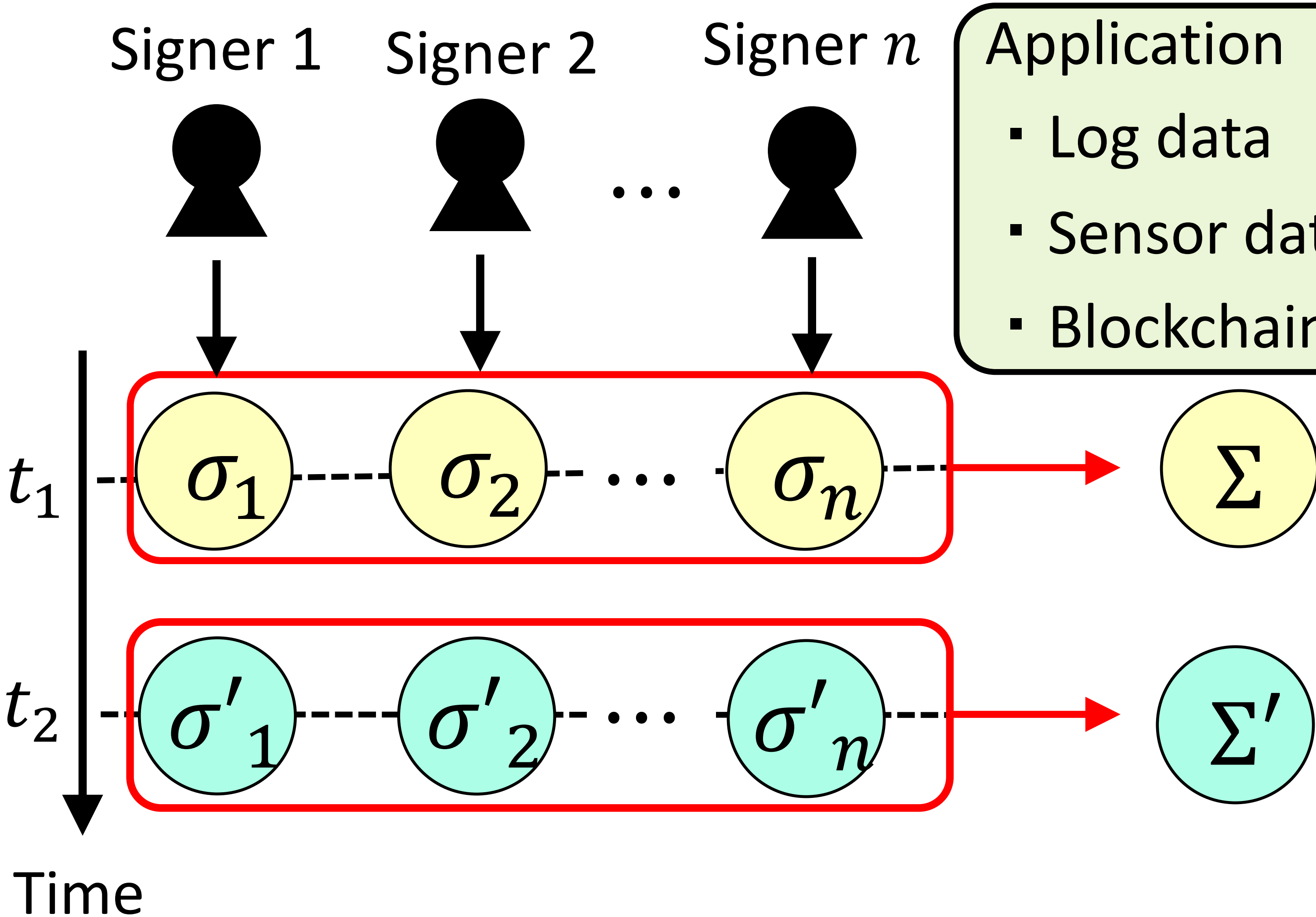
Sequential Aggregate Signature (SeqAS) [LMRS04]



Synchronized Aggregate Signature (SyncAS) [GR06,AGH10]



Synchronized Aggregate Signature (SyncAS) [GR06,AGH10]



Application
- Log data
- Sensor data
- Blockchain protocol

Syntax of SyncAS [AGH 10]

$\mathsf{Setup}(1^\lambda, 1^T) \to pp$

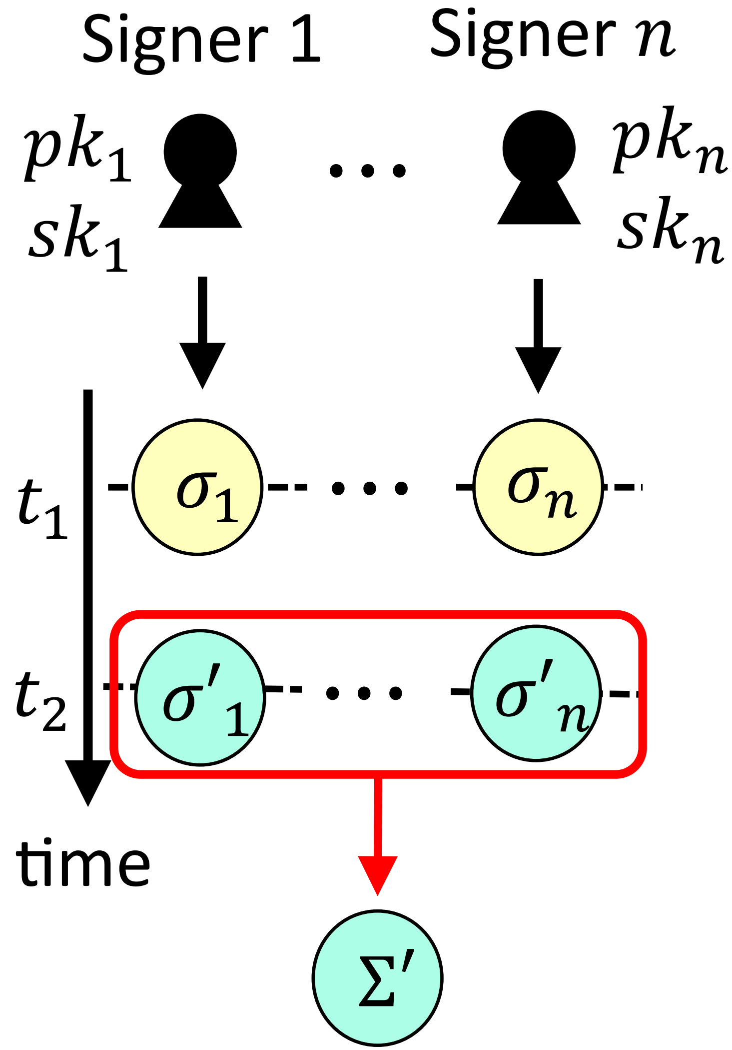
$\mathsf{KeyGen}(pp) \to (pk, sk)$

$\mathsf{Sign}(sk, t, m) \to \sigma$

$\mathsf{Verify}(pk, m, \sigma) \to 0 \text{ or } 1$

$\mathsf{Aggregate}(\{pk_i, m_i, \sigma_i\}_{i=1}^n) \to \Sigma$

$\mathsf{AggVerify}(\{pk_i, m_i\}_{i=1}^n, \Sigma) \to 0 \text{ or } 1$



EUF-CMA Security for SyncAS in the Certified-Key Model [AGH 10]

Challenger

Adversary

EUF-CMA Security for SyncAS in the Certified-Key Model [AGH 10]

Challenger

$pp \leftarrow \mathsf{Setup}(1^\lambda, 1^T)$

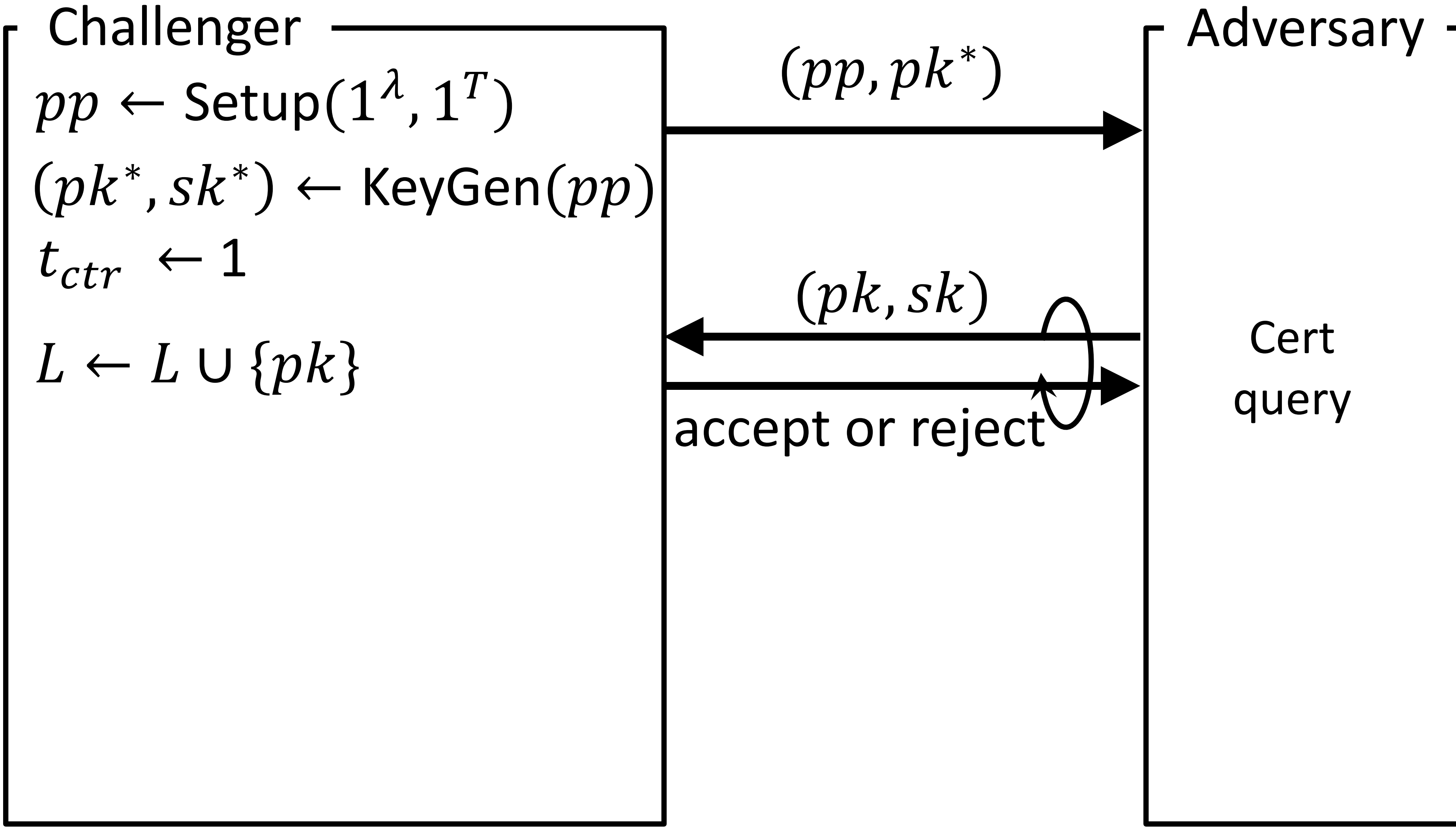
$(pk^*, sk^*) \leftarrow \mathsf{KeyGen}(pp)$

$t_{ctr} \leftarrow 1$

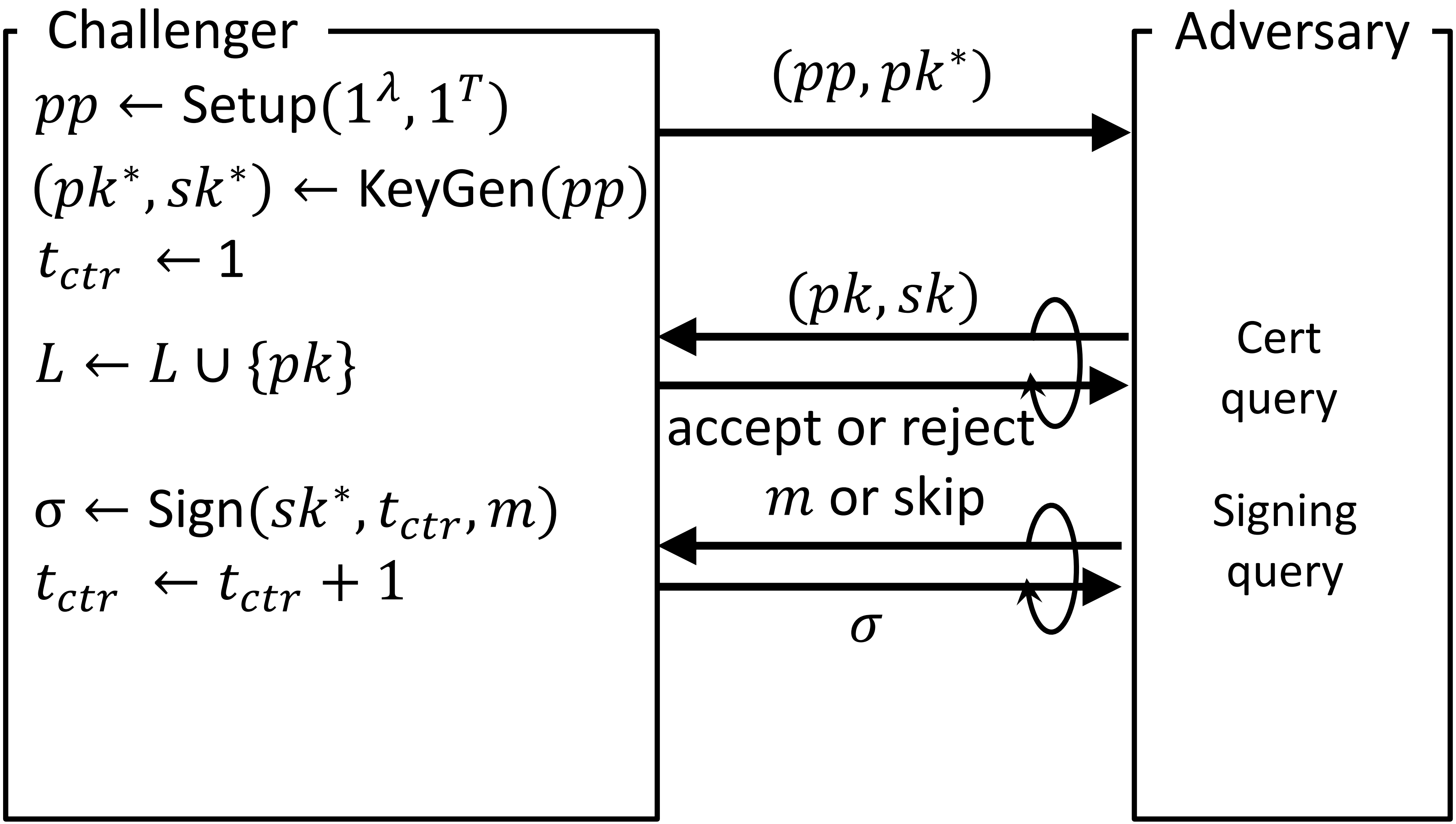
(pp, pk^*) $\longrightarrow$

Adversary

EUF-CMA Security for SyncAS in the Certified-Key Model [AGH 10]



EUF-CMA Security for SyncAS in the Certified-Key Model [AGH 10]



EUF-CMA Security for SyncAS in the Certified-Key Model [AGH 10]

Challenger

$pp \leftarrow \mathsf{Setup}(1^\lambda, 1^T)$

$(pk^*, sk^*) \leftarrow \mathsf{KeyGen}(pp)$

$t_{ctr} \leftarrow 1$

(pp, pk^*)

Cert query

(pk, sk)

$L \leftarrow L \cup \{pk\}$

accept or reject

Signing query

m or skip

$\sigma \leftarrow \mathsf{Sign}(sk^*, t_{ctr}, m)$

$t_{ctr} \leftarrow t_{ctr} + 1$

σ

Adversary

$$\begin{pmatrix} (pk_1, \cdots, pk_i = pk^*, \cdots, pk_n), \\ (m_1, \cdots, m_i, \cdots, m_n), \Sigma) \end{pmatrix}$$

EUF-CMA Security for SyncAS in the Certified-Key Model [AGH 10]

The adversary wins if:

1. $\begin{pmatrix} (pk_1, \cdots, pk_i = pk^*, \cdots, pk_n), \\ (m_1, \cdots, m_i, \cdots, m_n), \Sigma) \end{pmatrix}$ is valid.

2. Never queried m_i for the signing oracle.

3. All keys $(pk_1, \cdots, pk_n)$ are registered.

SyncAS Based on Bilinear Group

Scheme	Assumption	pk size	Agg sig size	Agg Ver (in paringig)
GR06	CDH + ROM	ID	3	3
AGH10	CDH	1	3	$k+3$
AGH10	CDH + ROM	1	2	4
LLY13	OT-LRSW + ROM	1	2	3

Most efficient scheme

SyncAS Based on Bilinear Group

Scheme	Assumption	pk size	Agg sig size	Agg Ver (in parinig)
GR06	CDH + ROM	ID	3	3
AGH10	CDH	1	3	$k + 3$
AGH10	CDH + ROM	1	2	4
LLY13	OT-LRSW + ROM	1	2	3

Most efficient scheme

☹ Interactive assumption !

Non-Interactive Assumption

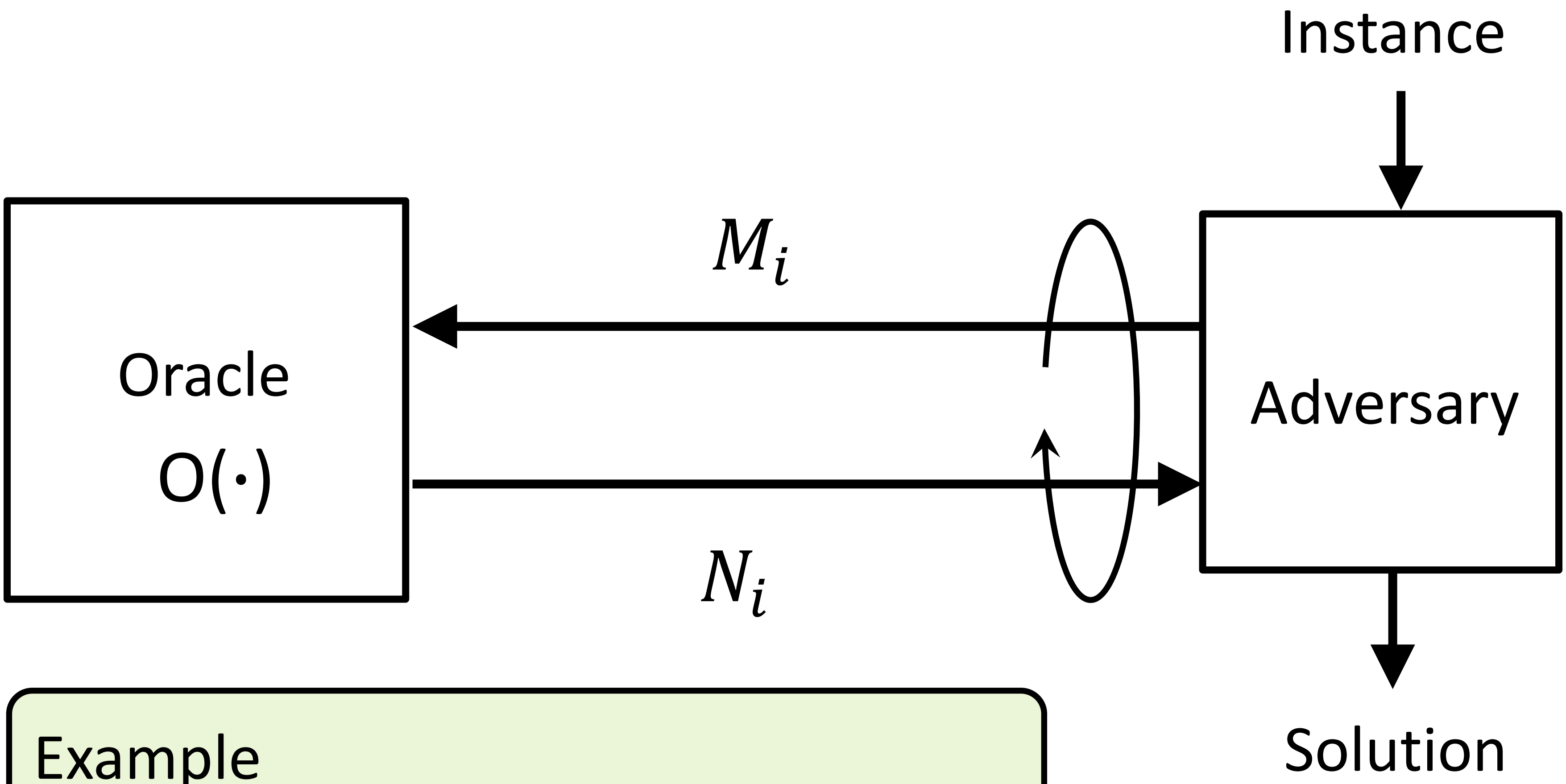
Example

DDH, CDH, DL,

SXDH, qSDH

etc...

Interactive Assumption

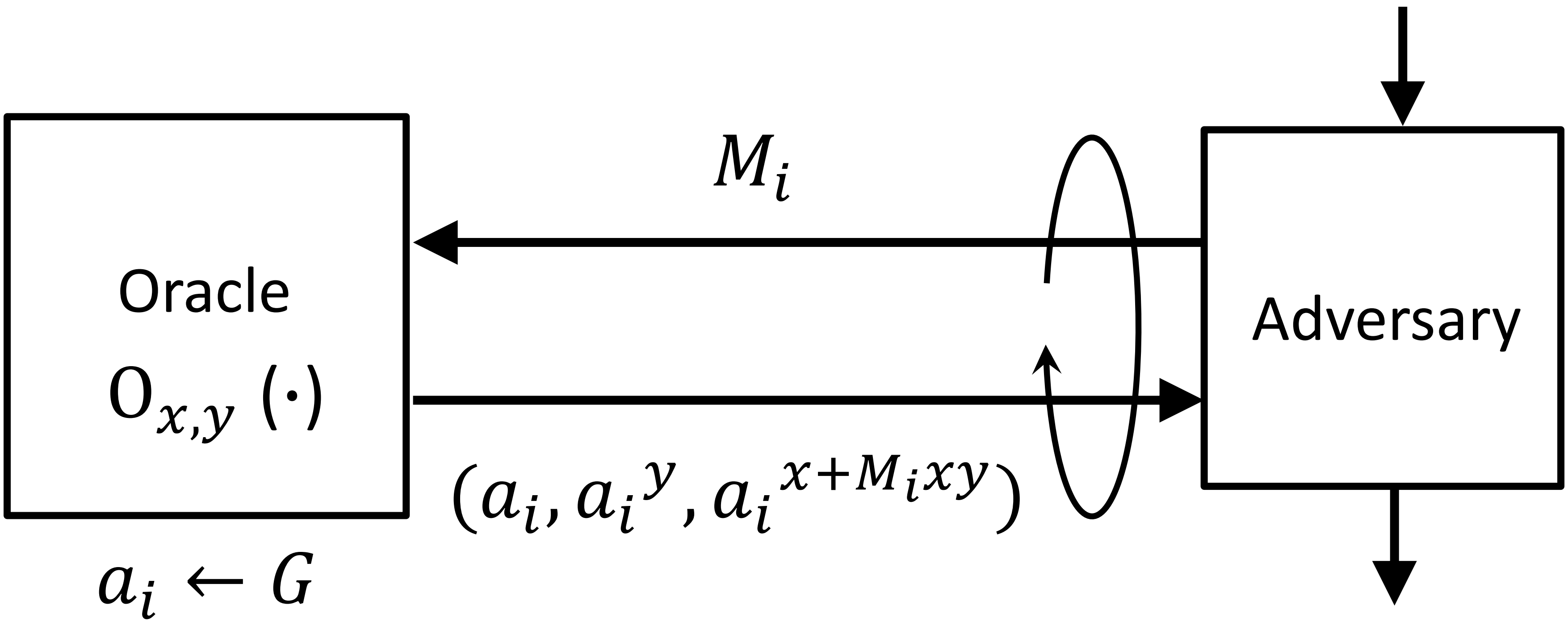


Example

LRSW [LRSW99], PS [PS16] etc…

(OT-)LRSW Assumption [LRSW99]

Instance $(p, G, G_T, e, g, X = g^x, Y = g^y)$



Solution (M, a, b, c)

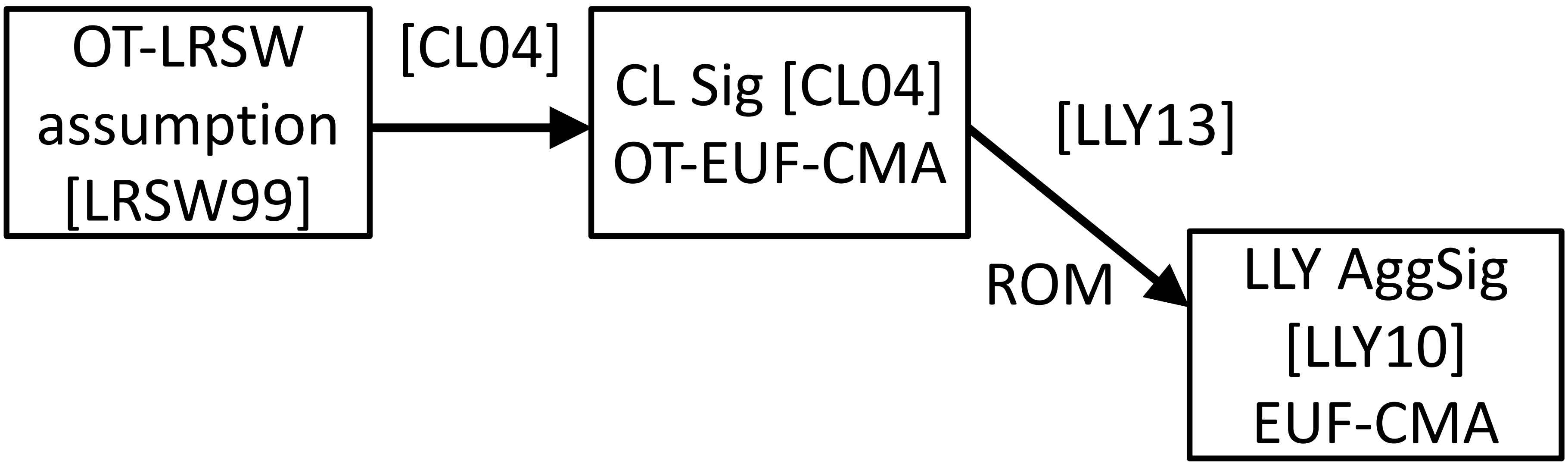
$M \notin \{M_i\}, M \in Z_p^*, a \in G, b = a^y, c = a^{x+Mxy}$

Our Contribution

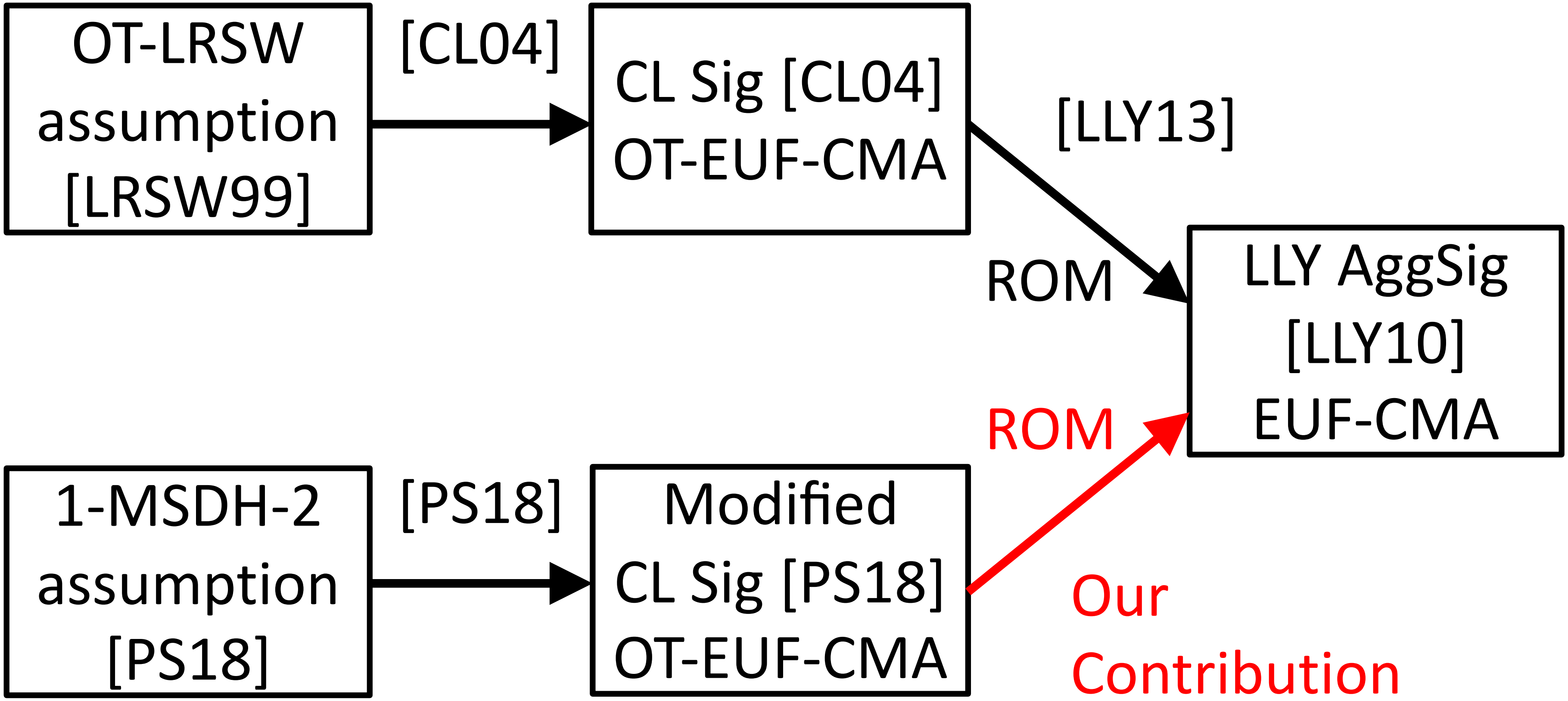
Scheme	Assumption	pk size	Agg sig size	Agg Ver (parinig)
GR06	CDH + ROM	ID	3	3
AGH10	CDH	1	3	$k + 3$
AGH10	CDH + ROM	1	2	4
LLY13	$\boxed{\text{OT-LRSW}}$ + ROM	1	2	3
LLY13 (New Proof)	$\boxed{\text{1-MSDH-2}}$ + ROM			

☺ Non-interactive and static assumption !

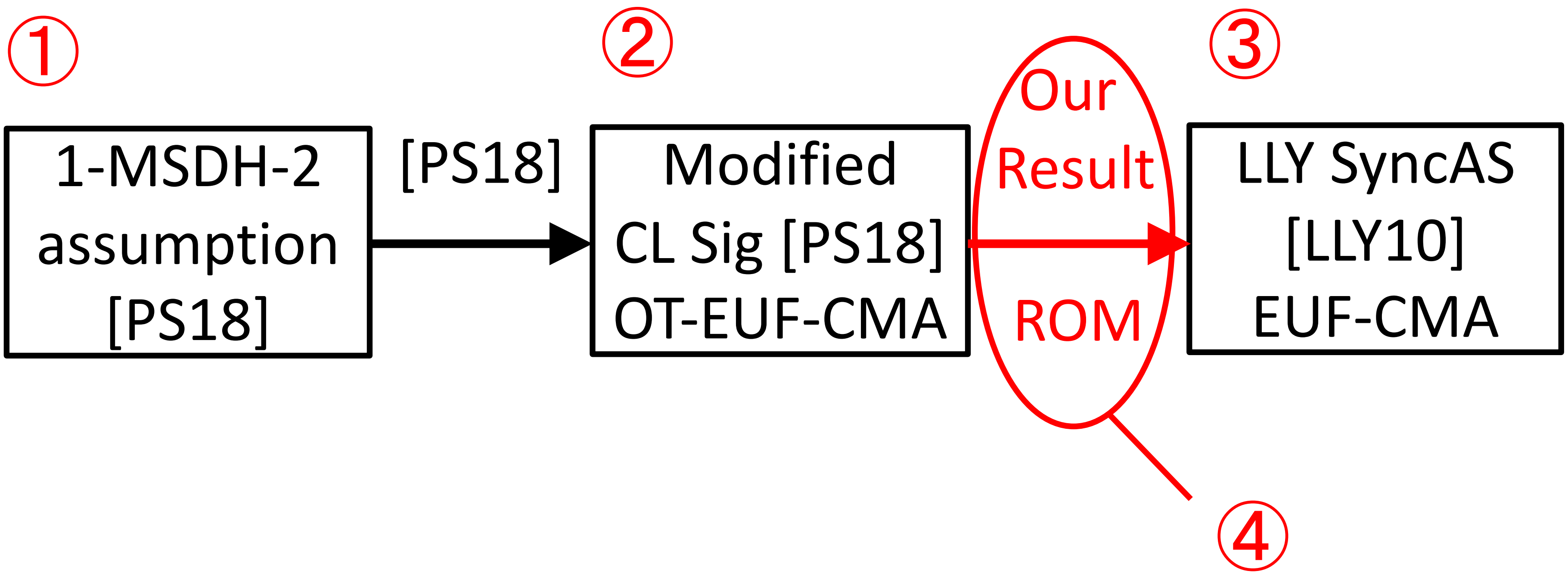
Security proof for LLY SyncAS



Security proof for LLY SyncAS



Our Contribution



① q-MSDH-2 Assumption [PS18]

Instance $\left(p, G, G_T, e, g, \left\{g^{x^i}, g^{b\cdot x^i}\right\}_{i=1}^{q+1}, g^{a}, g^{abx}\right)$

$\downarrow$

Adversary

$\downarrow$

Solution $\left(w, P, h^{\frac{1}{x+w}}, h^{\frac{a}{x\cdot P(x)}}\right)$

$w \neq 0, \deg(\mathrm{P}) \leq q,$

$X + w$ and $P(X)$ are relative prime.

If we fix $q = 1$,
we can regard 1-MSDH-2
as a static assumption.

② Modified CL Signature (MCL Sig) [PS18]

$pp = (p, G, G_T, e)$

KeyGen(pp)

$sk = (x, y, z) \leftarrow {Z_p}^3$

$g \leftarrow G^*, X \leftarrow g^x,$

$Y \leftarrow g^y, Z \leftarrow g^z$

$pk = (g, X, Y, Z)$

Sign$(sk, m \in Z_p)$

$m' \leftarrow Z_p, A \leftarrow G^*, B \leftarrow A^y$

$C \leftarrow A^z, D \leftarrow C^y, E \leftarrow A^x B^{mx} D^{m'x}$

$\sigma \leftarrow (m', A, B, C, D, E)$

Verify(pk, m, σ)

$e(A, Y) = e(B, g)$?

$e(A, Z) = e(C, g)$?

$e(C, Y) = e(D, g)$?

$e(AB^m D^{m'}, X) = e(E, g)$?

② Modified CL Signature (MCL Sig) [PS18]

Theorem [PS18]

If the q-MSDH-2 assumption holds,
the modified CL signature is EUF-CMA secure.
(q is a bound on the number of signing queries.)

We only use

If the 1-MSDH-2 assumption holds,
the modified CL signature is OT-EUF-CMA secure.

③ LLY SyncAS [LLY13]

$pp = (p, G, G_T, e, g, H_1, H_2, H_3)$

Public key and Secret key

$$sk_i = x_i \leftarrow Z_p, \quad pk_i = X_i \leftarrow g^{x_i}$$

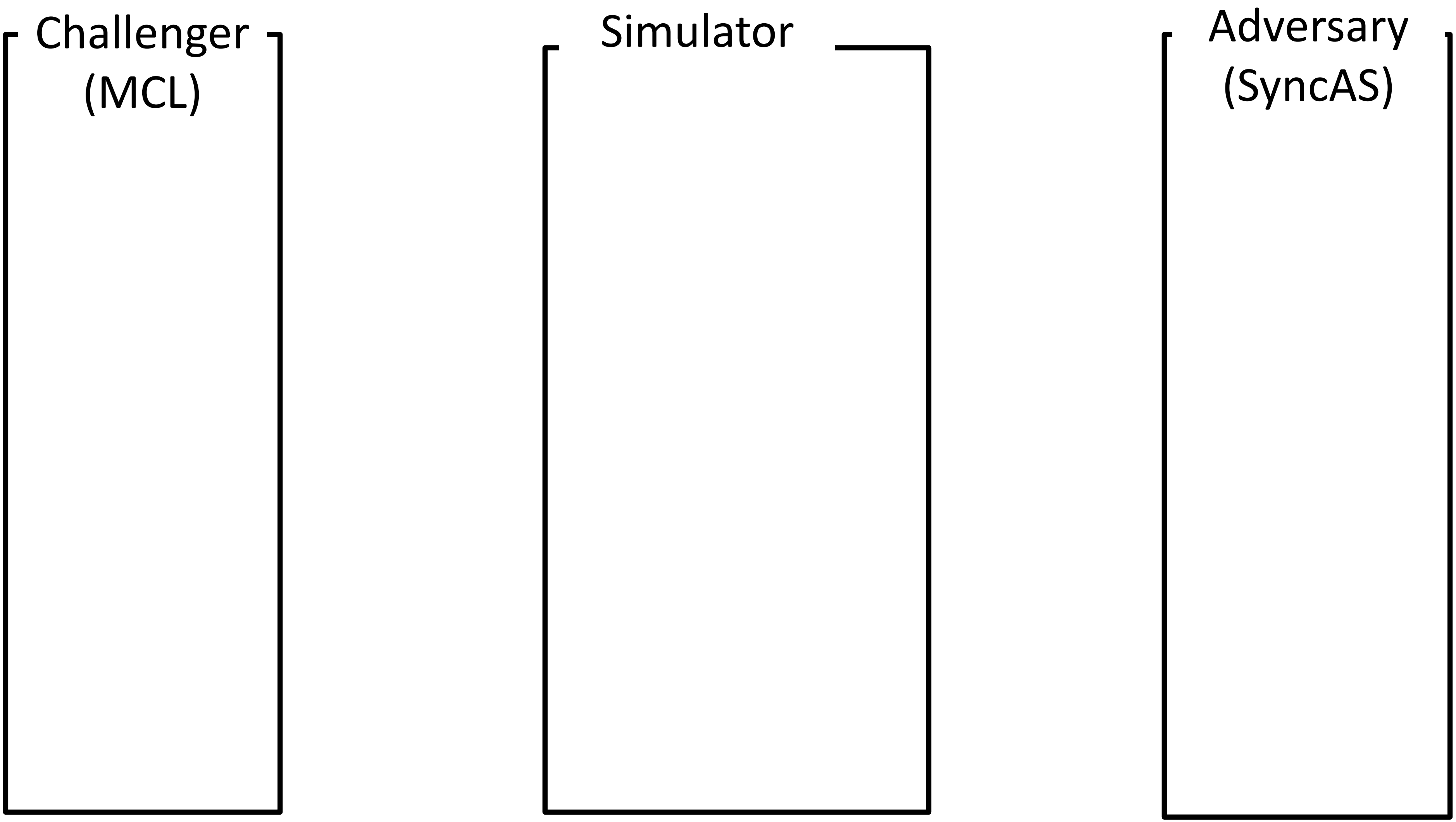
Signature on a message $m \in Z_p$ in time period t

$$E_i \leftarrow H_1(t)^{x_i} \cdot H_2(t)^{H_3(t,m_i)x_i}, \sigma \leftarrow (E_i, t)$$

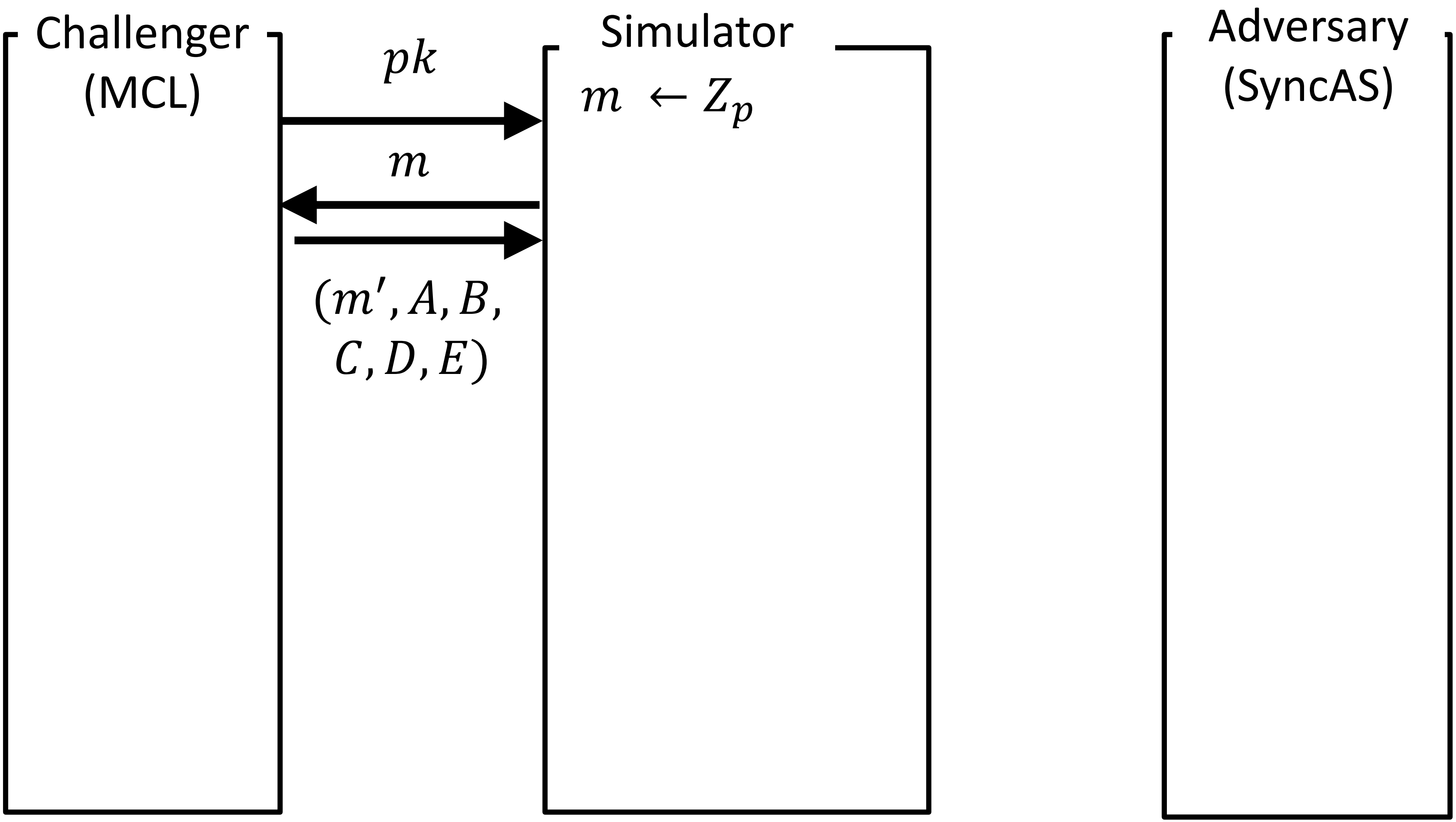
Aggregate signature

$$E \leftarrow \prod_{i=1}^{n} E_i = \prod_{i=1}^{n} H_1(t)^{x_i} \cdot H_2(t)^{H_3(t,m_i)x_i}$$
$$\Sigma \leftarrow (E, t)$$

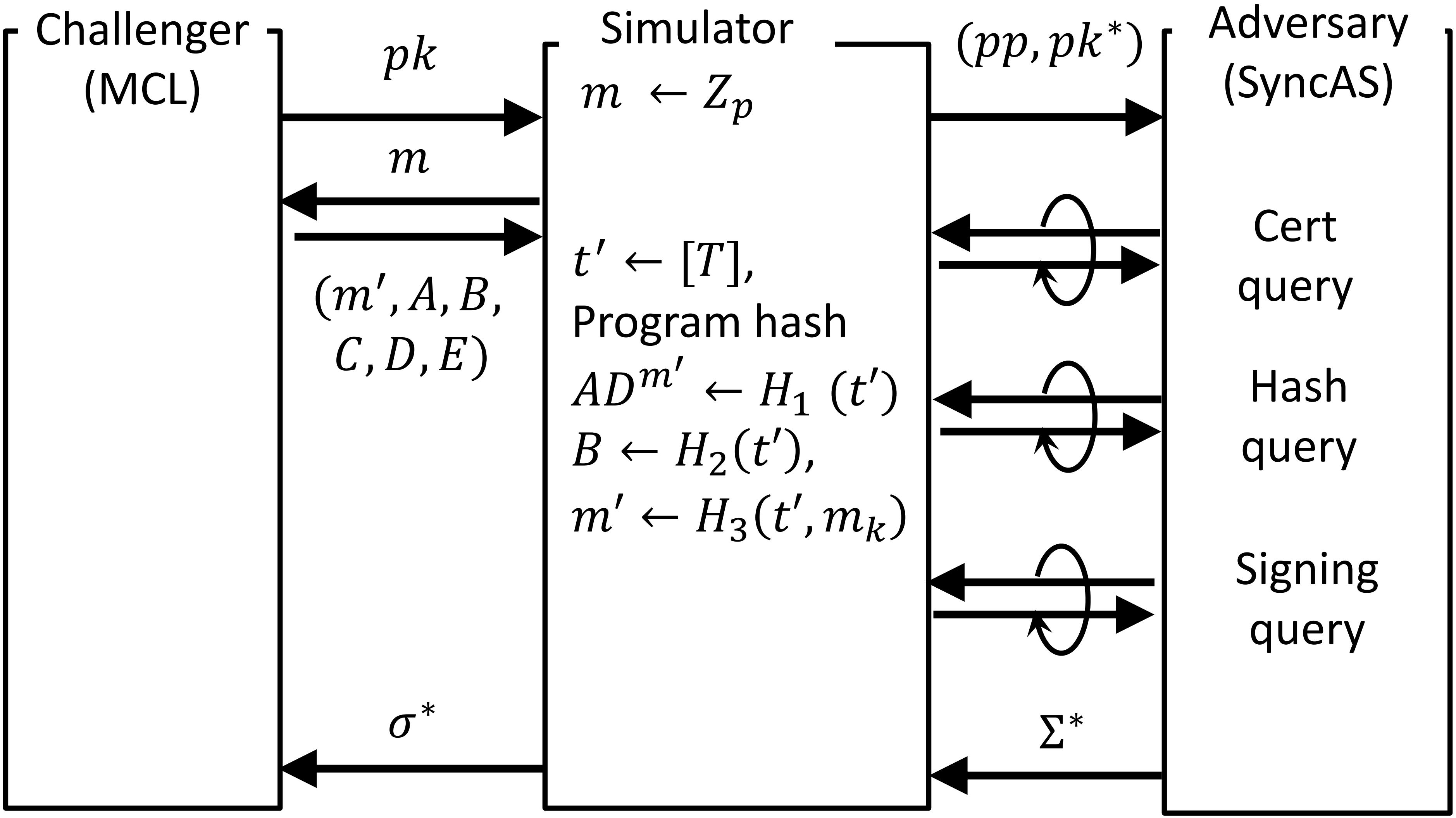
④ Overview of Our Security Proof



④ Overview of Our Security Proof



④ Overview of Our Security Proof



④ Conversion from MCL Sig to LLY SyncAS

MCL signature

$$\sigma_i \leftarrow (m_i{}', A_i, B_i \leftarrow A_i{}^{y_i}, C_i \leftarrow A_i{}^{y_i}, D_i \leftarrow C_i{}^{y_i},$$
$$E_i \leftarrow A_i{}^{x_i} D_i{}^{m_i{}' x_i} B_i{}^{m_i x_i})$$

I. Force signers to use same $m_i{}', A_i, B_i, C_i, D_i$.

$$\Sigma \leftarrow \left(m', A, B, C, D, E = \prod_{i=1}^{n} E_i = \prod_{i=1}^{n} \left(\left(A D^{m'} \right)^{x_i} B^{m_i x_i} \right), t \right)$$

II. Change $AD^{m'}$ to $H_1(t)$, B to $H_2(t)$,
m_i to $H_3(t, m_i)$.

$$\Sigma \leftarrow \left(E = \prod_{i=1}^{n} E_i = \prod_{i=1}^{n} H_1(t)^{x_i} H_2(t)^{H_3(t, m_i) x_i}, t \right)$$

References 1/2

[AGH10] Ahn, Green, and Hohenberger.
Synchronized aggregate signatures: new definitions, constructions and applications. (ACM CCS 2010)

[BGLS03] Boneh, Gentry, Lynn,and Shacham.
Aggregate and verifiably encrypted signatures from bilinear maps. (EUROCRYPT 2003)

[CL04] Camenisch and Lysyanskaya.
Signature schemes and anonymous credentials from bilinear maps. (CRYPTO 2004)

[GR06] Gentry and Ramzan.
Identity-based aggregate signatures. (PKC 2006)

References 2/2

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

[LLY 13] Lee, Lee, and Yung.
Aggregating CL-signatures revisited: Extended functionality and better efficiency. (FC 2013)

[LRSW99] Lysyanskaya, Rivest, Sahai, and Wolf.
Pseudonym systems. (SAC1999)

[PS16] Pointcheval and Sanders.
Short Randomizable Signatures. (CT-RSA 2016)

[PS18] Pointcheval and Sanders.
Reassessing security of randomizable signatures. (CT-RSA 2018)

Appendix: Modified CL Signature

$pp = (p, G, G_T, e)$

KeyGen(pp)

$sk = (x, y, z) \leftarrow Z_p$

$g \leftarrow G^*, X \leftarrow g^x,$

$Y \leftarrow g^y, Z \leftarrow g^z$

$pk = (g, X, Y, Z)$

Verify(pk, m, σ)

$e(A, Y) = e(B, g)$?

$e(A, Z) = e(C, g)$?

$e(C, Y) = e(D, g)$?

$e(AB^m D^{m'}, X) = e(E, g)$?

Sign(sk, m)

$m' \leftarrow Z_p, A \leftarrow G^*, B \leftarrow A^y$

$C \leftarrow A^z, D \leftarrow C^y, E \leftarrow A^x B^{mx} D^{m'x}$

$\sigma \leftarrow (m', A, B, C, D, E)$