A $t\text{-}out\text{-}of\text{-}n$ redactable signature scheme

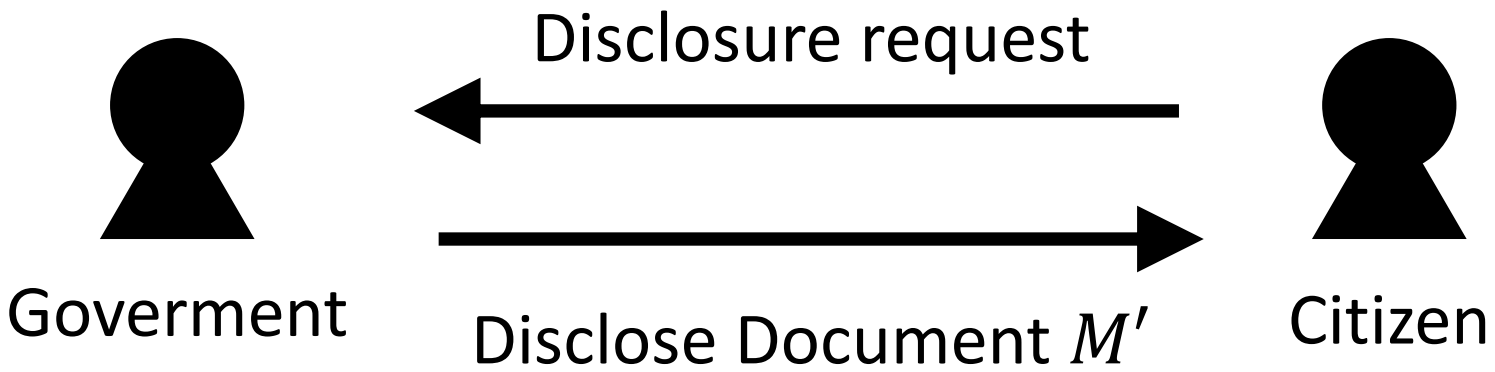
Masayuki Tezuka, Xiangyu Su, Keisuke Tanaka

Tokyo Institute of Technology

Version: 2020/12/23

CANS 2019 Full presentation slide

Digital signature scheme

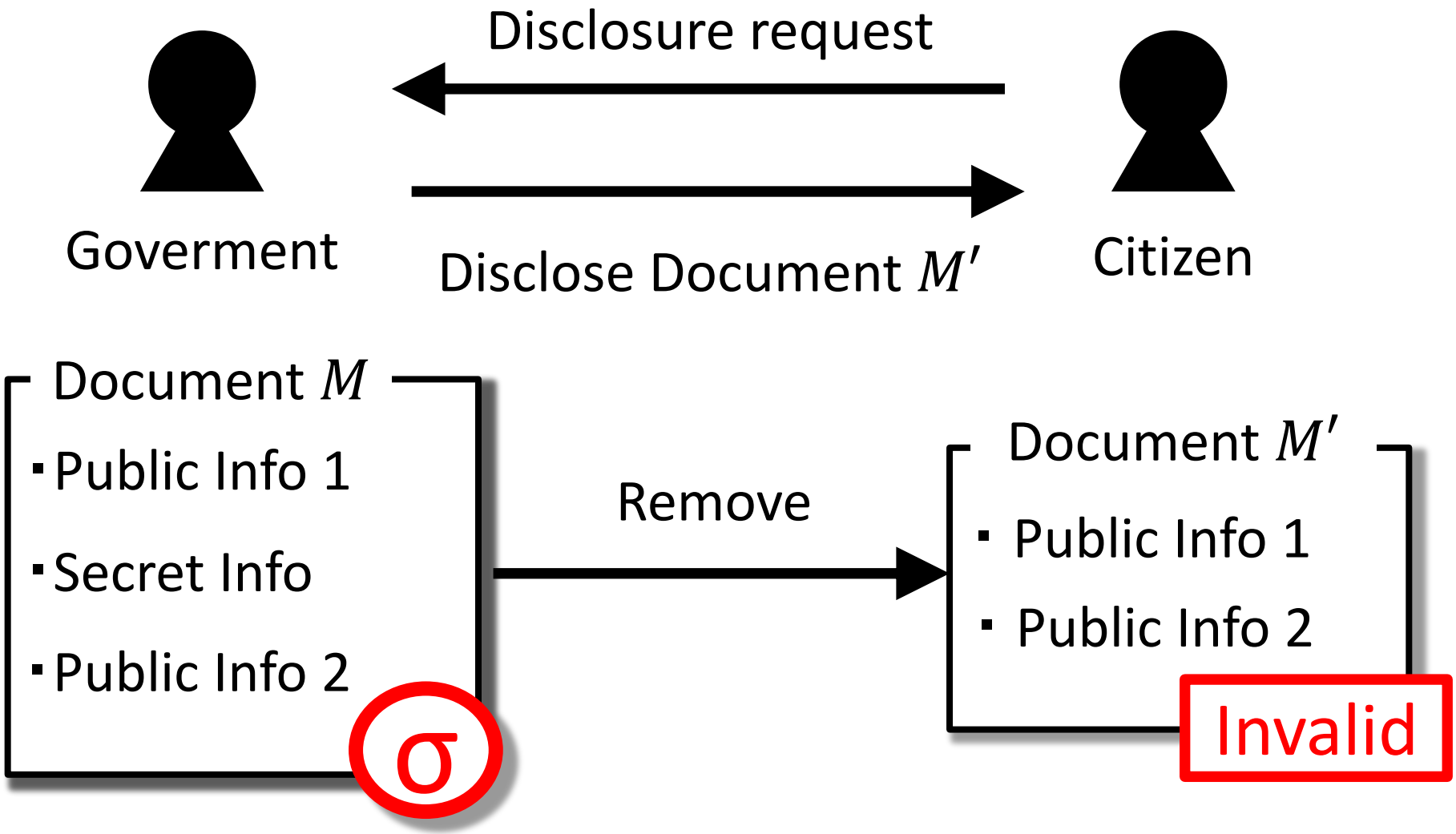


Document M

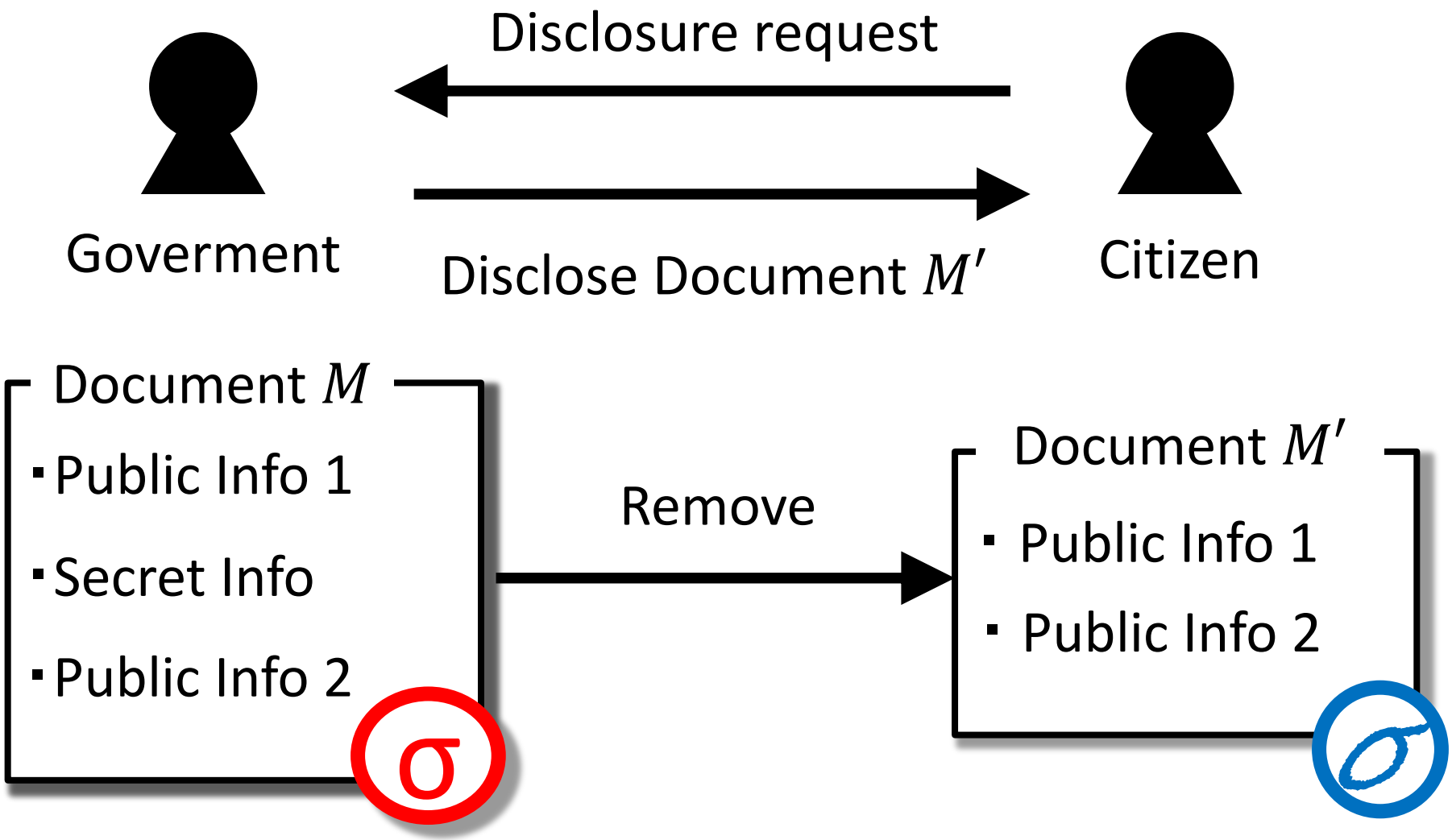
- Public Info 1
- Secret Info
- Public Info 2

σ

Digital signature scheme



What is redactable signature scheme ?



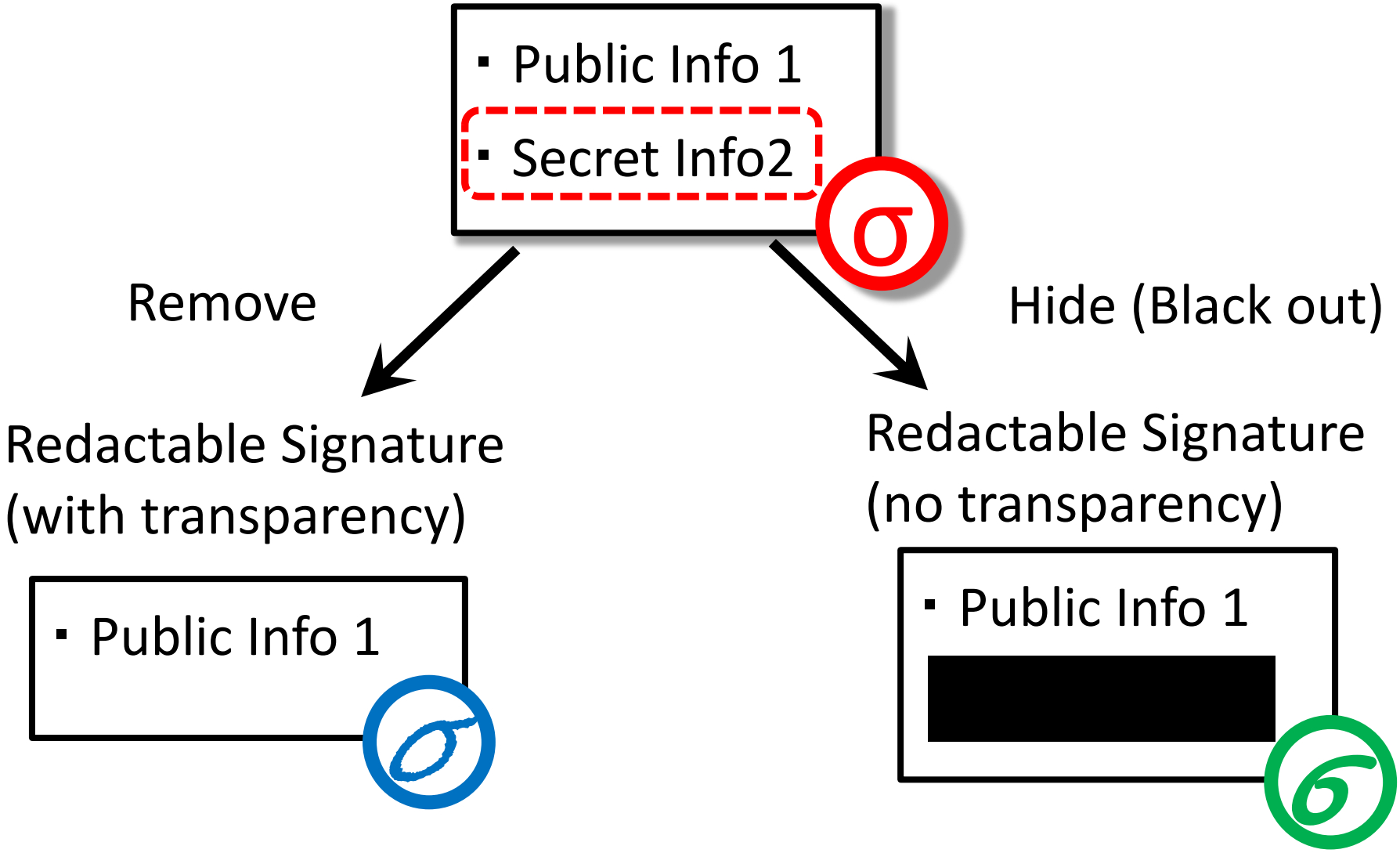
Pioneerings of redactable signatature scheme

- Steinfeld, Bull, Zheng (ICISC'01)
  - ➡ Content extraction signature

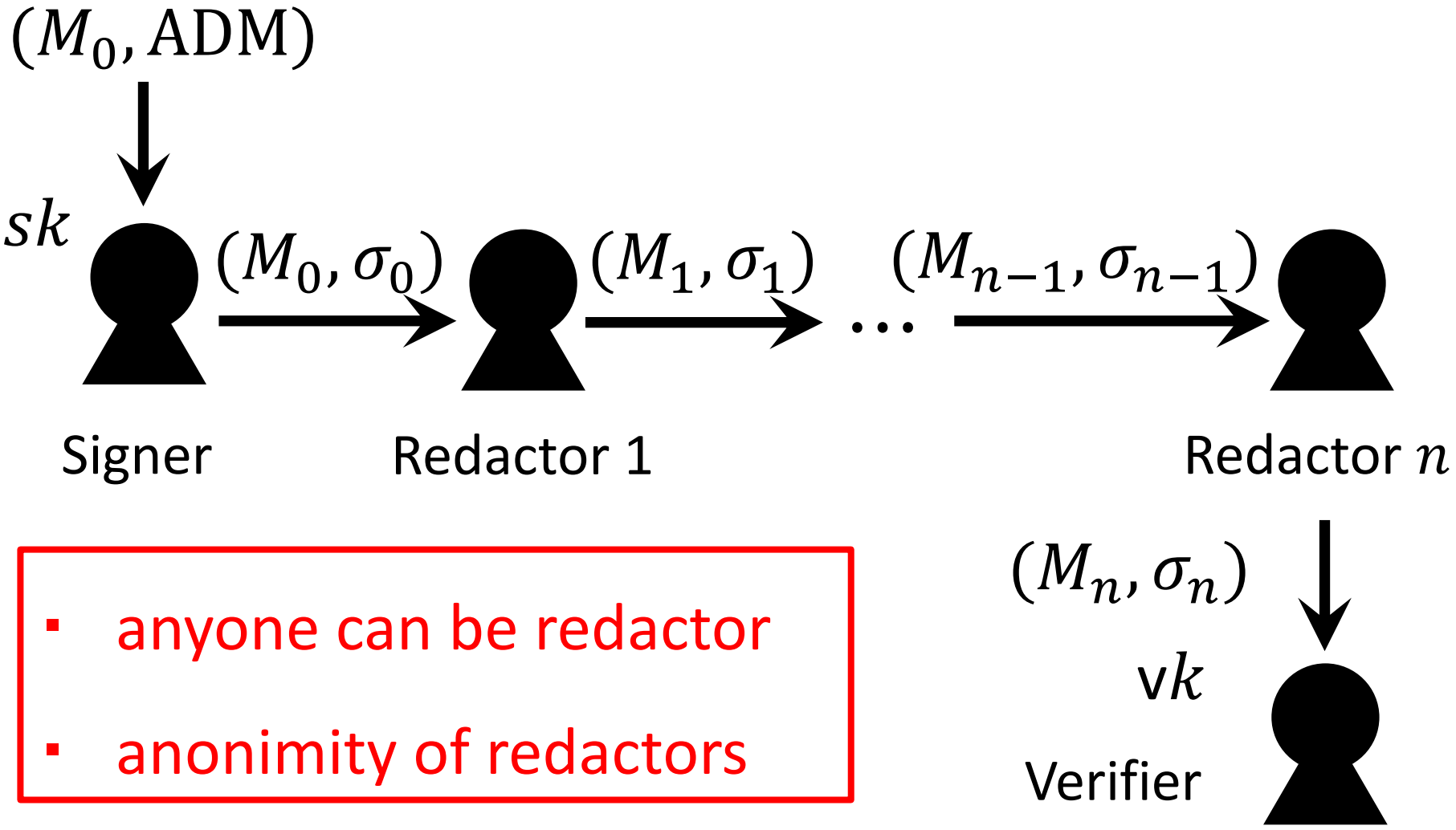
- Johnson, Molnar, Song, Wagner (CT-RSA'02)
  - ➡ Redactable signature

- Miyazaki, Susaki, Iwamura, Matsumoto, Sasaki, Yoshiura (IEICE'03)
  - ➡ Digital document sanitizing problem, SUMI-4

Types of redactable signature



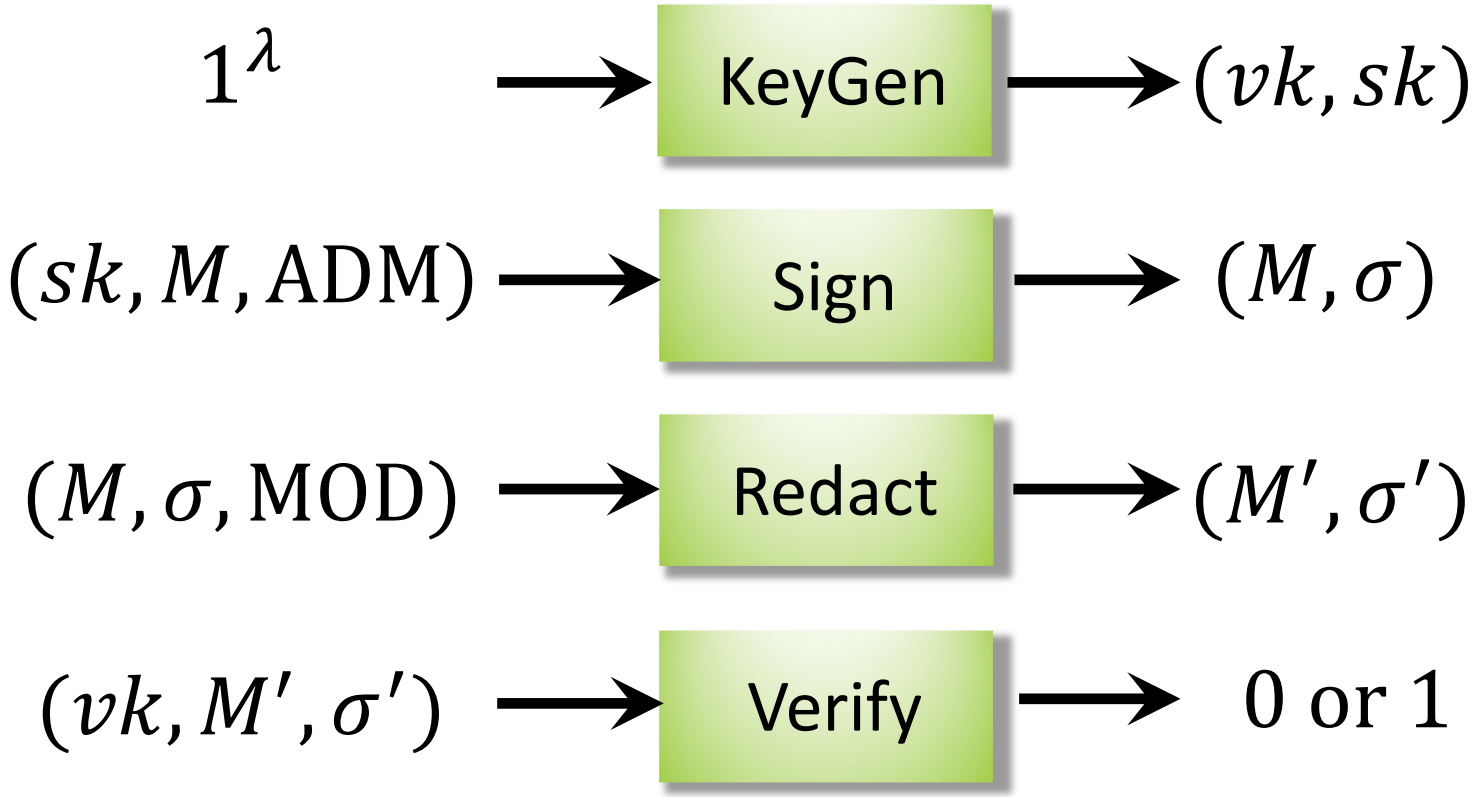
Redactable signature scheme



- anyone can be redactor
- anonimity of redactors

Syntax of redactable signature scheme

Derler, Pöhls, Samelin, Slamanig (ICISC'15)



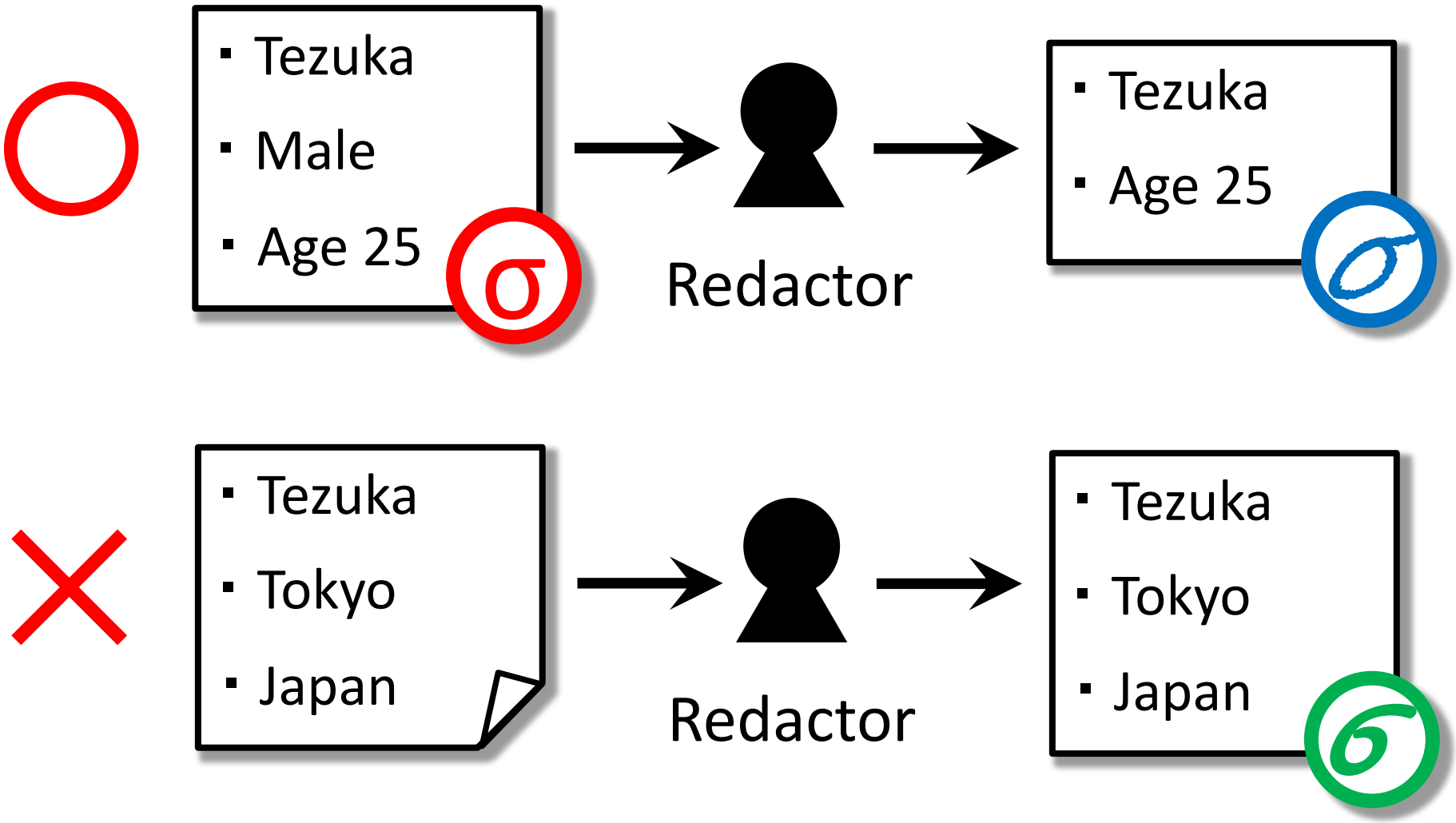
ADM can be extracted from (M, σ).

Security of redactable signature scheme

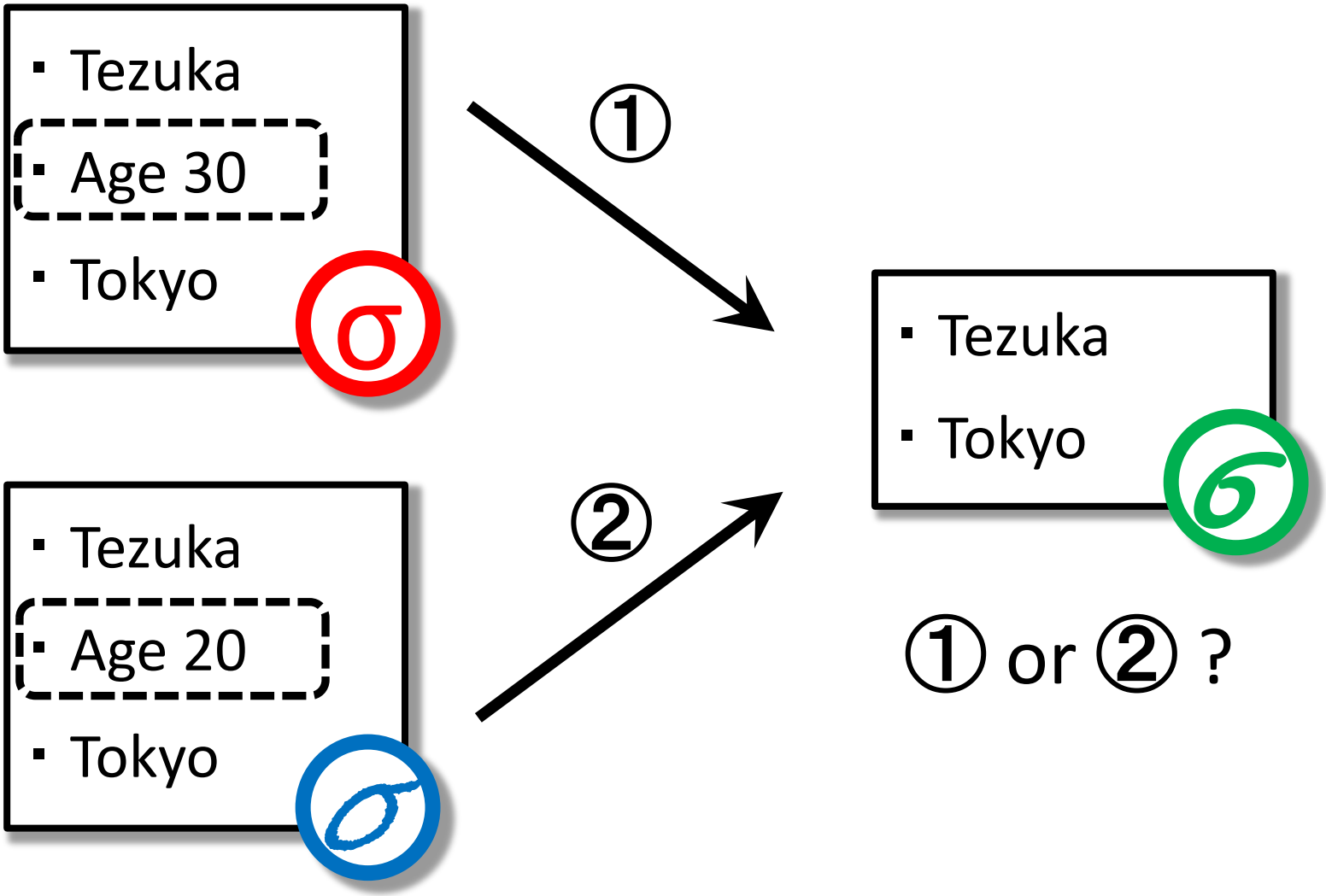
Barzska, Busch, Dagdelen, Fischkin, Franz, Katzenbeisser, Manulis, Onete, Peter, Poettering, Schröder （ACNS’10)

- ☐ Unforgeability
- ☐ Privacy
- ☐ Transparency

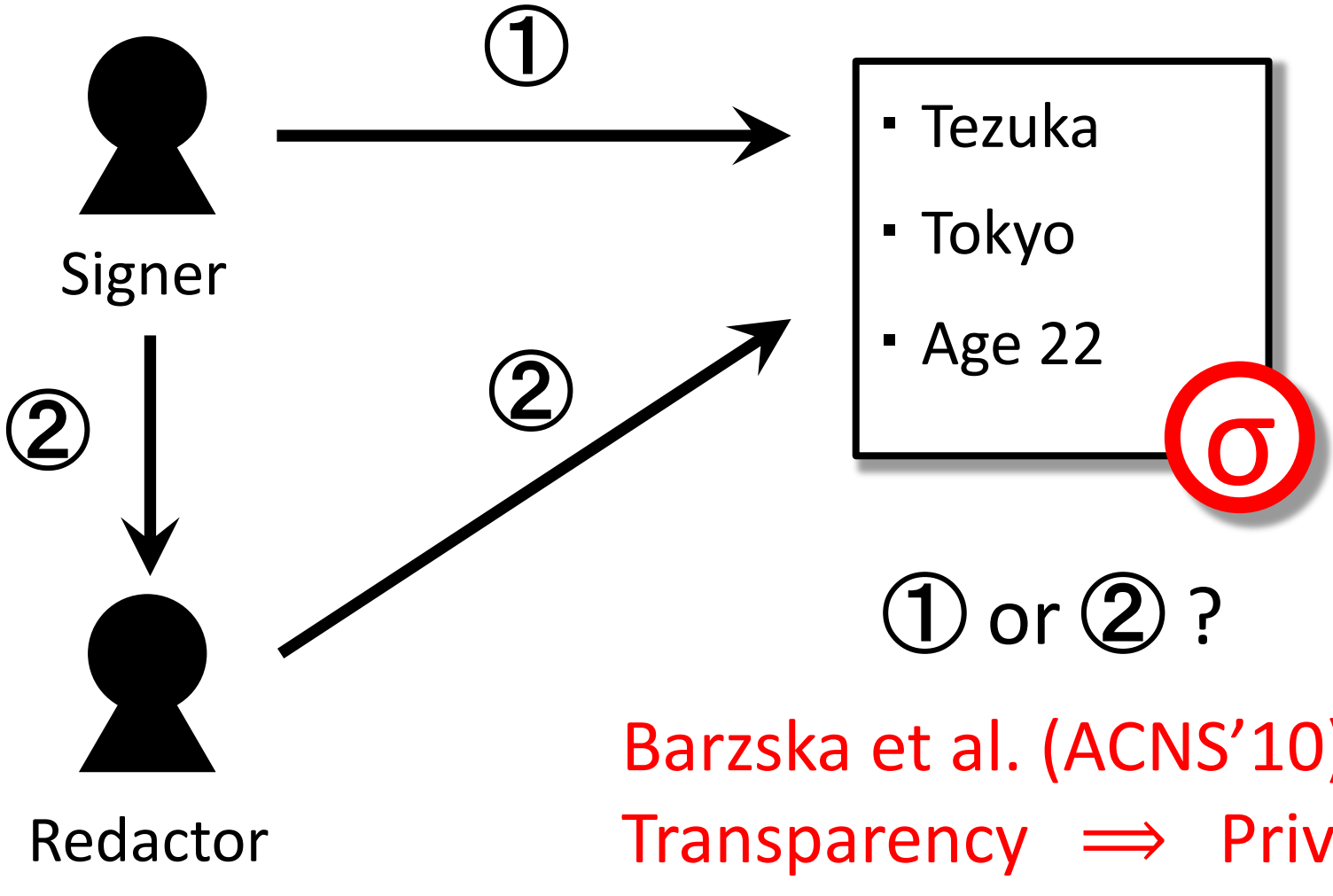
Unforgeability



Privacy


・Tezuka
・Age 30
・Tokyo
σ
①
・Tezuka
・Age 20
・Tokyo
σ
②
・Tezuka
・Tokyo
σ
① or ② ?

Transparency



Barzska et al. (ACNS'10)

Transparency ⟹ Privacy

Constructions of redactable signature schemes

- ☐ Merkle hash tree based
- ☐ Accumulator based
- ☐ Aggregate signature based

Constructions of redactable signature schemes

- ☐ Merkle hash tree based
- ☐ Accumulator based
- ☐ Aggregate signature based
  Miyazaki, Hanaoka, Imai (ASIACCS'06)
  (Based on BLS-signature scheme)

Redactable signature scheme based on aggregate signature (KeyGen)

$pp = (q, G_1, G_2, G_T, e, g_1, g_2) \leftarrow \mathcal{G}(1^\lambda)$

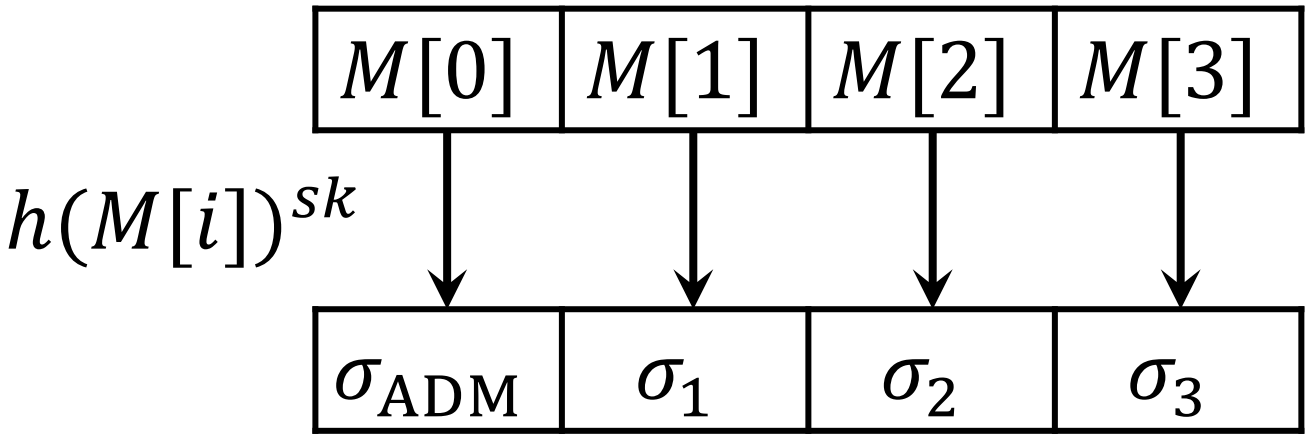
- $sk \xleftarrow{\$} Z_q,$
- $\mathrm{v}k \leftarrow g_2^{sk}$

Output (vk, sk)

Redactable signature scheme based on aggregate signature（Sign）

$(sk,\ M = \{m_1, m_2, m_3\}, \mathrm{ADM} = \{m_1\})$

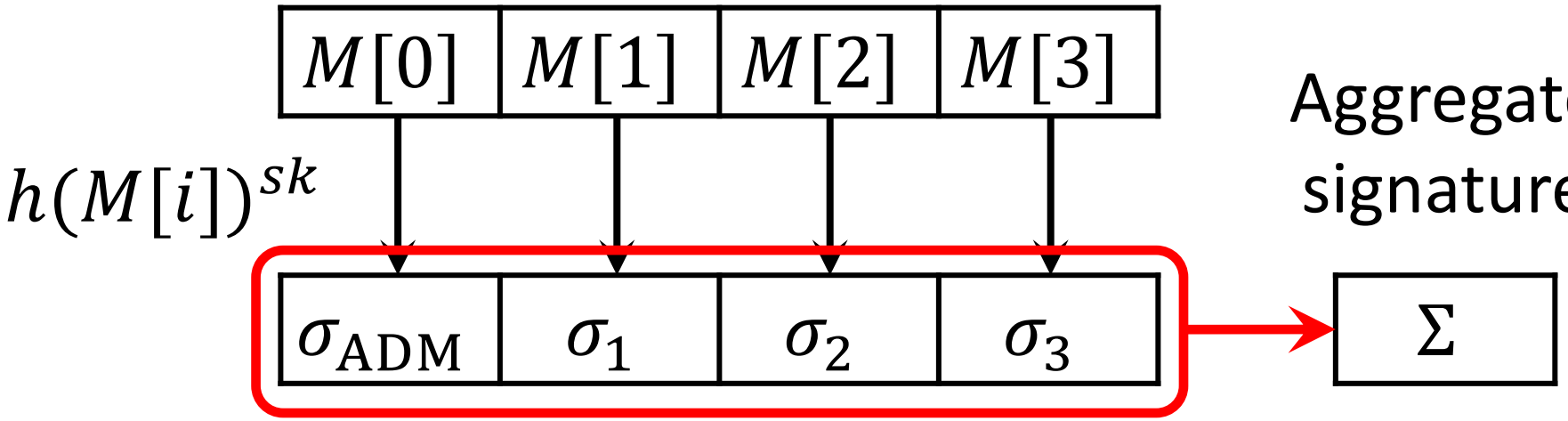
- $\mathrm{DID} \xleftarrow{\$} \{0,1\}^d$,
- $M[0] \leftarrow (\mathrm{DID} \parallel \mathrm{ord}(\mathrm{ADM})), M[j] \leftarrow (\mathrm{DID} \parallel m_j)$



Redactable signature scheme based on aggregate signature (Sign)

$(sk,\ M = \{m_1, m_2, m_3\}, \mathrm{ADM} = \{m_1\})$

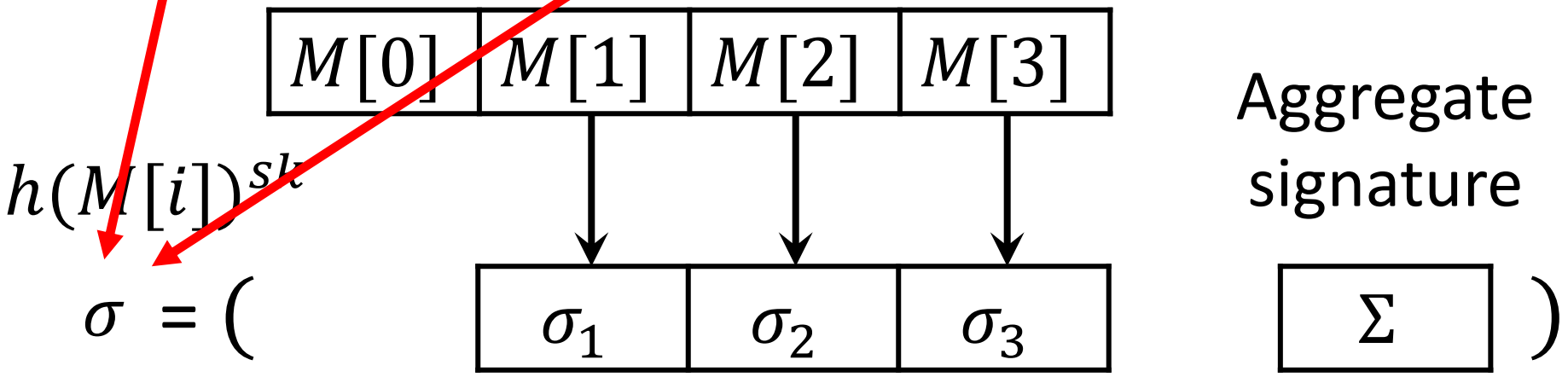
- $\mathrm{DID} \xleftarrow{\$} \{0,1\}^d$,
- $M[0] \leftarrow (\mathrm{DID} \parallel \mathrm{ord}(\mathrm{ADM})), M[j] \leftarrow (\mathrm{DID} \parallel m_j)$



Redactable signature scheme based on aggregate signature（Sign）

$(sk,\ M = \{m_1, m_2, m_3\}, \mathrm{ADM} = \{m_1\})$

- $\mathrm{DID} \xleftarrow{\$} \{0,1\}^d$,
- $M[0] \leftarrow (\mathrm{DID} \parallel \mathrm{ord}(\mathrm{ADM})), M[j] \leftarrow (\mathrm{DID} \parallel m_j)$



Output (M, σ)

Redactable signature scheme based on aggregate signature (Redact)

$(M = \{m_1, m_2, m_3\}, \sigma, \mathrm{MOD} = \{m_2\})$

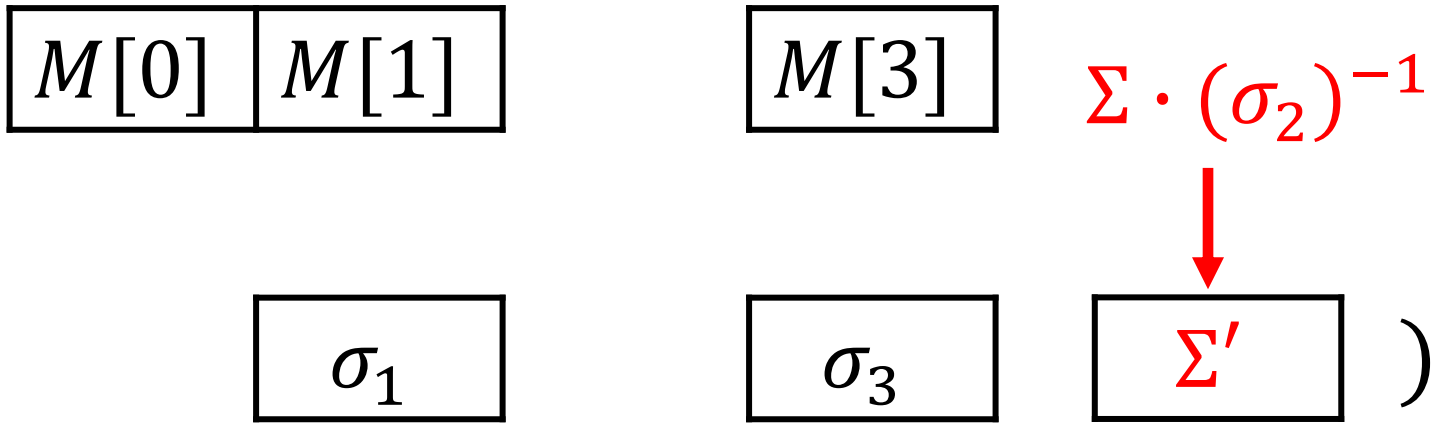
$M[0]$	$M[1]$	$M[2]$	$M[3]$

$\sigma = ($ | σ_1 | σ_2 | σ_3 | | Σ | $)$

Redactable signature scheme based on aggregate signature (Redact)

$(M = \{m_1, m_2, m_3\}, \sigma, \mathrm{MOD} = \{m_2\})$

- $M' \leftarrow M/\{m_2\}$



Output (M', σ')

Redactable signature scheme based on aggregate signature (Redact)

$(vk, M = \{m_1, m_3\}, \sigma)$

- $M' \leftarrow M/\{m_2\}$

The final redactor can prohibit further redaction by discarding all but the aggregate signature.

Redactable signature scheme based on aggregate signature (Verify)

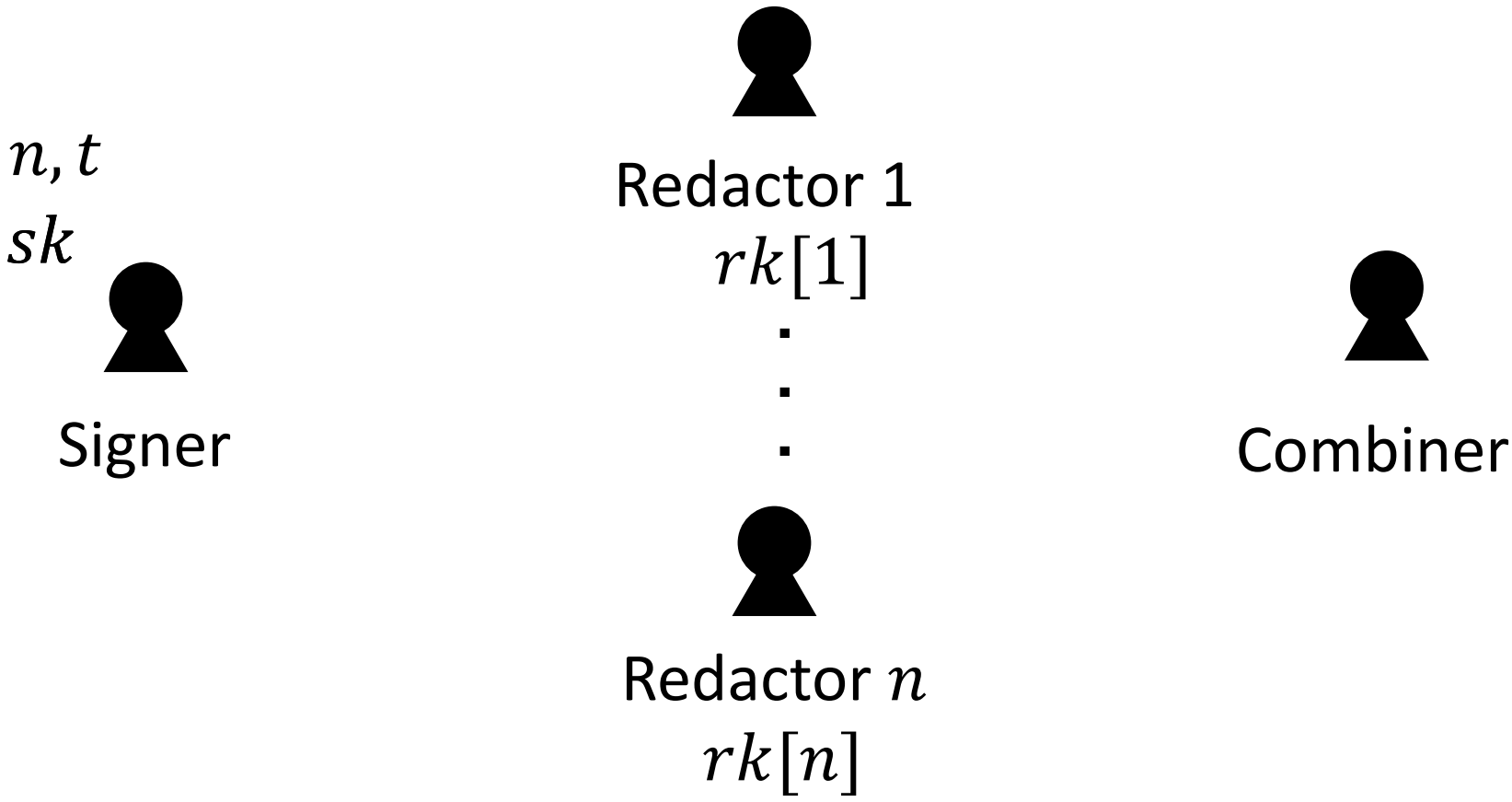
$(vk, M' = \{m'_1, m'_2\}, \sigma')$

- Parse σ' as $(\mathrm{ADM} = \{m'_1\}, \mathrm{DID}, \{\sigma_i\}_{i=1}^{3}, \Sigma)$
- Check $\mathrm{ADM} \subseteq M'$
- Check

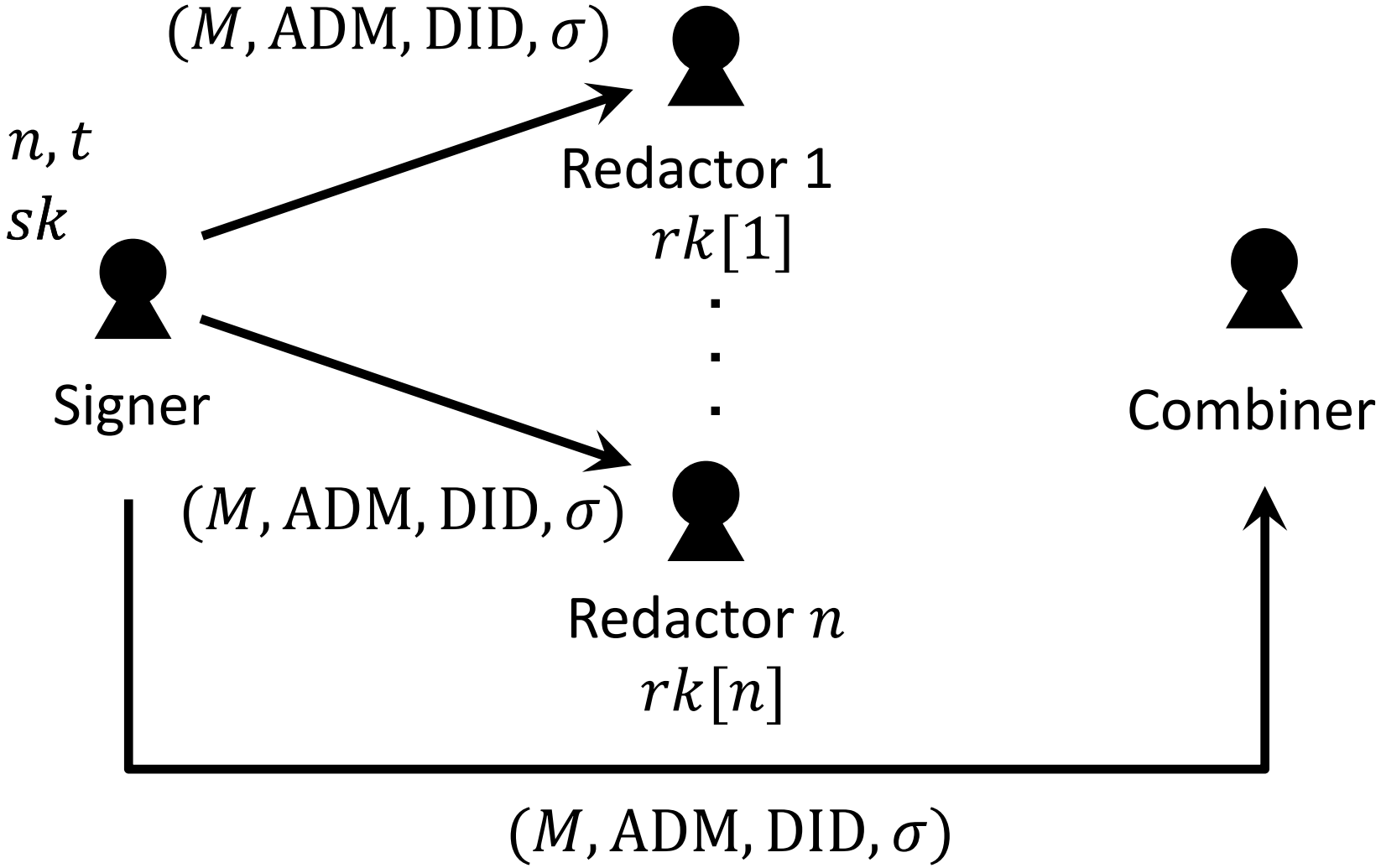
$$\mathrm{e}(\Sigma, g_2) = e(h(\mathrm{DID} \parallel \mathrm{ord}(\mathrm{ADM})), vk) \cdot \prod_{i=1}^{2} e(h(\mathrm{DID} \parallel m'_i), vk)$$

Output ``1 (Accept)" or ``0 (Reject)"

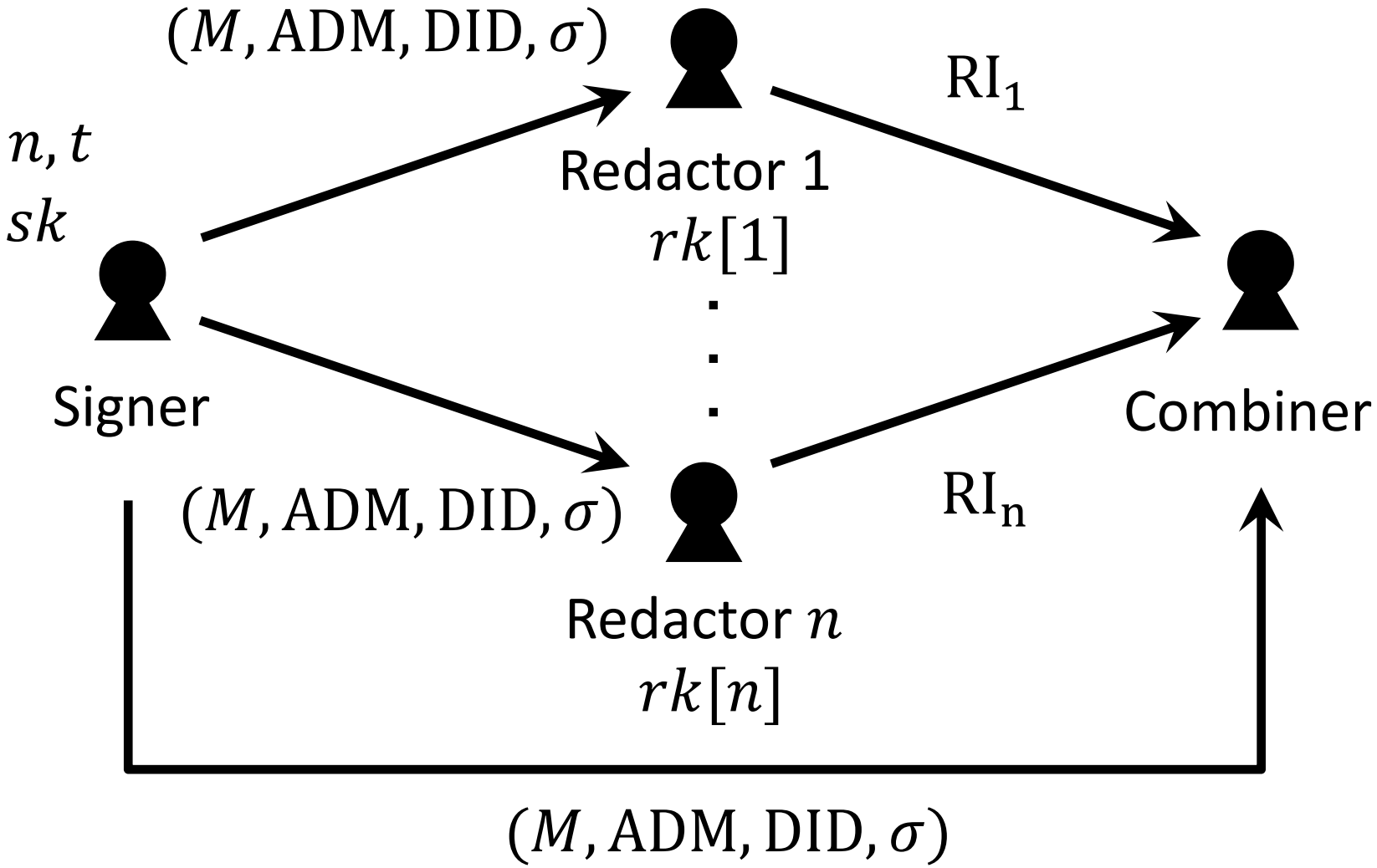
$t-out-of-n$ redactable signature scheme



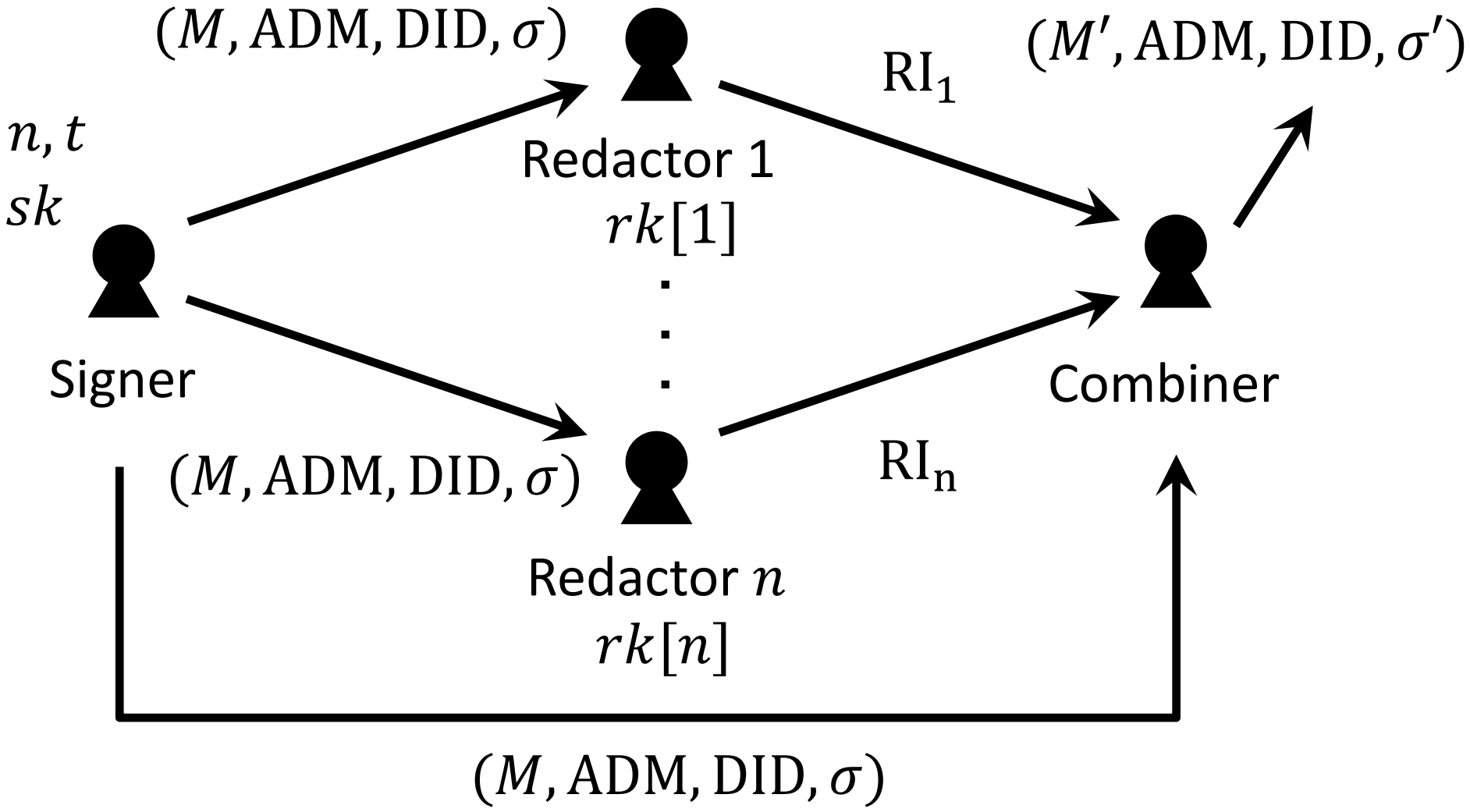
$t-out-of-n$ redactable signature scheme



$t-out-of-n$ redactable signature scheme



$t-out-of-n$ redactable signature scheme



$t-out-of-n$ redactable signature scheme construction for set（KeyGen）

KeyGen $(1^\lambda, t, n)$

$pp = (q, G_1, G_2, G_T, e, g_1, g_2) \leftarrow \mathcal{G}(1^\lambda)$

- Choose polynomial $f(X) = \sum_{i=0}^{t-1} a_i x^i$
- $rk[i] \leftarrow (i, x_i = f(i))$ for $i \in [n]$
- $sk \leftarrow f(0)$, $pk \leftarrow g_2^{sk}$
- $vk \leftarrow (g_2^{sk}, t, n)$

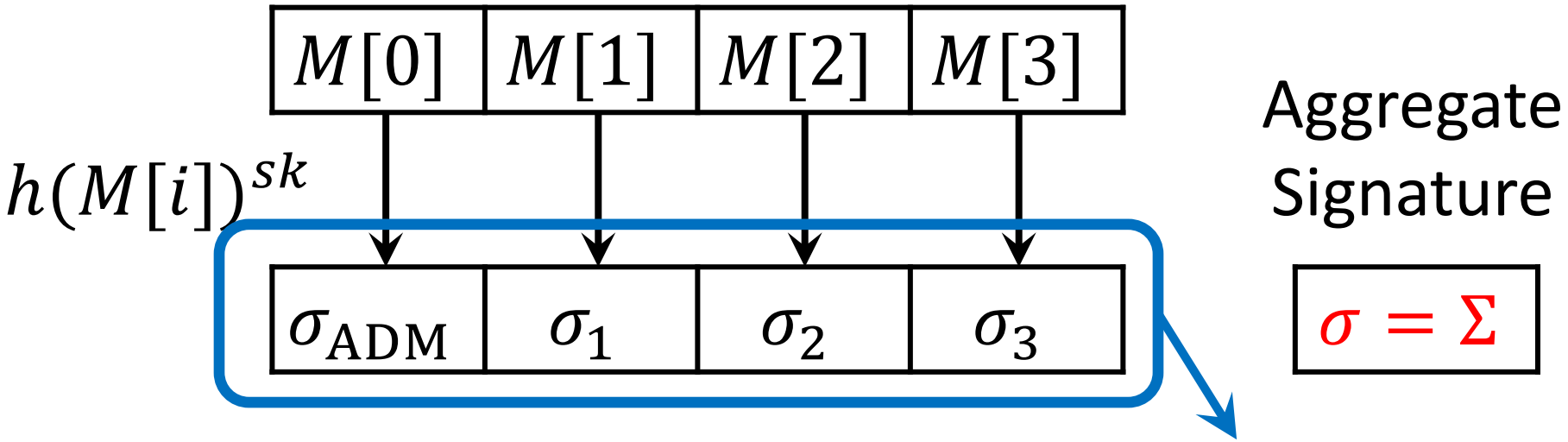
Shamir's secret sharing

Output $(vk, sk, rk[1], \cdots rk[n])$

$t-out-of-n$ redactable signature scheme construction（Sign）

Sign $(sk,\ M=\{m_1, m_2, m_3\}, \mathrm{ADM}=\{m_1\})$

- $\mathrm{DID} \xleftarrow{\$} \{0,1\}^d$,
- $M[0] \leftarrow (\mathrm{DID} \parallel \mathrm{ord}(\mathrm{ADM})), M[j] \leftarrow (\mathrm{DID} \parallel m_j)$



Output $(M, \mathrm{ADM}, \mathrm{DID}, \sigma)$

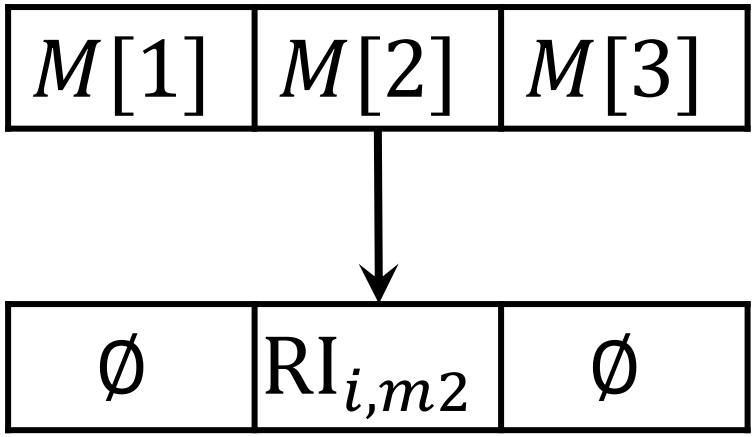
Not including σ

$t-out-of-n$ redactable signature scheme construction (Redactor i)

RedInf $(vk, M = \{m_1, m_2, m_3\}, \mathrm{ADM},$
$\mathrm{DID}, \sigma, \mathrm{MOD} = \{m_2\})$

- $M[j] \leftarrow (\mathrm{DID}||m_j)$

$h(M[j])^{rk[i]}$

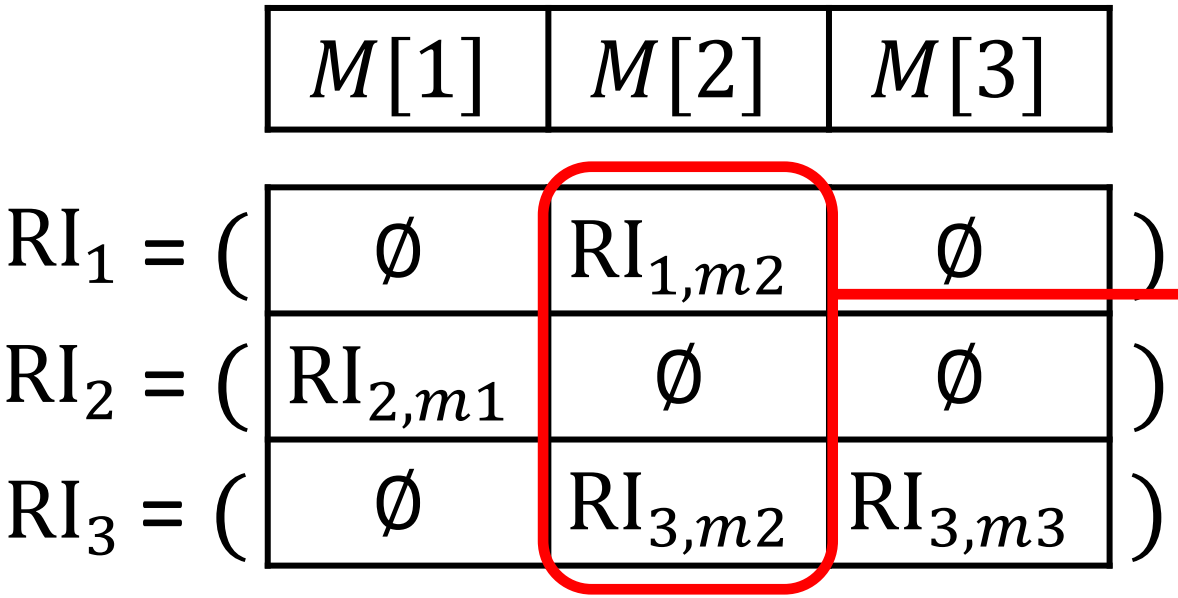


$\mathrm{RI}_i = ($ $)$

Output RI_i

$t-out-of-n$ redactable signature scheme construction（Combiner）

ThrRed $(vk, M = \{m_1, m_2, m_3\}, \mathrm{ADM}, \mathrm{DID}, \sigma, \{RI_i\}_{i=1}^{n})$



The case o f
$n = 3, t = 2$

- $M' \leftarrow M/\{m_2\}, \sigma' \leftarrow \Sigma' = \Sigma \cdot (\sigma_2)^{-1}$

Output $(M', \mathrm{ADM}, \mathrm{DID}, \sigma')$

$t-out-of-n$ redactable signature scheme construction (Verify)

Verify $(vk, M' = \{m'_1, m'_2\}, \mathrm{ADM} = \{m'_1\}, \mathrm{DID}, \sigma)$

- Check $\mathrm{ADM} \subseteq M'$
- Check

$$\mathrm{e}(\sigma, g_2) = e(h(\mathrm{DID} \parallel \mathrm{ord}(\mathrm{ADM})), vk) \cdot \prod_{i=1}^{2} e(h(\mathrm{DID} \parallel m'_i), vk)$$

Output ``1 (Accept)" or ``0 (Reject)"

Conclusion

- Introduce the notion of $t\text{–}out\text{–}of\text{–}n$ redactable signature schemes (One-time redaction model)
- Define security notions of unforgeability, privacy, and transparency for $t\text{–}out\text{–}of\text{–}n$ redactable signature schemes
- Give a construction based on computational co-Diffie-Hellman (co-CDH) assumption in ROM.