Foundations of Multi-Designated Verifier Signature

Comprehensive Formalization and New Constructions in Subset Simulation

Keitaro Hashimoto

AIST

Kyosuke Yamashita

The University of Osaka
AIST

Keisuke Hara

AIST
Yokohama National University

38th IEEE Computer Security Foundations Symposium
June 16-20, 2025 - Santa Cruz, CA, USA

What is **multi-designated verifier signature?**

Multi-designated verifier signature (MDVS)

[LV04,ZAYS12, DHM+20]

Verifier 1

$(vpk_1, vsk_1) \leftarrow \mathrm{VKGen}(pp)$

$pp \leftarrow \mathrm{Setup}(1^\kappa)$

Signer

$(spk, ssk) \leftarrow \mathrm{SKGen}(pp)$

Verifier 2

$(vpk_2, vsk_2) \leftarrow \mathrm{VKGen}(pp)$

Verifier 3

$(vpk_3, vsk_3) \leftarrow \mathrm{VKGen}(pp)$

[LV04] F. Laguillaumie and D. Vergnaud. Multi-designated verifiers signatures. ICICS 2004.
[ZAYS12] Y. Zhang, M. H. Au, G. Yang, and W. Susilo. (strong) multi-designated verifiers signatures secure against rogue key attack. Network and System Security 2012.
[DHM+20] I. Damgård et al., Stronger security and constructions of multi-designated verifier signatures. TCC 2020.

Multi-designated verifier signature (MDVS)

[LV04,ZAYS12, DHM+20]

Verifier 1

(vpk_1, vsk_1)

Signer

(spk, ssk)

$\boldsymbol{D} := \{\boldsymbol{vpk_1}, \boldsymbol{vpk_2}\}$
$\sigma \leftarrow \mathrm{Sign}(ssk, \boldsymbol{D}, m)$

Signer specifies the verifiers

Verifier 2

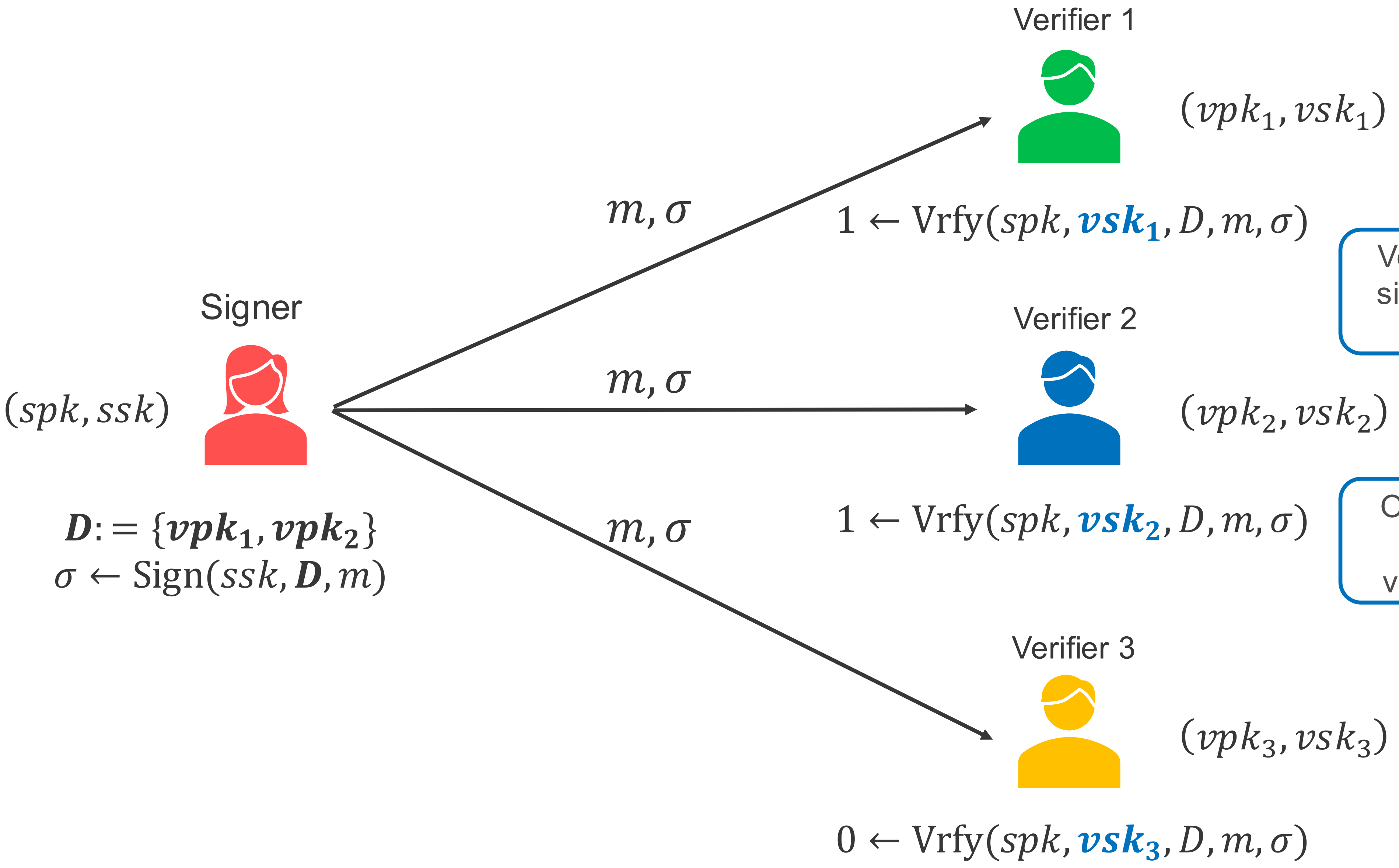
(vpk_2, vsk_2)

Verifier 3

(vpk_3, vsk_3)

Multi-designated verifier signature (MDVS)

[LV04,ZAYS12, DHM+20]



Verifier verifies a signature with its secret key

Only designated verifiers can verify the signer

Special property of MDVS

- A subset of the designated verifiers can generate a fake signature with Sim algorithm [DHM+20]
- Fake signature is indistinguishable from real one

(vpk_1, vsk_1)

$\boldsymbol{C} \subseteq \boldsymbol{D}$

(spk, ssk)

(vpk_2, vsk_2)

$$D := \{vpk_1, vpk_2, vpk_3\} \qquad\qquad D := \{vpk_1, vpk_2, vpk_3\}$$
$$\qquad\qquad\qquad\qquad \boldsymbol{C := \{vsk_1, vsk_2\}}$$
$$\sigma \leftarrow \mathrm{Sign}(ssk, D, m) \quad \overset{?}{\approx} \quad \tilde{\sigma} \leftarrow \mathrm{Sim}(spk, D, C, m)$$

(vpk_3, vsk_3)

Applications of MDVS

- Deniable authentication in secure group messaging [MPR22,DHM+20,CHMR23]
  - Senders can claim that the signature is a fake one since it may be simulated by designated verifiers

- Watermarking for large language models (LLMs) [HZM+24]
  - Authenticate output texts from LLMs so that only designated detectors can verify whether the texts are generated by LLMs or humans

[CHMR23] S. Chakraborty et al., Deniable authentication when signing keys leak. EUROCRYPT 2023.
[MPR22] U. Maurer et al, “Multi-designated receiver signed public key encryption,” EUROCRYPT 2022.
[HZM+24] Z. Huang et al., “Multi-designated detector watermarking for language models,” Cryptology ePrint Archive, 2024.

Motivation and our goal

While MDVS is becoming more attractive,
its security is ambiguous ☹

- Different security notions in the literature [ZAYS12, DHM+20, CHMR23]
  - Those differences and relations are not fully discussed

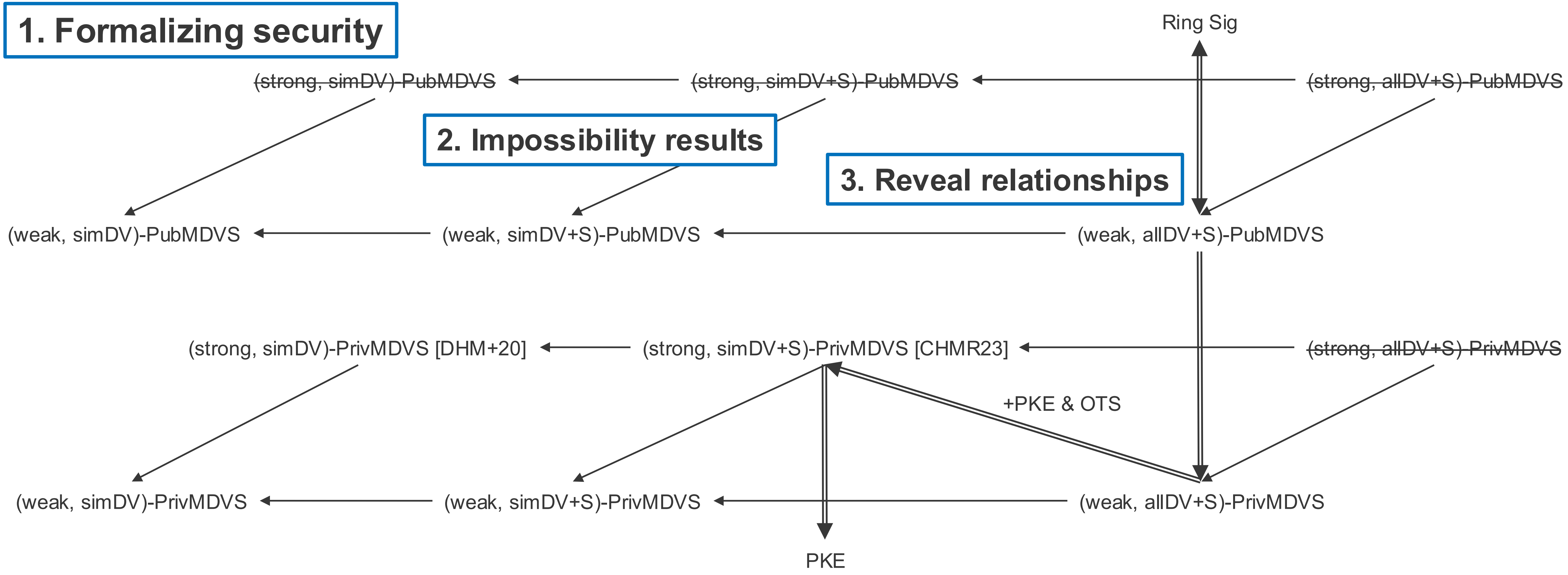
⇩

-Our goal-
Clarify the security of MDVS for the creation of applications

- Organize various security definitions of MDVS and reveal their relations
- Provide a (simple) construction of MDVS with various types of security
  - Existing constructions [DHM+20,CHMR23] are too complex

Our contributions

Comprehensive formalization and analysis of MDVS



Formalize security definitions of **MDVS**

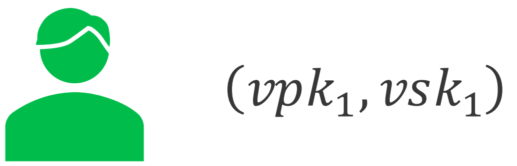
Formalize security definitions of **MDVS**

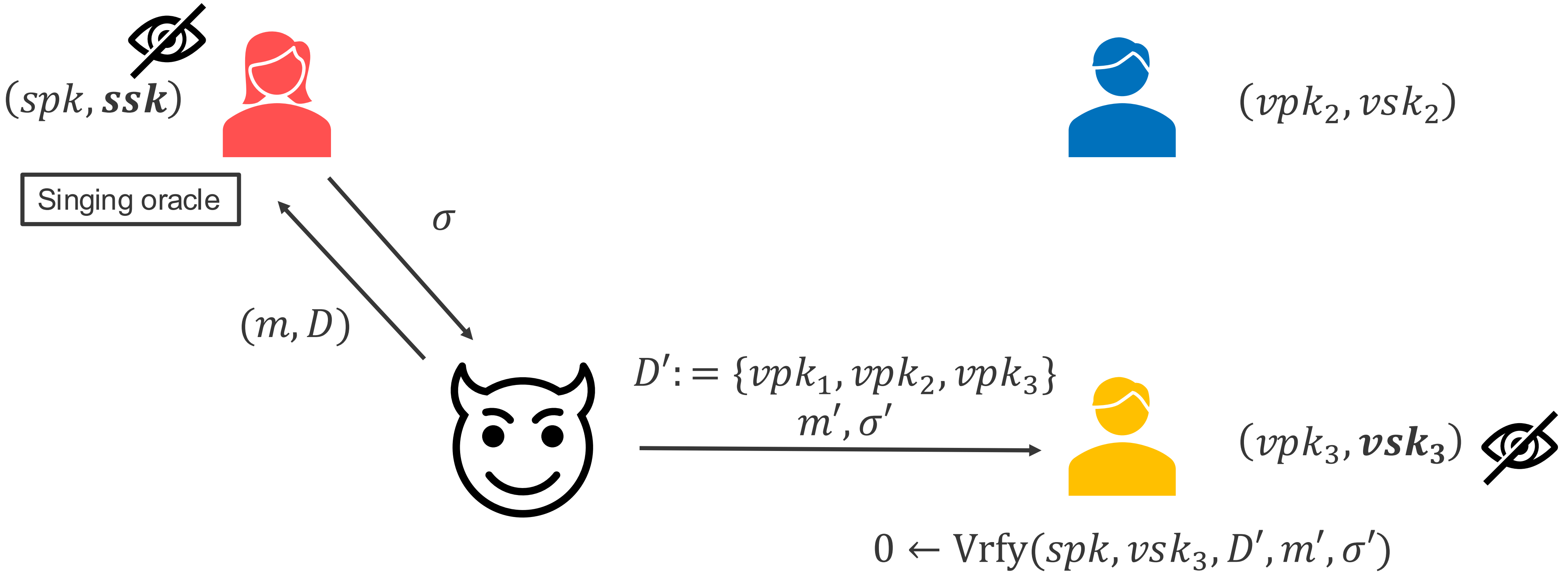
- We start with formalizing the existing security definitions in [ZAYS12, DHM+20, CHMR23]

- Fundamental notions are unforgeability and OTR
- Start with unforgeability and OTR in [ZAYS12, DHM+20, CHMR23]

Property of MDVS: Unforgeability

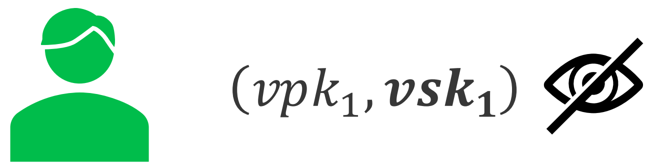
- Adversary who does not know the signer's secret key ssk and the target verifier's secret key vsk cannot forge a signature
- 2 variants depending on whether the adversary can run Sim algorithm by itself

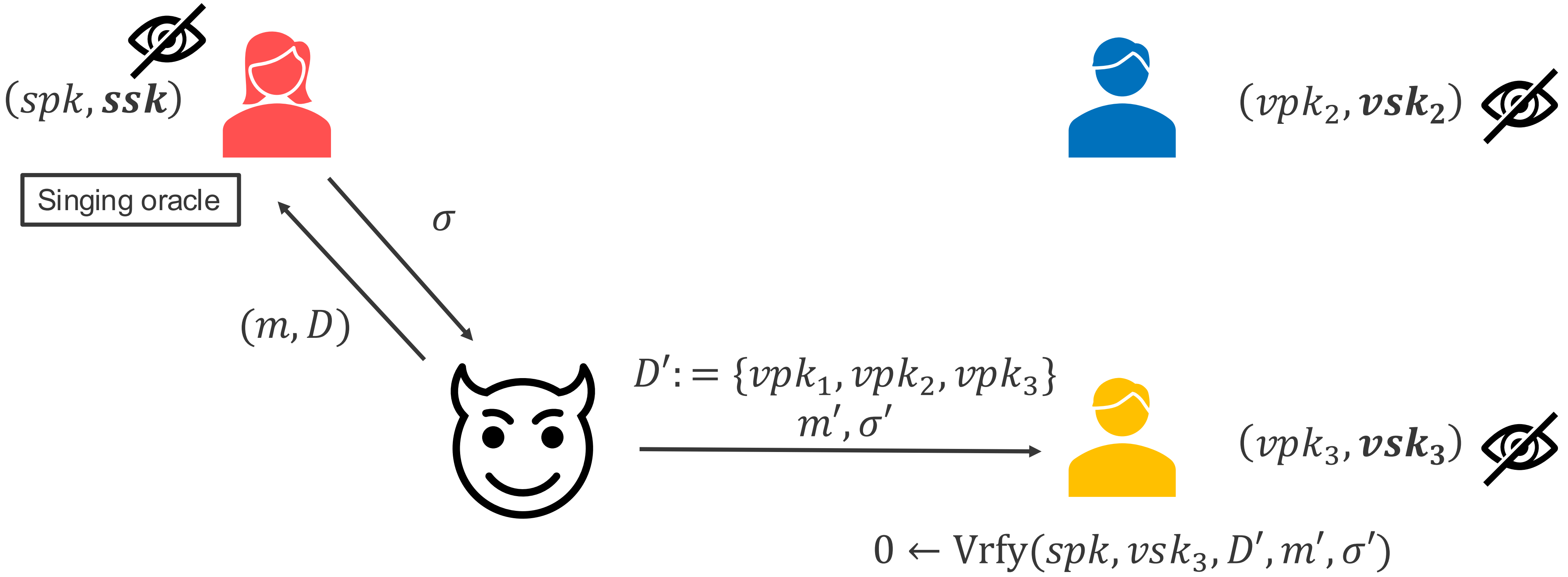




Variations of unforgeability

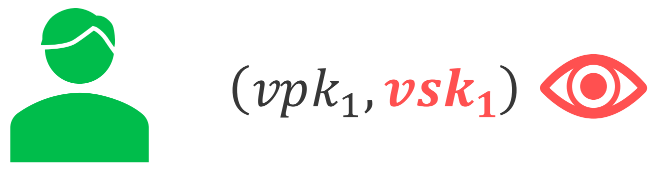
- 2 variants depending on whether the adversary can run Sim algorithm by itself
  - **Weak**: Cannot run Sim = any vsk in D are unknown [ZAYS12]
    - Fake signature is valid for any vsk in D

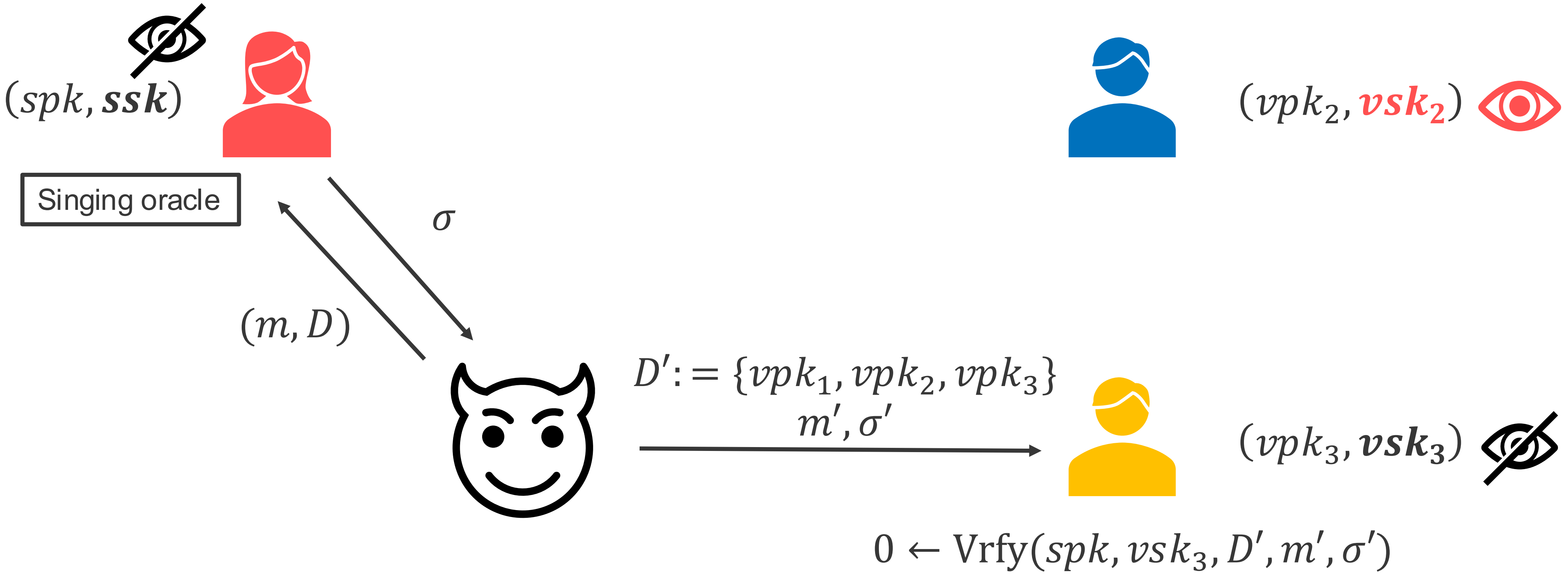




Variations of unforgeability

- 2 variants depending on whether the adversary can run Sim algorithm by itself
  - Weak: Cannot run Sim = any vsk in D are unknown [ZAYS12]
    - Fake signature is valid for any vsk in D
  - **Strong**: Can run Sim = some vsk in D is known [DHM+20]
    - Fake signature is invalid for any vsk in $D \setminus C$





Property of MDVS: Off-the-record (OTR)

- Indistinguishability of real and fake signatures
- 3 variants depending on the adversary's knowledge about secret keys

(vpk_1, vsk_1)

(vpk_2, vsk_2)

(spk, ssk)

$D := \{vpk_1, vpk_2, vpk_3\}$
$\sigma \leftarrow \mathrm{Sign}(ssk, D, m)$

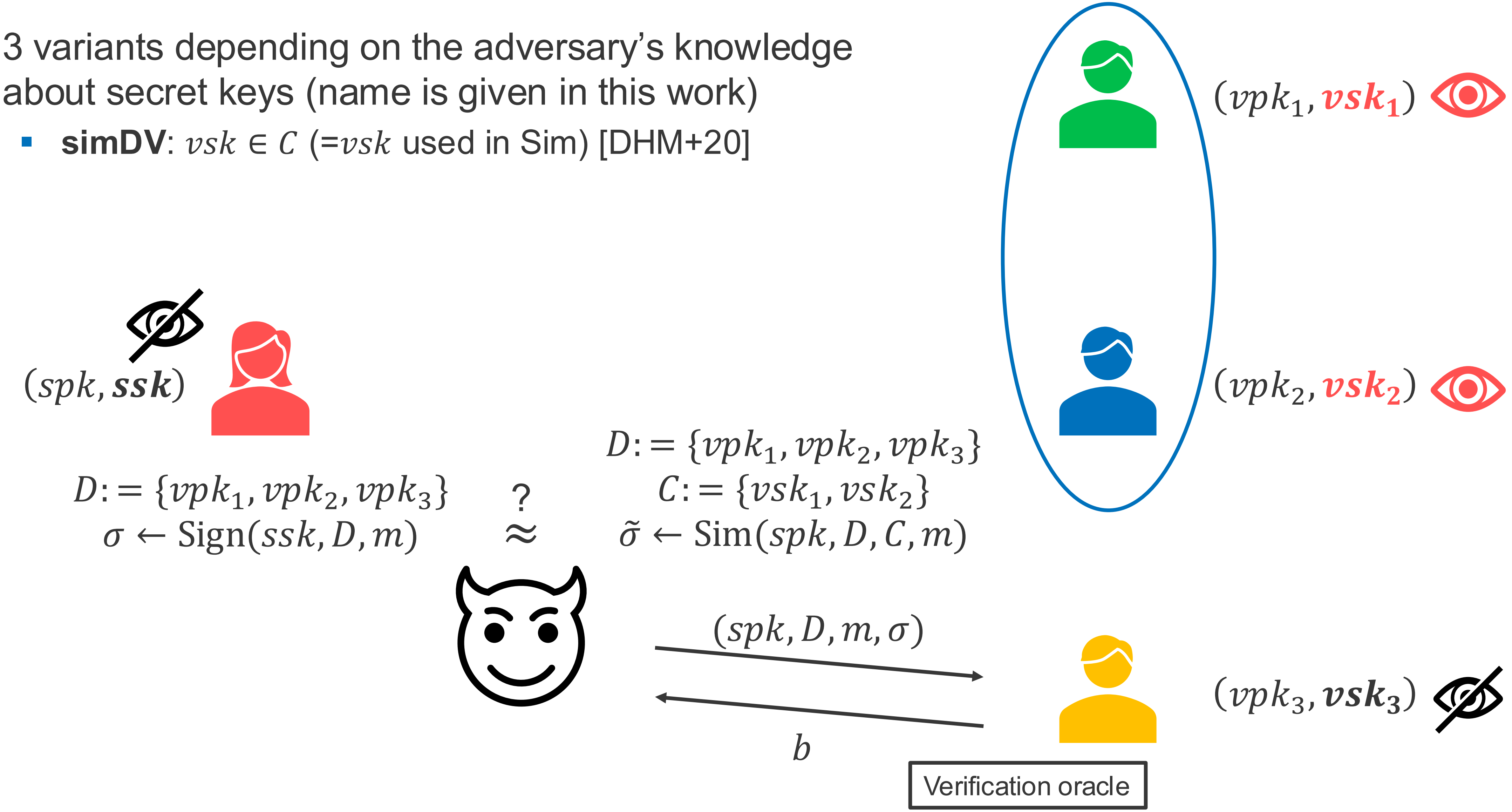
$\overset{?}{\approx}$

$D := \{vpk_1, vpk_2, vpk_3\}$
$C := \{vsk_1, vsk_2\}$
$\tilde{\sigma} \leftarrow \mathrm{Sim}(spk, D, C, m)$

(vpk_3, vsk_3)

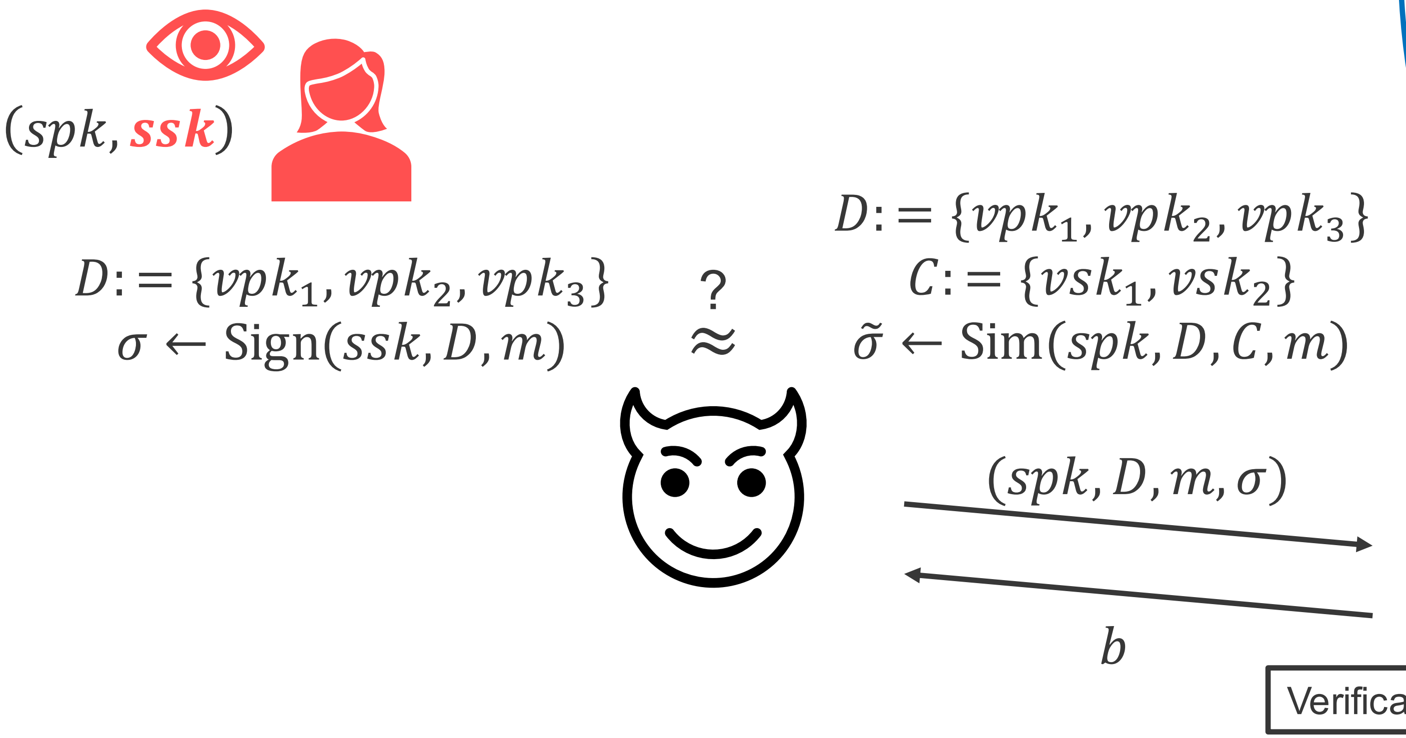
Variations of off-the-record (OTR)

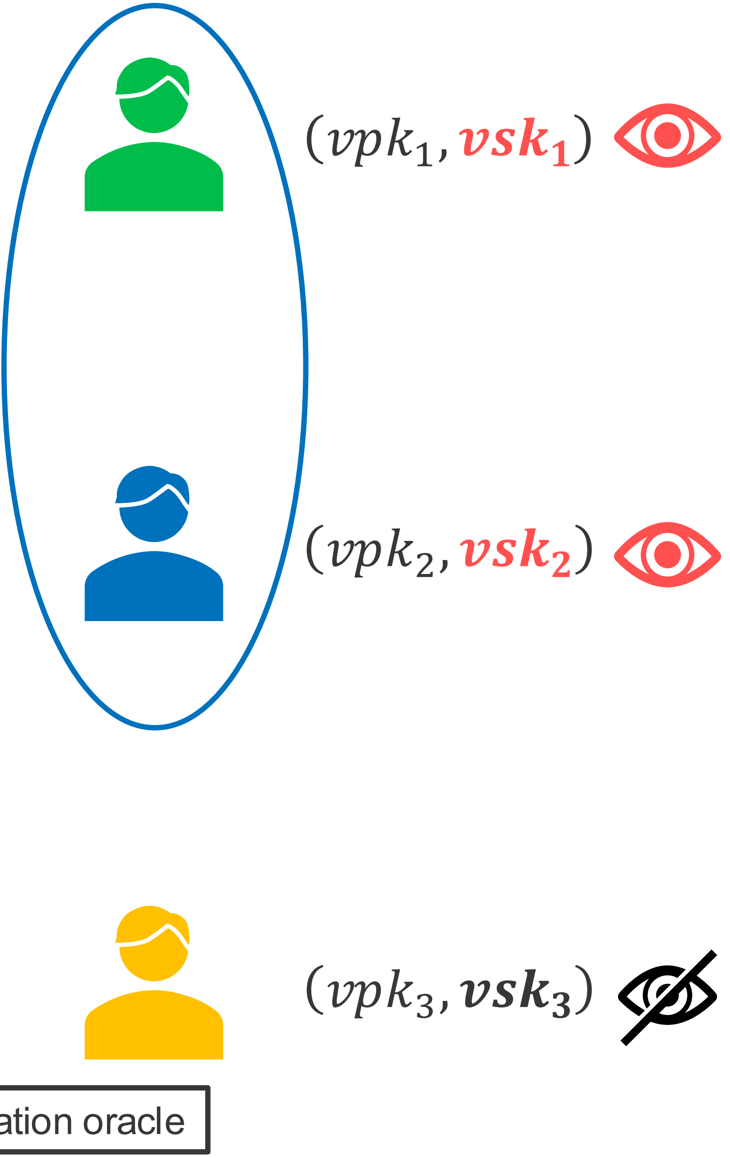
- 3 variants depending on the adversary's knowledge about secret keys (name is given in this work)
  - **simDV**: $vsk \in C$ (=vsk used in Sim) [DHM+20]



Variations of off-the-record (OTR)

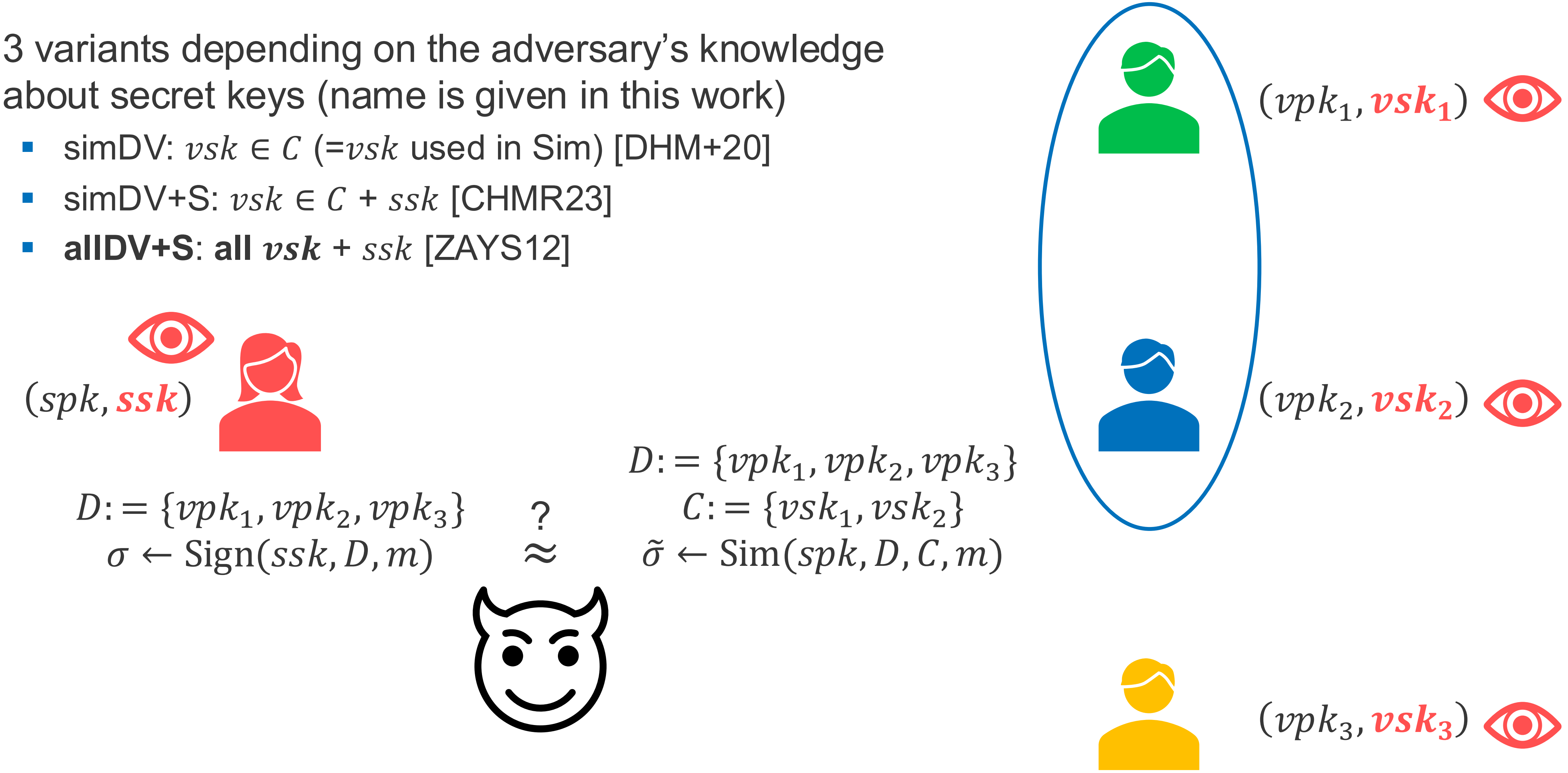
- 3 variants depending on the adversary's knowledge about secret keys (name is given in this work)
  - simDV: $vsk \in C$ (=vsk used in Sim) [DHM+20]
  - **simDV+S**: $vsk \in C$ **+** $\boldsymbol{ssk}$ [CHMR23]





Variations of off-the-record (OTR)

- 3 variants depending on the adversary's knowledge about secret keys (name is given in this work)
  - simDV: $vsk \in C$ (=vsk used in Sim) [DHM+20]
  - simDV+S: $vsk \in C$ + ssk [CHMR23]
  - **allDV+S**: **all** $\boldsymbol{vsk}$ + ssk [ZAYS12]



Verifiability: public and private

- We can define publicly verifiable MDVS
  - Signature verification does not use any secret keys
  - Considered in (Single)DVS [BFG+22]
    - Public verifiable DVS and ring signature are equivalent [BFG+22,**H**KKP22]

(spk, ssk)

m, σ

$\longrightarrow$

(vpk_2, vsk_2)

$D := \{vpk_1, vpk_2, vpk_3\}$
$\sigma \leftarrow \mathrm{Sign}(ssk, D, m)$

$\boxed{\text{Private verification: } 1/0 \leftarrow \mathbf{Priv}\mathrm{Vrfy}(spk, \boldsymbol{vsk_2}, D, m, \sigma)}$

or

$\boxed{\text{Public verification: } 1/0 \leftarrow \mathbf{Pub}\mathrm{Vrfy}(spk, D, m, \sigma)}$

[BFG+22] J. Brendel, R. Fiedler, F. Günther, C. Janson, and D. Stebila. Post-quantum asynchronous deniable key exchange and the signal handshake. PKC 2022.
[**H**KKP22] K. Hashimoto, S. Katsumata, K. Kwiatkowski, and T. Prest. An Efficient and Generic Construction for Signal's Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable. Journal of Cryptology, 2022.

Identify possible MDVSs

{weak, strong}-Unf x {simDV, simDV+S, allDV+S}-OTR
x {Priv, Pub}-Verify = 12 variants of MDVS

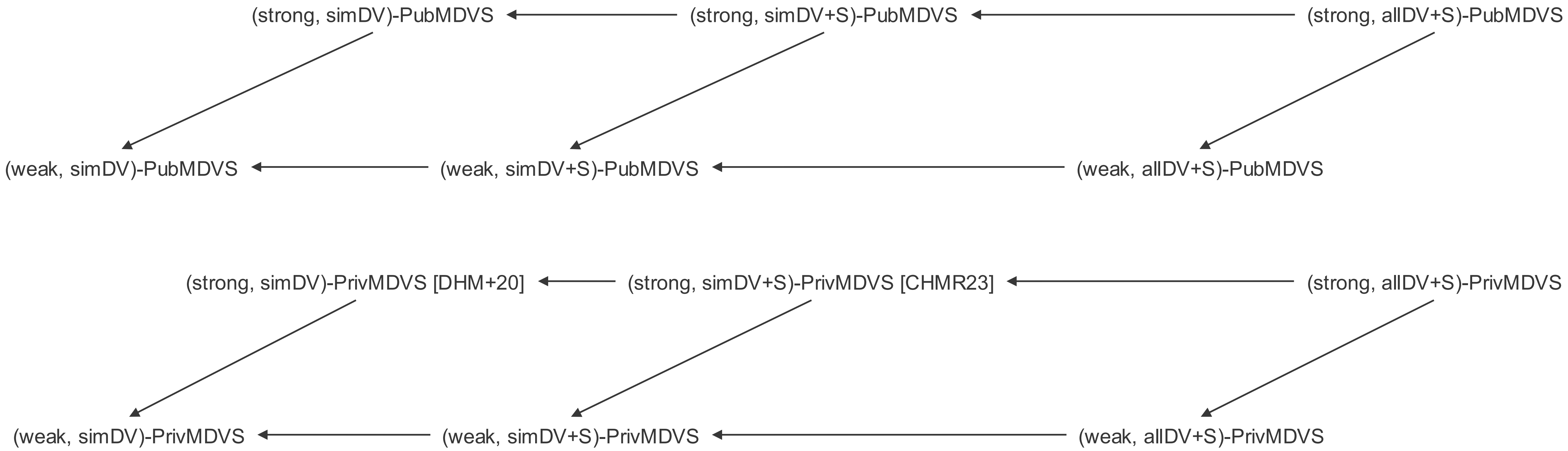
$$
\begin{tikzcd}
 & \text{(strong, simDV)-PubMDVS} \arrow[dl] & & \text{(strong, simDV+S)-PubMDVS} \arrow[ll] \arrow[dl] & & \text{(strong, allDV+S)-PubMDVS} \arrow[ll] \arrow[dl] \\
\text{(weak, simDV)-PubMDVS} & & \text{(weak, simDV+S)-PubMDVS} \arrow[ll] & & \text{(weak, allDV+S)-PubMDVS} \arrow[ll] &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & \text{(strong, simDV)-PrivMDVS [DHM+20]} \arrow[dl] & & \text{(strong, simDV+S)-PrivMDVS [CHMR23]} \arrow[ll] \arrow[dl] & & \text{(strong, allDV+S)-PrivMDVS} \arrow[ll] \arrow[dl] \\
\text{(weak, simDV)-PrivMDVS} & & \text{(weak, simDV+S)-PrivMDVS} \arrow[ll] & & \text{(weak, allDV+S)-PrivMDVS} \arrow[ll] &
\end{tikzcd}
$$

Comprehensive analysis of MDVS

Analysis of MDVS

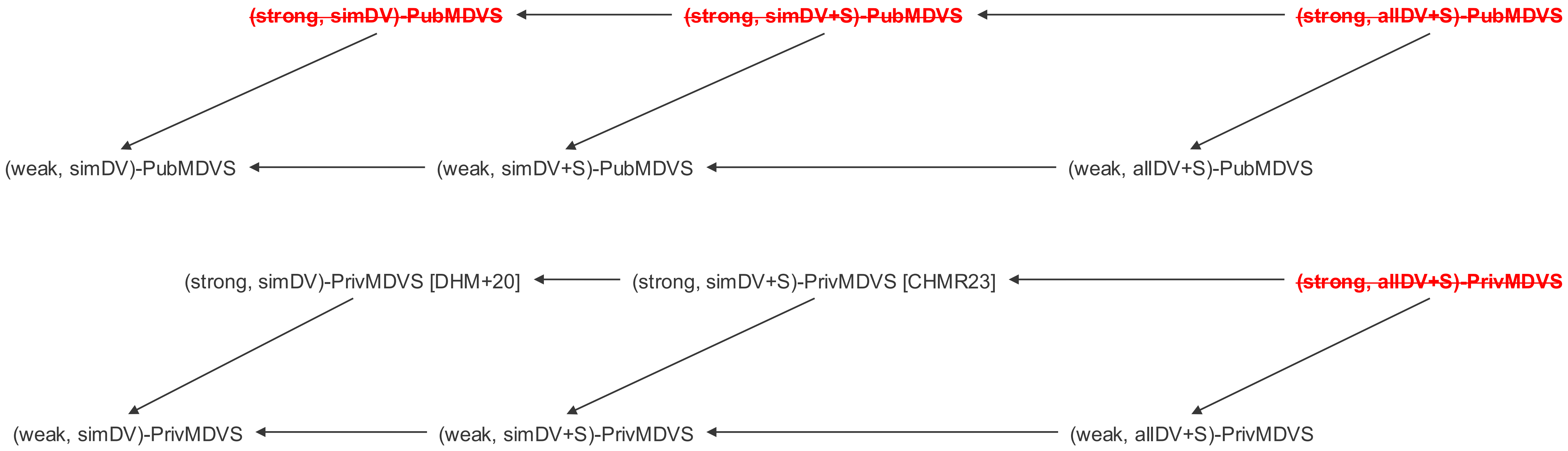
Q1: Can we realize all of the MDVSs?



Impossibility in MDVS

A: We cannot construct the following MDVS schemes

- Strong unforgeability and allDV+S OTR are conflict in PrivMDVS
- Strong unforgeability and any OTR are conflict in PubMDVS



Analysis of MDVS

We identified that some of MDVS cannot be realized

Q2: How do we construct other MDVSs?

~~(strong, simDV)-PubMDVS~~ ← ~~(strong, simDV+S)-PubMDVS~~ ← ~~(strong, allDV+S)-PubMDVS~~

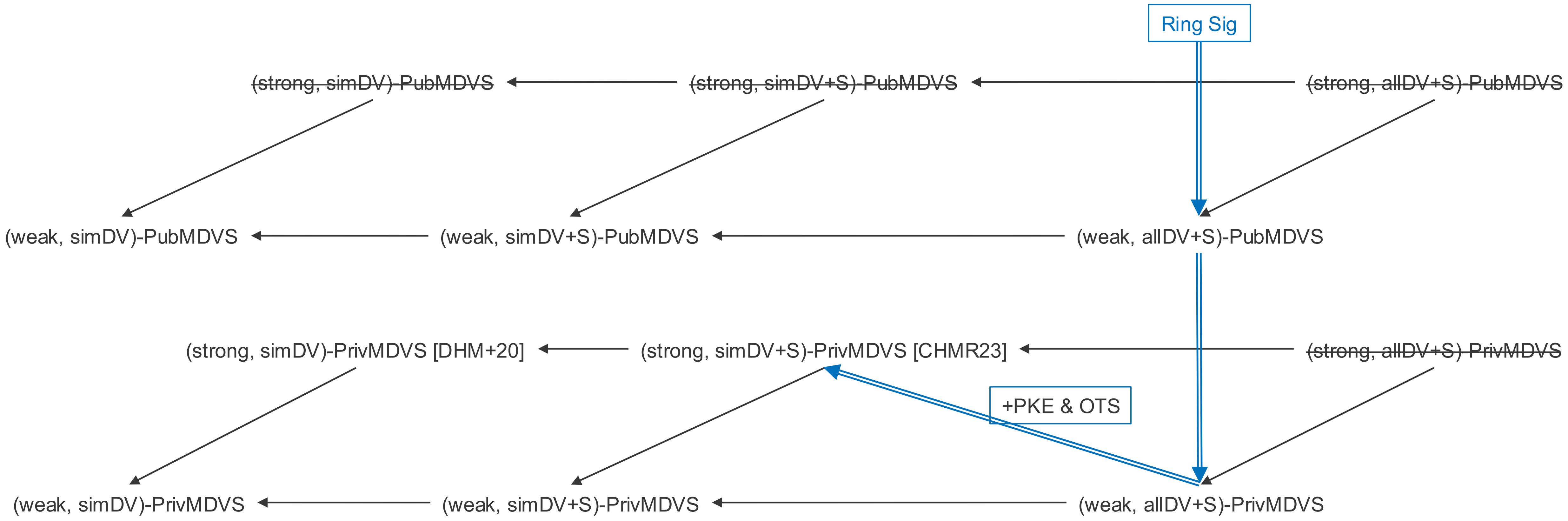
(weak, simDV)-PubMDVS ← **(weak, simDV+S)-PubMDVS** ← **(weak, allDV+S)-PubMDVS**

(strong, simDV)-PrivMDVS [DHM+20] ← **(strong, simDV+S)-PrivMDVS [CHMR23]** ← ~~(strong, allDV+S)-PrivMDVS~~

(weak, simDV)-PrivMDVS ← **(weak, simDV+S)-PrivMDVS** ← **(weak, allDV+S)-PrivMDVS**

New constructions of MDVS

A2: New constructions based on ring signatures and PKE



(weak, allDV+S)-PubMDVS from RS

- Ring R consists of designated verifier set D and spk
- Weak-Unf: Unforgeability of RS
- allDV+S: Anonymity w.r.t. full key exposure of RS

$(vpk_1, vsk_1) \leftarrow \mathrm{RS.KGen}()$

$(spk, ssk) \leftarrow \mathrm{RS.KGen}()$

m, σ

$(vpk_2, vsk_2) \leftarrow \mathrm{RS.KGen}()$

$\underline{\mathrm{MDVS.Sign}(ssk, D, m):}$
// $D := \{vpk_1, vpk_2, vpk_3\}$
$\sigma \leftarrow \mathrm{RS.Sign}(ssk, D \cup \{spk\}, m)$

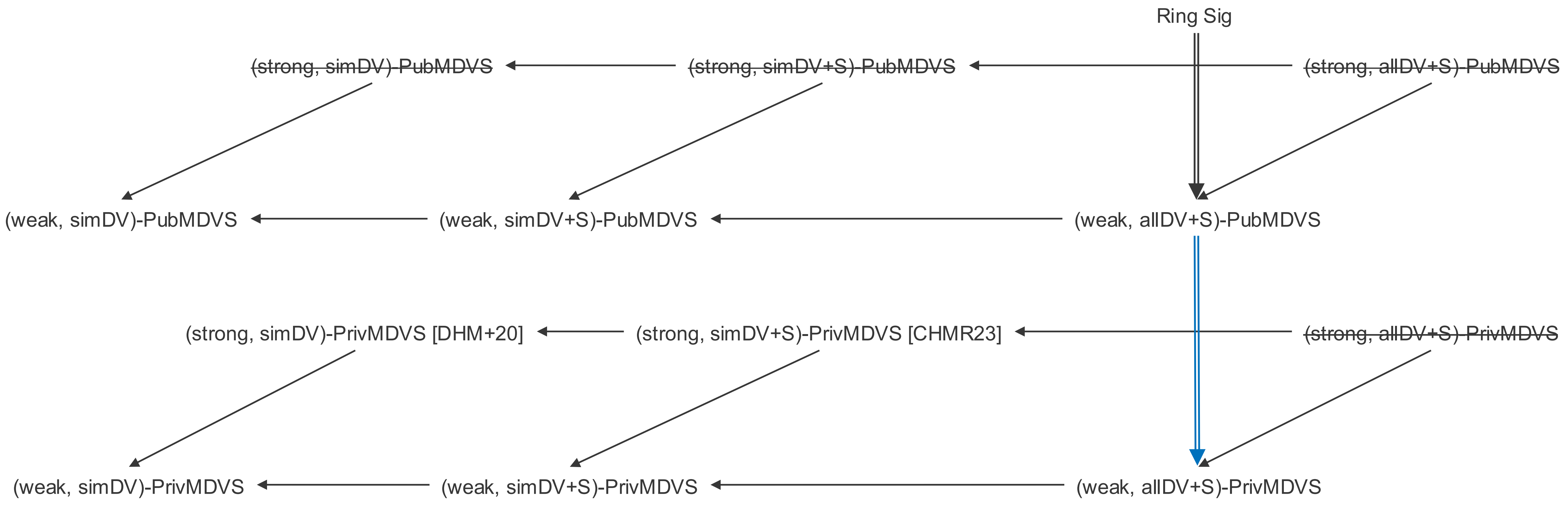
$\underline{\mathrm{MDVS.PubVrfy}(spk, D, m, \sigma):}$
$b \leftarrow \mathrm{RS.Vrfy}(D \cup \{spk\}, m, \sigma)$

$\underline{\mathrm{MDVS.Sim}\ (spk, D, C, m):}$
$vsk \leftarrow C$ // Chose e.g., 1st one
$\sigma \leftarrow \mathrm{RS.Sign}(vsk, D \cup \{spk\}, m)$

$(vpk_3, vsk_3) \leftarrow \mathrm{RS.KGen}()$

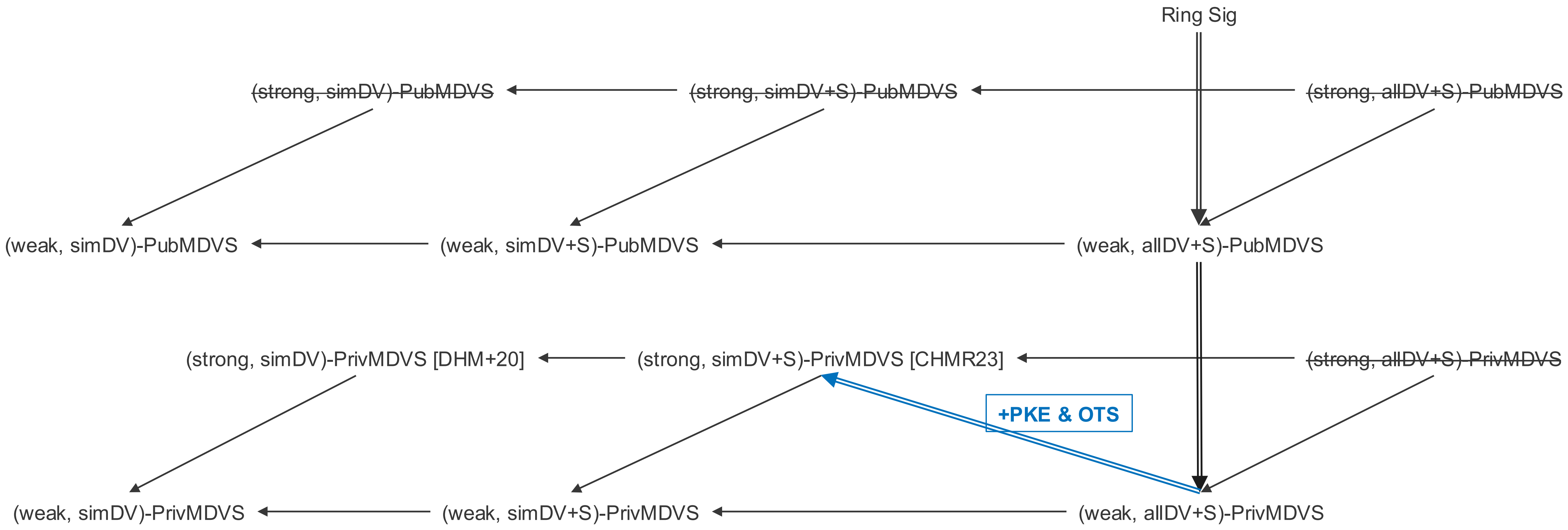
(weak, allDV+S)-PrivMDVS from PubMDVS

- Each algorithm of PrivMDVS runs the corresponding one of PubMDVS
  - $\mathrm{PrivVrfy}(spk, vsk, D, m, \sigma)$: Run $\mathrm{PubVrfy}(spk, D, m, \sigma)$ (ignore vsk)
  - allDV+S-OTR and OTR for PubVrfy have the same situation



(strong, simDV+S)-PrivMDVS from (weak, allDV+S)-PrivMDVS

Construct (strong, simDV+S)-PrivMDVS from (weak, allDV+S)-PrivMDVS with PKE and OTS



(weak, allDV+S)-PrivMDVS $\xrightarrow{+\text{PKE}}$ (strong, simDV+S)-PrivMDVS

(weak, allDV+S)-PrivMDVS

$\underline{\mathrm{MDVS'.Sign}(ssk, D, m):}$
For each $vpk_j \in D$:
$\quad \boldsymbol{\sigma_j \leftarrow \mathbf{MDVS.Sign}(ssk, \{vpk_j\}, m)}$
$\sigma \leftarrow \{\sigma_j\}$

- Pair-wise signature for signer and each verifier
  - Each verifier checks the signature sent to itself
- It achieves strong unforgeability
  - Adversary does not know both ssk and the target verifier's vsk
    $\Rightarrow$ It cannot generate both real sign and fake sig
  - Implied from weak unforgeability of PrivMDVS

(weak, allDV+S)-PrivMDVS $\xRightarrow{+\text{PKE}}$ (strong, simDV+S)-PrivMDVS

(weak, allDV+S)-PrivMDVS

$\underline{\mathrm{MDVS}'.\mathrm{Sign}(ssk, D, m)}$:
For each $vpk_j \in D$:
$\sigma_j \leftarrow \mathrm{MDVS}.\mathrm{Sign}(ssk, \{vpk_j\}, m)$
$\sigma \leftarrow \{\sigma_j\}$

Can generate a fake signature for verifiers in C ☺

$\underline{\mathrm{MDVS}'.\mathrm{Sim}(spk, D, C, m)}$:
For each $vpk_j \in D$:
If $vsk_j \in C$: $\boldsymbol{\sigma_j \leftarrow \mathrm{MDVS}.\mathrm{Sim}(spk, \{vpk_j\}, \{vsk_j\}, m)}$
Else: $\boldsymbol{\sigma_j \leftarrow 0}$
$\sigma \leftarrow \{\sigma_j\}$

Cannot generate a fake signature for verifiers not in C ☹

(weak, allDV+S)-PrivMDVS $\xRightarrow{+\text{PKE}}$ (strong, simDV+S)-PrivMDVS

(weak, allDV+S)-PrivMDVS ✚ PKE

$\underline{\text{MDVS}'.\text{Sign}(ssk, D, m):}$
For each $(vpk_j, pk_j) \in D$:
$\sigma_j \leftarrow \text{MDVS}.\text{Sign}(ssk, \{vpk_j\}, m)$
$\boldsymbol{CT_j \leftarrow \text{PKE}.\text{Enc}(pk_j, \sigma_j)}$
$\sigma \leftarrow \{CT_j\}$

$\underline{\text{MDVS}'.\text{Sim}(spk, D, C, m):}$
For each $(vpk_j, pk_j) \in D$:
If $vsk_j \in C$: $\sigma_j \leftarrow \text{MDVS}.\text{Sim}(spk, \{vpk_j\}, \{vsk_j\}, m)$
Else: $\sigma_j \leftarrow 0$
$\boldsymbol{CT_j \leftarrow \text{PKE}.\text{Enc}(pk_j, \sigma_j)}$
$\sigma \leftarrow \{CT_j\}$

Encrypt each signature with verifier's PKE key $\boldsymbol{pk}$

(weak, allDV+S)-PrivMDVS $\overset{+\text{PKE}}{\Longrightarrow}$ (strong, simDV+S)-PrivMDVS

(weak, allDV+S)-PrivMDVS ✚ PKE

$\underline{\mathrm{MDVS}'.\mathrm{Sign}(ssk, D, m)}$:
For each $(vpk_j, pk_j) \in D$:
$\sigma_j \leftarrow \mathrm{MDVS}.\mathrm{Sign}(ssk, \{vpk_j\}, m)$
$\boldsymbol{CT_j \leftarrow \mathrm{PKE}.\mathrm{Enc}(pk_j, \sigma_j)}$
$\sigma \leftarrow \{CT_j\}$

$\underline{\mathrm{MDVS}'.\mathrm{Sim}(spk, D, C, m)}$:
For each $(vpk_j, pk_j) \in D$:
If $vsk_j \in C$: $\sigma_j \leftarrow \mathrm{MDVS}.\mathrm{Sim}(spk, \{vpk_j\}, \{vsk_j\}, m)$
Else: $\sigma_j \leftarrow 0$
$\boldsymbol{CT_j \leftarrow \mathrm{PKE}.\mathrm{Enc}(pk_j, \sigma_j)}$
$\sigma \leftarrow \{CT_j\}$

- Verifier not in C: Security of PKE ensures indistinguishability
  - simDV: Adversary does not know verifiers' PKE key outside C
- Verifier in C: allDV+S-OTR ensures indistinguishability

$\Rightarrow$ simDV+S-OTR

(weak, allDV+S)-PrivMDVS $\overset{+\text{PKE}}{\Longrightarrow}$ (strong, simDV+S)-PrivMDVS

(weak, allDV+S)-PrivMDVS + IND-CCA PKE + Strong OTS = (strong, simDV+S)-PrivMDVS

$\underline{\mathrm{MDVS}'.\mathrm{Sign}(ssk, D, m):}$
$(ovk, osk) \leftarrow \mathrm{OTS.Gen}()$
For each $(vpk_j, pk_j) \in D$:
$\quad \sigma_j \leftarrow \mathrm{MDVS.Sign}(ssk, \{vpk_j\}, m)$
$\quad CT_j \leftarrow \mathrm{PKE.Enc}(pk_j, \sigma_j || ovk)$
$osig \leftarrow \mathrm{OTS.Sign}(osk, spk||D||m||\{CT_j\})$
$\sigma \leftarrow (\{CT_j\}, ovk, osig)$

$\underline{\mathrm{MDVS}'.\mathrm{Sim}(spk, D, C, m):}$
$(ovk, osk) \leftarrow \mathrm{OTS.Gen}()$
For each $(vpk_j, pk_j) \in D$:
$\quad$ If $vsk_j \in C$: $\sigma_j \leftarrow \mathrm{MDVS.Sim}(spk, \{vpk_j\}, \{vsk_j\}, m)$
$\quad$ Else: $\sigma_j \leftarrow 0$
$\quad CT_j \leftarrow \mathrm{PKE.Enc}(pk_j, \sigma_j || ovk)$
$osig \leftarrow \mathrm{OTS.Sign}(osk, spk||D||m||\{CT_j\})$
$\sigma \leftarrow (\{CT_j\}, ovk, osig)$

- **Use OTS to prevent verifing CT_j with another $spk||D||m$**
- **Use CCA PKE to answer verification oracle**

Efficiency of MDVS

Evaluate the signature size and the running time in classical and PQ settings of
Scheme 1: (weak, allDV+S)-PrivMDVS from RS and
Scheme 2: (strong, simDV+S)-PrivMDVS from RS+PKE

Signature size

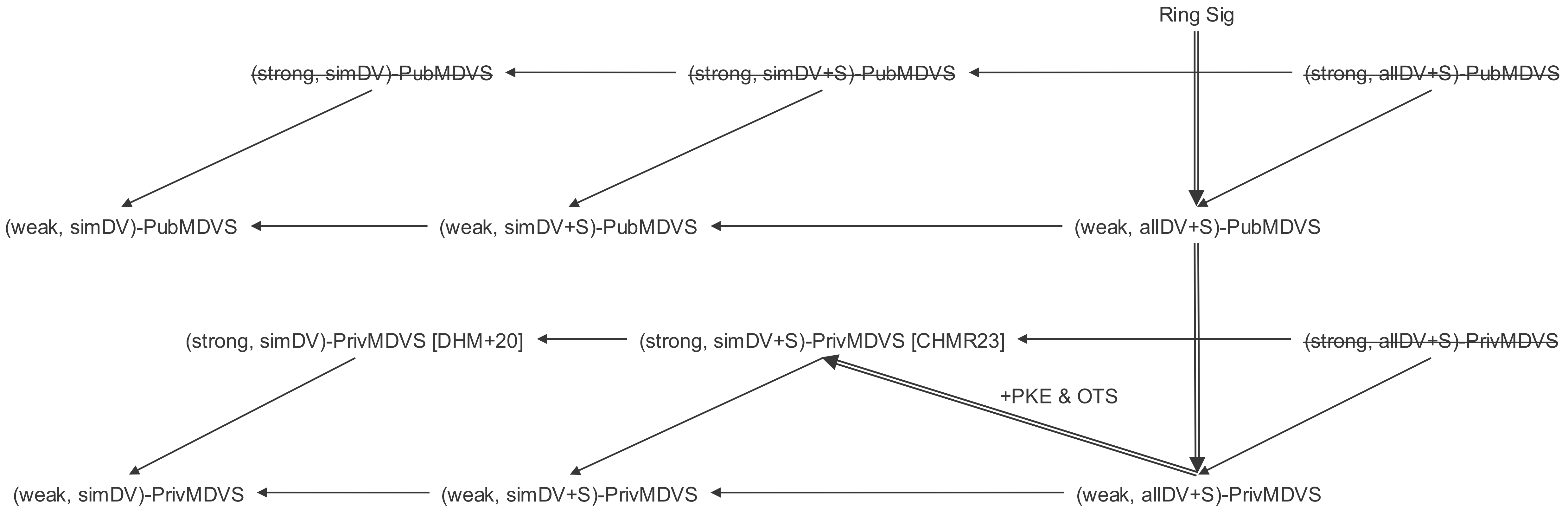
#Verifiers	2^1	2^3	2^6	2^{10}	PQ?
Scheme 1	195 B 4.5 KB	327 B 4.6 KB	525 B 6.0 KB	789 B 31.2 KB	X O
Scheme 2	614 B 17.9 KB	2168 B 59.3 KB	16672 B 445.7 KB	265312 B 7069.7 KB	X O

Signing time

#Verifiers	2^1	2^3	2^6	2^{10}	PQ?
Scheme 1	8 ms 2348 ms	36 ms 3015 ms	266 ms 7247 ms	4118 ms 72920 ms	X O
Scheme 2	17 ms 4696 ms	67 ms 18784 ms	538 ms 150273 ms	8602 ms 2404362 ms	X O

Relations from MDVS to other primitives

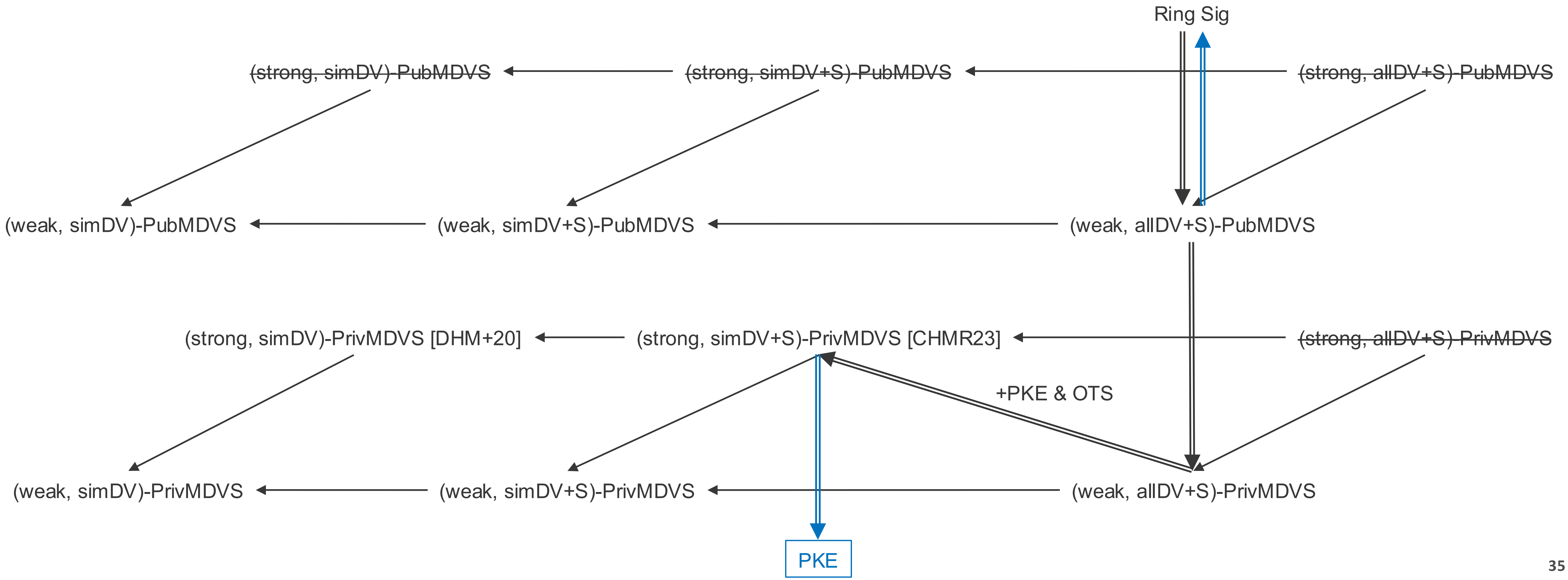
Q3: MDVS implies other cryptographic primitives?



Relations to other primitives

A3: Obtain the following implication results

- (weak, allDV+S)-PubMDVS implies ring signatures (i.e., they are equivalent)
- (strong, simDV+S)-PrivMDVS implies PKE



(weak, allDV+S)-PubMDVS ⇒ RS

- Prepare a virtual signer in public parameter, and designated verifier set D is considered ring R
- RS.Sign runs MDVS.Sim to generate signatures
- Require MDVS.PubVrfy for public verifiability of RS

$pp_{RS} \coloneqq (pp_{MDVS}, \boldsymbol{spk})$

$(pk_1, sk_1) \leftarrow \mathrm{MDVS.VKGen}()$

$D =$ ring R

m, σ

$(pk_2, sk_2) \leftarrow \mathrm{MDVS.VKGen}()$

$(pk_3, sk_3) \leftarrow \mathrm{MDVS.VKGen}()$

$\underline{\mathrm{RS.Sign}(sk_2, R, m)\text{:}}$
// $R := \{pk_1, pk_2, pk_3\}$
$\sigma \leftarrow \mathrm{MDVS.Sim}\,(spk, D, \{sk_2\}, m)$

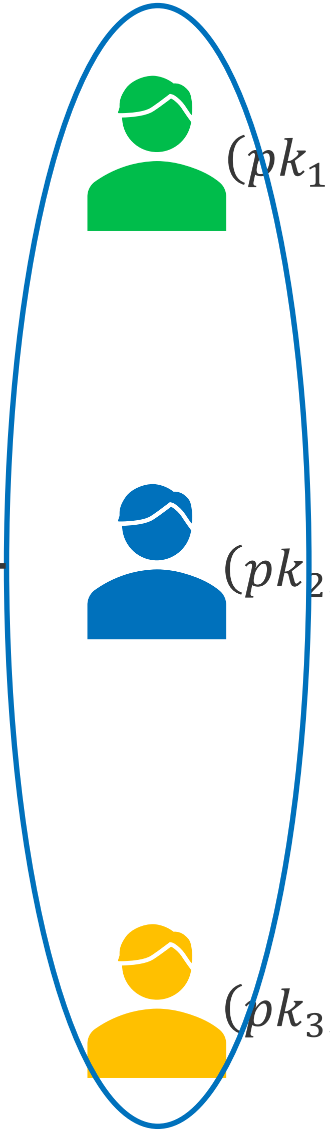
$\underline{\mathrm{RS.Vrfy}(m, R, \sigma)\text{:}}$
$b \leftarrow \mathrm{MDVS.PubVrfy}(spk, R, m, \sigma)$

(weak, allDV+S)-PubMDVS ⇒ RS

- Unforgeability of RS: weak-Unf of MDVS
  - allDV+S-OTR ensures real sig ≈ fake sig
- Anonymity of RS: allDV+S-OTR of MDVS
  - Any fake signatures are indistinguishable from real signature

$pp_{RS} \coloneqq (pp_{MDVS}, \boldsymbol{spk})$

m, σ



$(pk_1, sk_1) \leftarrow \mathrm{MDVS.VKGen}()$

$D =$ ring R

$(pk_2, sk_2) \leftarrow \mathrm{MDVS.VKGen}()$

$(pk_3, sk_3) \leftarrow \mathrm{MDVS.VKGen}()$

<u>$\mathrm{RS.Sign}(sk_2, R, m)$:</u>
// $R := \{pk_1, pk_2, pk_3\}$
$\sigma \leftarrow \mathrm{MDVS.Sim}\ (spk, D, \{sk_2\}, m)$

<u>$\mathrm{RS.Vrfy}(m, R, \sigma)$:</u>
$b \leftarrow \mathrm{MDVS.PubVrfy}(spk, R, m, \sigma)$

(strong, simDV+S)-PrivMDVS ⇒ IND-CCA PKE

$$pp_{PKE} := (pp_{MDVS}, \underbrace{spk, ssk}_{\text{signer's key}}, \underbrace{vpk, vsk}_{\text{verifier's key}}, \overbrace{m}^{\text{some message for signing}})$$

$pk := \widehat{vpk}$

$(pk, sk) := \left(\widehat{vpk}, \widehat{vsk}\right) \leftarrow \mathrm{VKGen}()$

$$CT := \sigma$$

<u>Enc($pk, M \in \{0,1\}$):</u>
If $M = 1$
$\quad \sigma \leftarrow \mathrm{Sign}(ssk, \{vpk, \widehat{vpk}\}, m)$
If $M = 0$
$\quad \sigma \leftarrow \mathrm{Sim}(spk, \{vpk, \widehat{vpk}\}, \{vsk\}, m)$

<u>Dec(sk, CT):</u>
$\quad M \leftarrow \mathrm{PrivVrfy}(\mathrm{spk}, \widehat{vsk}, \{vpk, \widehat{vpk}\}, \sigma, m)$

(strong, simDV+S)-PrivMDVS ⇒ IND-CCA PKE

<u>Sender secretly sends information on "whether or not σ is simulated"</u>

$$pp_{PKE} := (pp_{MDVS}, spk, ssk, vpk, vsk, m)$$

$pk := \widehat{vpk}$

$sk := \widehat{vsk}$

$CT := \sigma$

<u>Enc($pk, M \in \{0,1\}$):</u>
If $M = 1$
$\quad \sigma \leftarrow \mathrm{Sign}(ssk, \{vpk, \widehat{vpk}\}, m)$
If $M = 0$
$\quad \sigma \leftarrow \mathrm{Sim}(spk, \{vpk, \widehat{vpk}\}, \{vsk\}, m)$

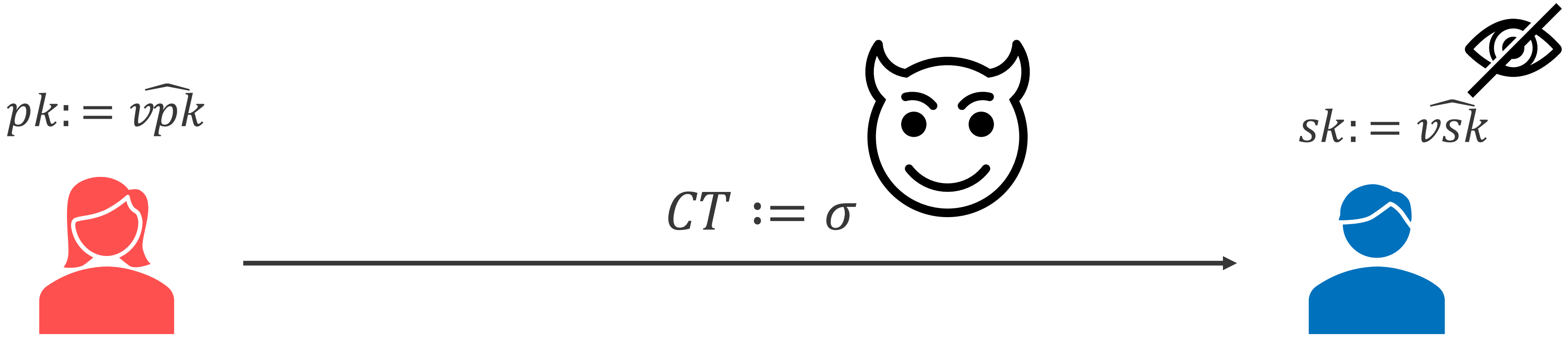
<u>Dec(sk, CT):</u>
$\quad M \leftarrow \mathrm{PrivVrfy}(\mathrm{spk}, \widehat{vsk}, \{vpk, \widehat{vpk}\}, \sigma, m)$

- Receiver knows $\widehat{vsk}$
  ⇒ two signatures are distinguishable (Strong-Unf)
  - Real sig ⇒ $\mathrm{PrivVrfy}(\sigma) = 1$ (correctness)
  - Fake sig ⇒ $\mathrm{PrivVrfy}(\sigma) = 0$ ($\widehat{vsk}$ is not used in Sim)

(strong, simDV+S)-PrivMDVS ⇒ IND-CCA PKE

<u>Sender secretly sends information on "whether or not σ is simulated"</u>

$$pp_{PKE} := (pp_{MDVS}, spk, ssk, vpk, vsk, m)$$



<u>Enc($pk, M \in \{0,1\}$):</u>
If $M = 1$
$\sigma \leftarrow \mathrm{Sign}(ssk, \{vpk, \widehat{vpk}\}, m)$
If $M = 0$
$\sigma \leftarrow \mathrm{Sim}(spk, \{vpk, \widehat{vpk}\}, \{vsk\}, m)$

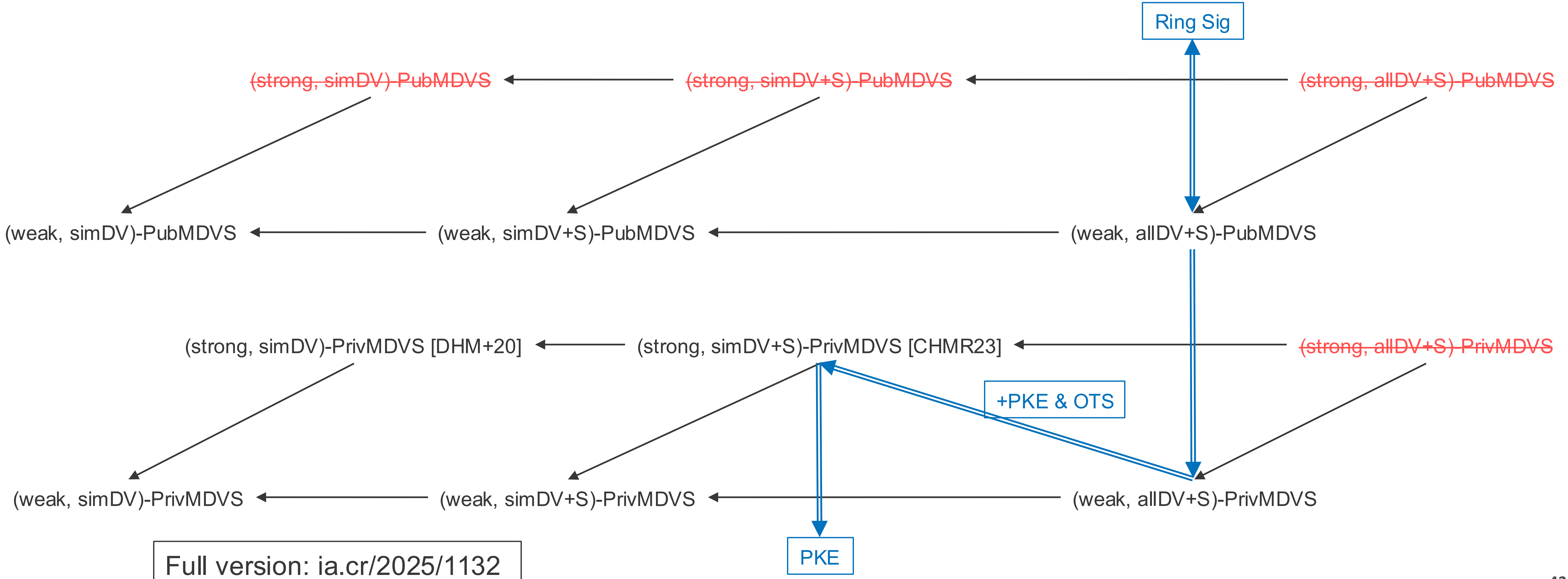
<u>Dec(sk, CT):</u>
$M \leftarrow \mathrm{PrivVrfy}(\mathrm{spk}, \widehat{vsk}, \{vpk, \widehat{vpk}\}, \sigma, m)$

- Adversary does not know $\widehat{vsk}$
  ⇒ signatures are indistinguishable (simDV+S-OTR)
  - Publish ssk to encrypt publicly ⇒ <u>require +S-OTR</u>
- Verify oracle in MDVS = Dec oracle in PKE ⇒ CCA

Conclusion

Summary of our results

Comprehensive formalization and analysis of MDVS



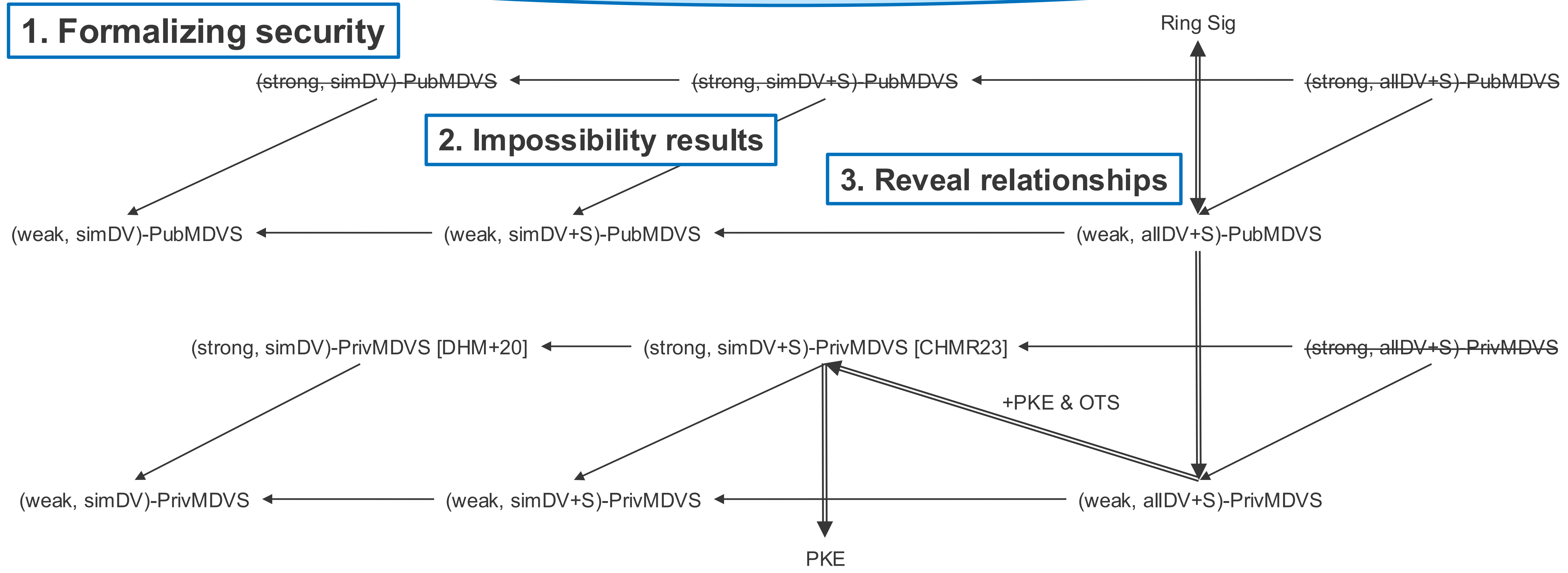
Full version: ia.cr/2025/1132

References

- [LV04] F. Laguillaumie and D. Vergnaud. Multi-designated verifiers signatures. ICICS 2004.
- [ZAYS12] Y. Zhang, M. H. Au, G. Yang, and W. Susilo. (strong) multi-designated verifiers signatures secure against rogue key attack. Network and System Security 2012.
- [TGL+19] N. Tyagi, P. Grubbs, J. Len, I. Miers, and T. Ristenpart. Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption. CRYPTO 2019.
- [DHM+20] I. Damgård, H. Haagh, R. Mercer, A. Nitulescu, C. Orlandi, and S. Yakoubov. Stronger security and constructions of multi-designated verifier signatures. TCC 2020.
- [BFG+22] J. Brendel, R. Fiedler, F. Günther, C. Janson, and D. Stebila. Post-quantum asynchronous deniable key exchange and the signal handshake. PKC 2022.
- [HKKP22] K. Hashimoto, S. Katsumata, K. Kwiatkowski, and T. Prest. An Efficient and Generic Construction for Signal's Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable. Journal of Cryptology, 2022.
- [CHMR23] S. Chakraborty, D. Hofheinz, U. Maurer, and G. Rito. Deniable authentication when signing keys leak. EUROCRYPT 2023.
- [MPR22] U. Maurer, C. Portmann, and G. Rito. Multi-designated receiver signed public key encryption, EUROCRYPT 2022.
- [HZM+24] Z. Huang, G. Zeng, X. Mu, Y. Wang, and Y. Yu. Multi-designated detector watermarking for language models, Cryptology ePrint Archive, 2024.

Our contributions

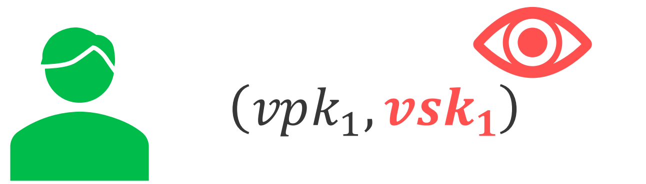
Comprehensive formalization and analysis of MDVS

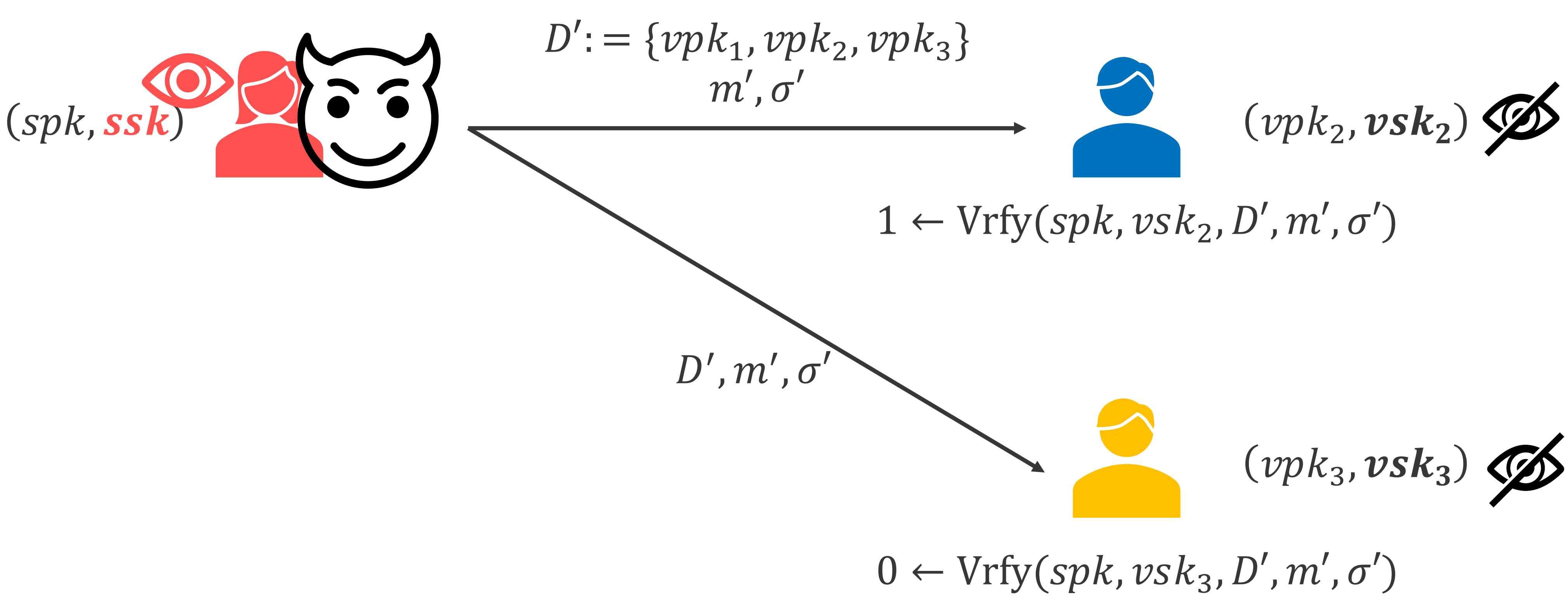


[DHM+20] I. Damgård et al., Stronger security and constructions of multi-designated verifier signatures. TCC 2020.

Property of MDVS: Consistency (Con)

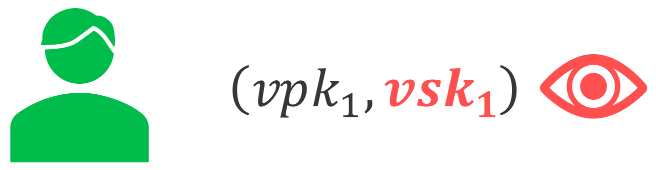
Malicious signer cannot generate a signature that leads different verification result for the designated verifiers

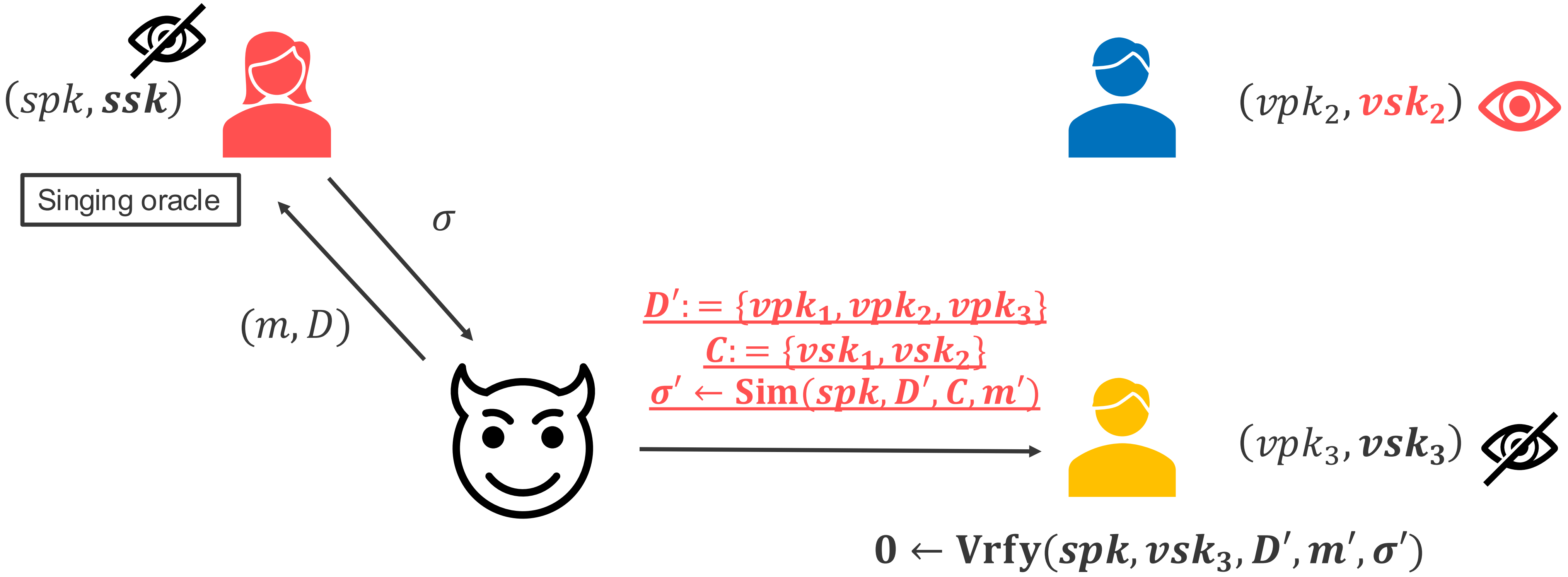




Properties of simulated signatures

- In strong unforgeability setting, the adversary can run Sim with corrupted verifier's keys
- Uncorrupted verifiers not in C must reject simulated signatures for strong unforgeability





Properties of simulated signatures

- In OTR setting, the adversary can run (Priv)Verify with corrupted verifier's keys
- Simulated signatures must be accepted with them for OTR (Real and simulated signatures must be indistinguishable)

$(vpk_1, \boldsymbol{vsk_1})$

$(vpk_2, \boldsymbol{vsk_2})$

$(vpk_3, \boldsymbol{vsk_3})$

$(spk, \boldsymbol{ssk})$

$$D := \{vpk_1, vpk_2, vpk_3\} \quad\quad D := \{vpk_1, vpk_2, vpk_3\}$$

$$\sigma \leftarrow \mathrm{Sign}(ssk, D, m) \quad \overset{?}{\approx} \quad C := \{vsk_1, vsk_2\}$$

$$\tilde{\sigma} \leftarrow \mathrm{Sim}(spk, D, C, m)$$

$\underline{\mathbf{Vrfy}(\boldsymbol{spk}, \boldsymbol{vsk_1}, \boldsymbol{D}, \boldsymbol{m}, \tilde{\boldsymbol{\sigma}})}$

$\underline{\mathbf{Vrfy}(\boldsymbol{spk}, \boldsymbol{vsk_2}, \boldsymbol{D'}, \boldsymbol{m'}, \tilde{\boldsymbol{\sigma}})}$

PrivMDVS + NIZK ⇒ PrivMDVS with Consistency

- NIZK π proves that signature is generated with Sign or Sim
- If π is valid and σ is generated with Sign, all verifiers must accept (correctness)
- If π is valid and σ is generated with Sim, verifiers s.t. $vsk \notin C$ must accept (prop. of Sim)

(vpk_1, vsk_1)

$D := \{vpk_1, vpk_2, vpk_3\}$
m, σ'

(spk, ssk)

(vpk_2, vsk_2)

$\underline{\mathrm{MDVS}'.\mathrm{Sign}(ssk, D, m)}$:
$\sigma \leftarrow \mathrm{MDVS}.\mathrm{Sign}(ssk, D, m)$
$\pi \leftarrow$ "σ' is correctly generated with Sign or Sim"
$\sigma' \leftarrow (\sigma, \pi)$

$\underline{\mathrm{MDVS}'.\mathrm{PrivVrfySign}(spk, vsk, D, m, \sigma')}$:
Verify π
$b \leftarrow \mathrm{PrivVrfy}(spk, vsk, D, m, \sigma)$

(vpk_3, vsk_3)