Designated-Verifier Linkable Ring Signatures with unconditional anonymity

Danai Balla, Pourandokht Behrouz, Panagiotis Grontas, Aris Pagourtzis, Marianna Spyrakou and Giannis Vrettos

School of Electrical and Computer Engineering
National Technical University of Athens

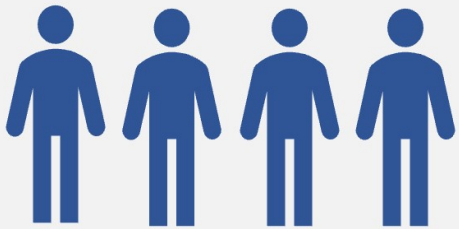
October 29, 2022

CAI 2022

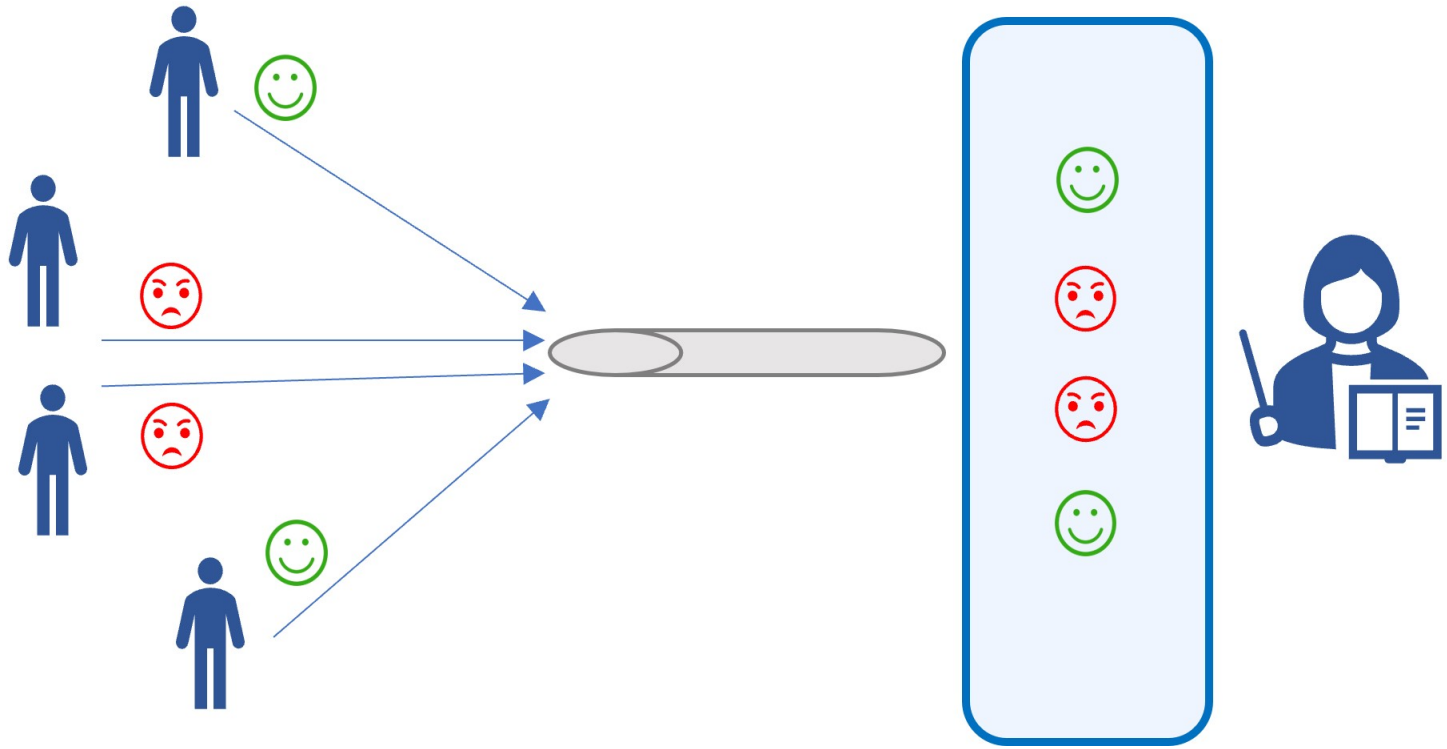
Overview

- anonymous feedback systems
- enhance anonymity of previously proposed constructions (DVLRS)
- prove the security properties in the $\mathcal{RO}$ model

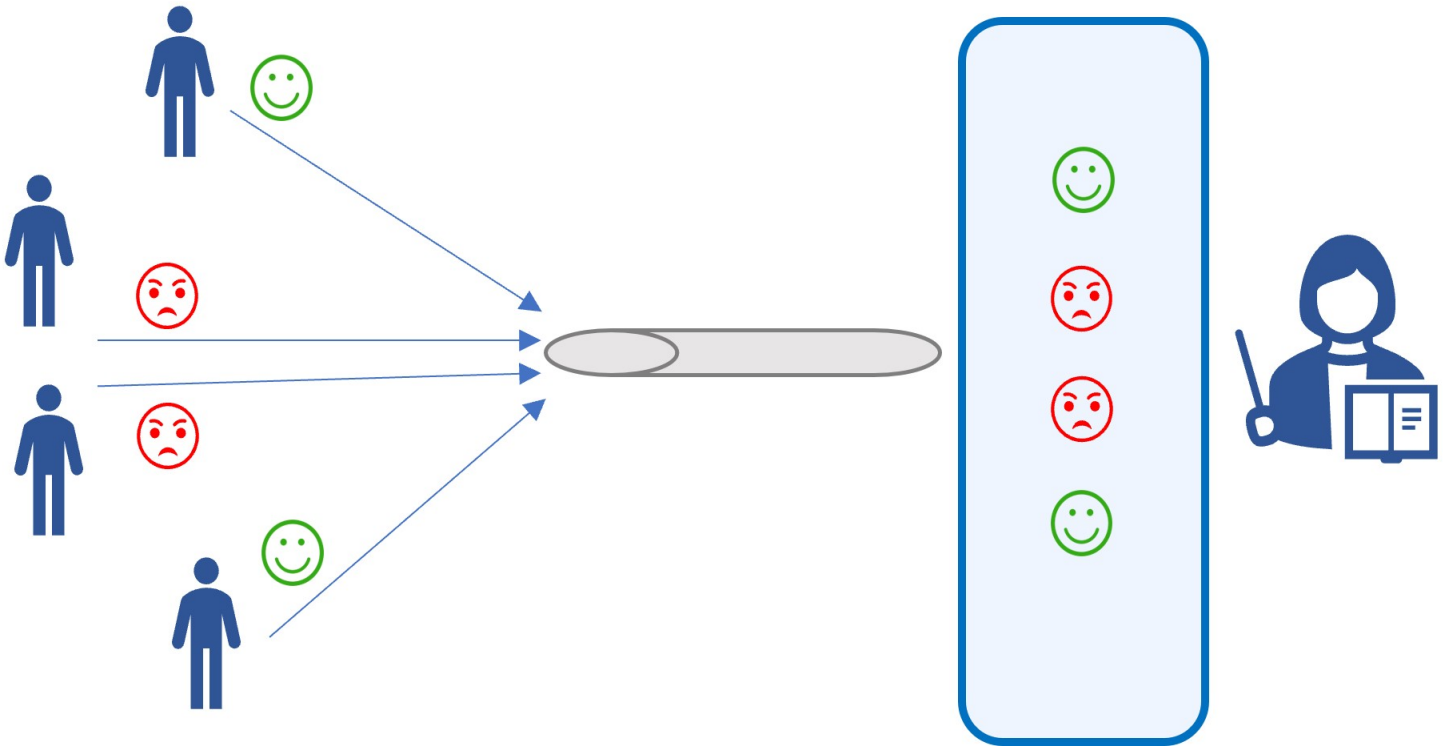
An Anonymous Feedback System



An Anonymous Feedback System

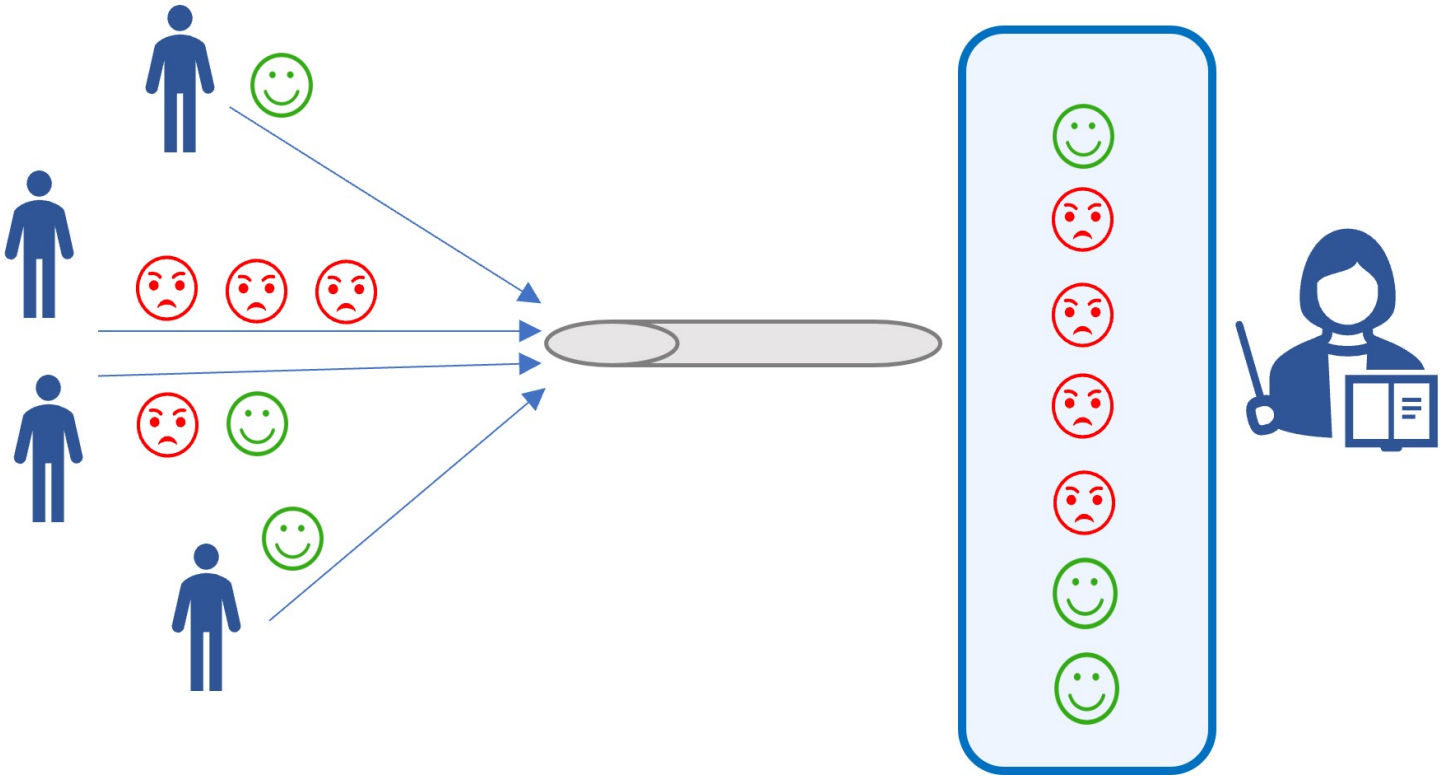


An Anonymous Feedback System

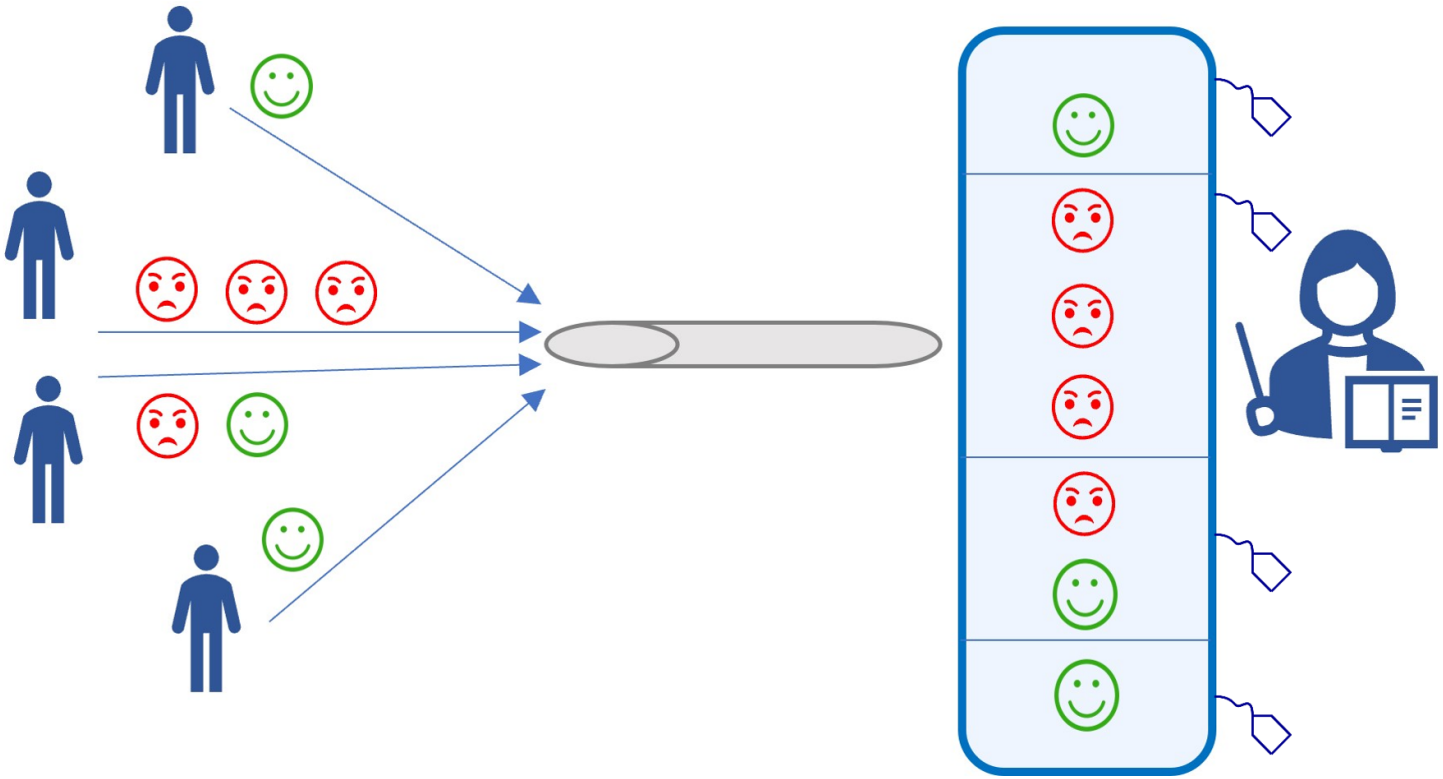


- Feedback from registered students
- Anonymous

An Anonymous Feedback System

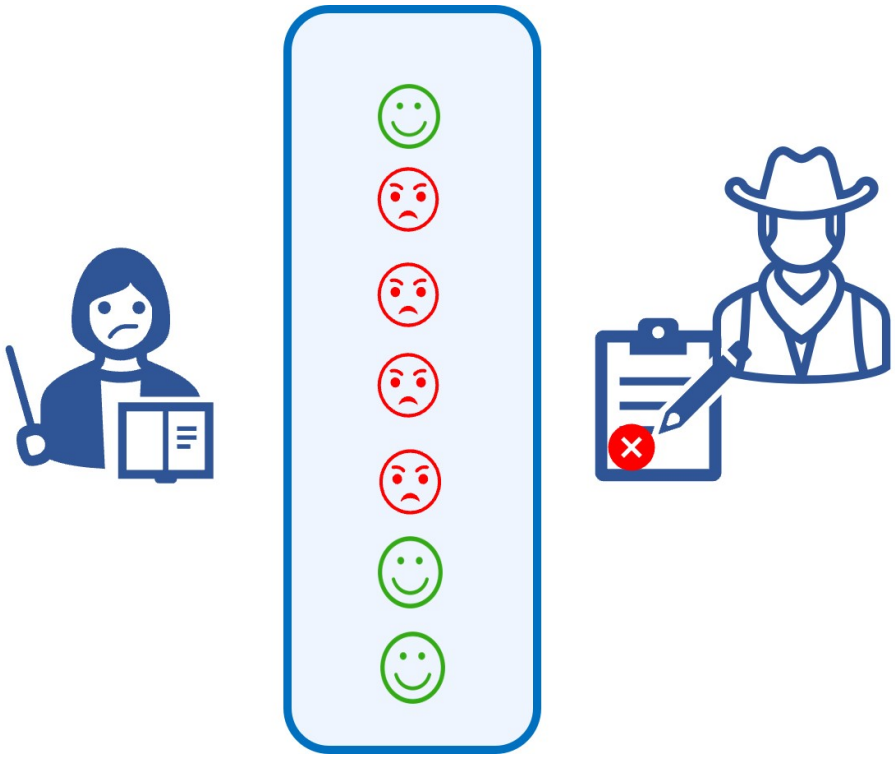


An Anonymous Feedback System



– The teacher can group feedback according to the linking tag, without knowing the actual identity of the student.

An Anonymous Feedback System



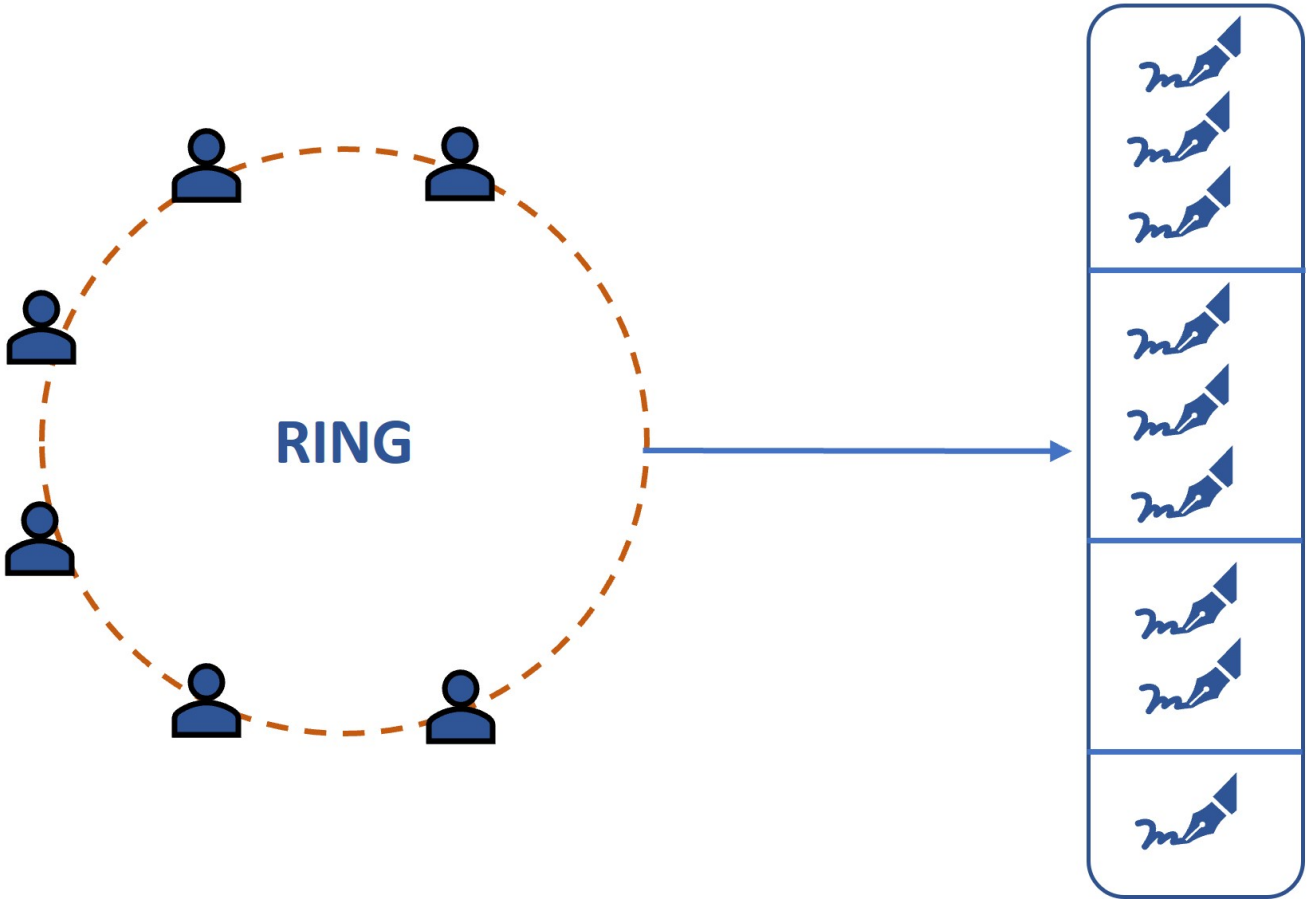
- Feedback only for the teacher
- Even if the teacher is forced to give away information

An Anonymous Feedback System

- A solution to the anonymous feedback system is given by DVLRS [Beh+21].
- DVLRS combines linkable ring signatures and designated verifier signatures.

[Beh+21] Behrouz, Grontas, Konstantakatos, Pagourtzis, Spyrakou. Designated Verifier Linkable Ring Signatures

Linkable Ring Signatures

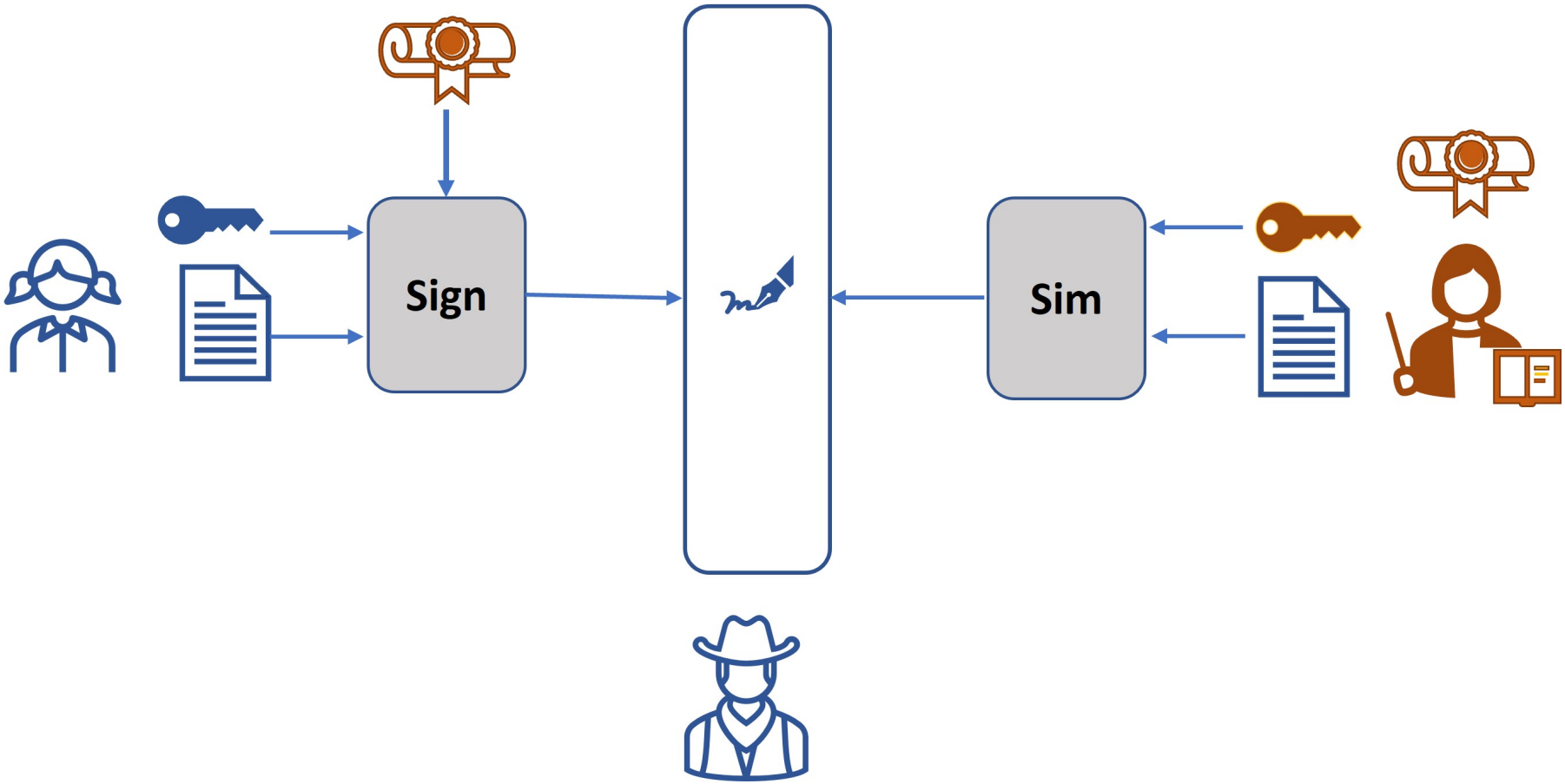


- Ring Signatures [RST01]
- Linkable Ring Signatures [LWW04]

[RST01] Rivest, Shamir, Tauman. How to Leak a Secret

[LWW04] Liu, Wei, Wong. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups

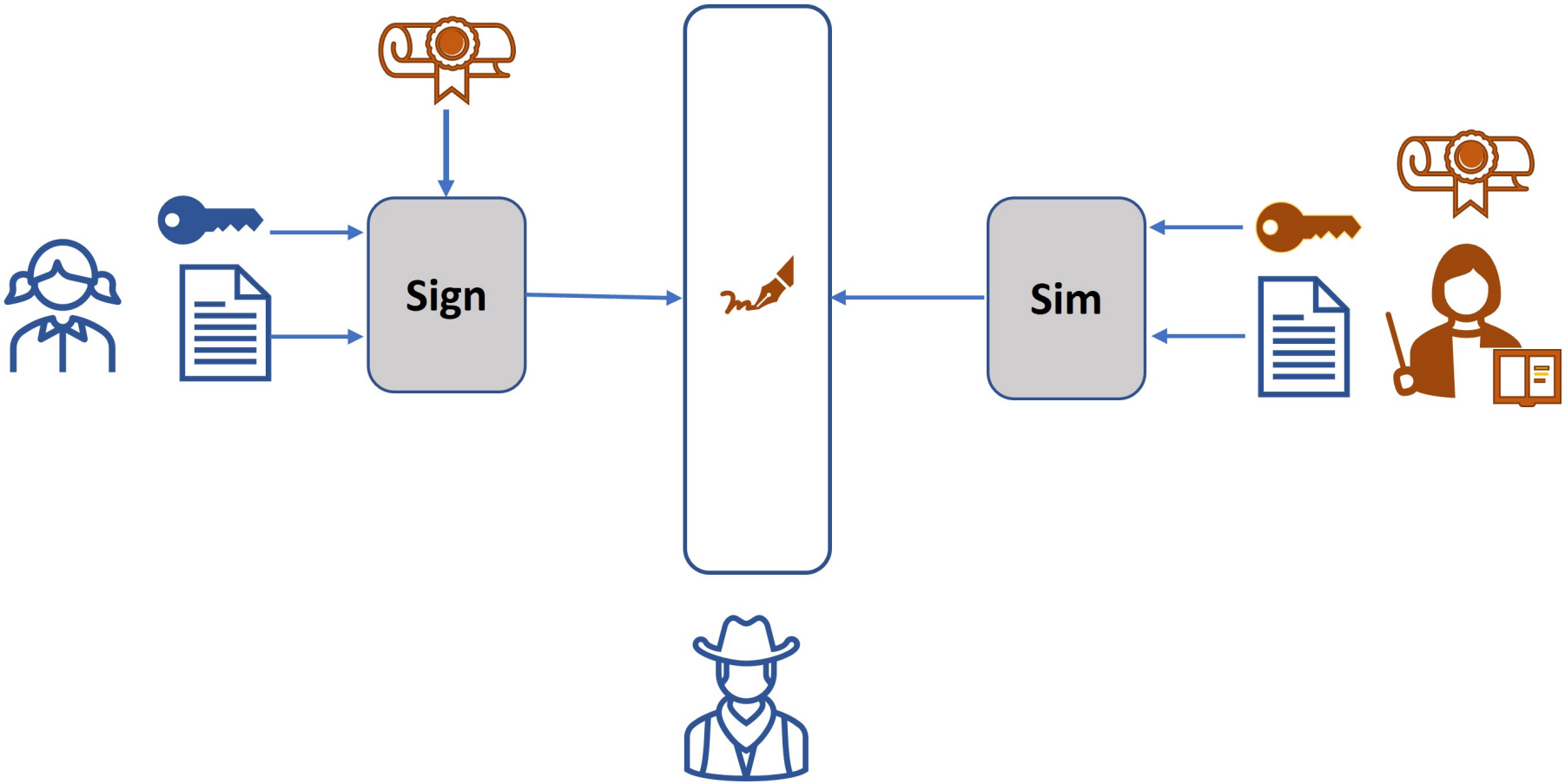
Designated-Verifier Signatures



- (Strong) Designated Verifier Signatures [JSI96]

[JSI96] Jakobsson, Sako, Impagliazzo. Designated Verifier Proofs and Their Applications

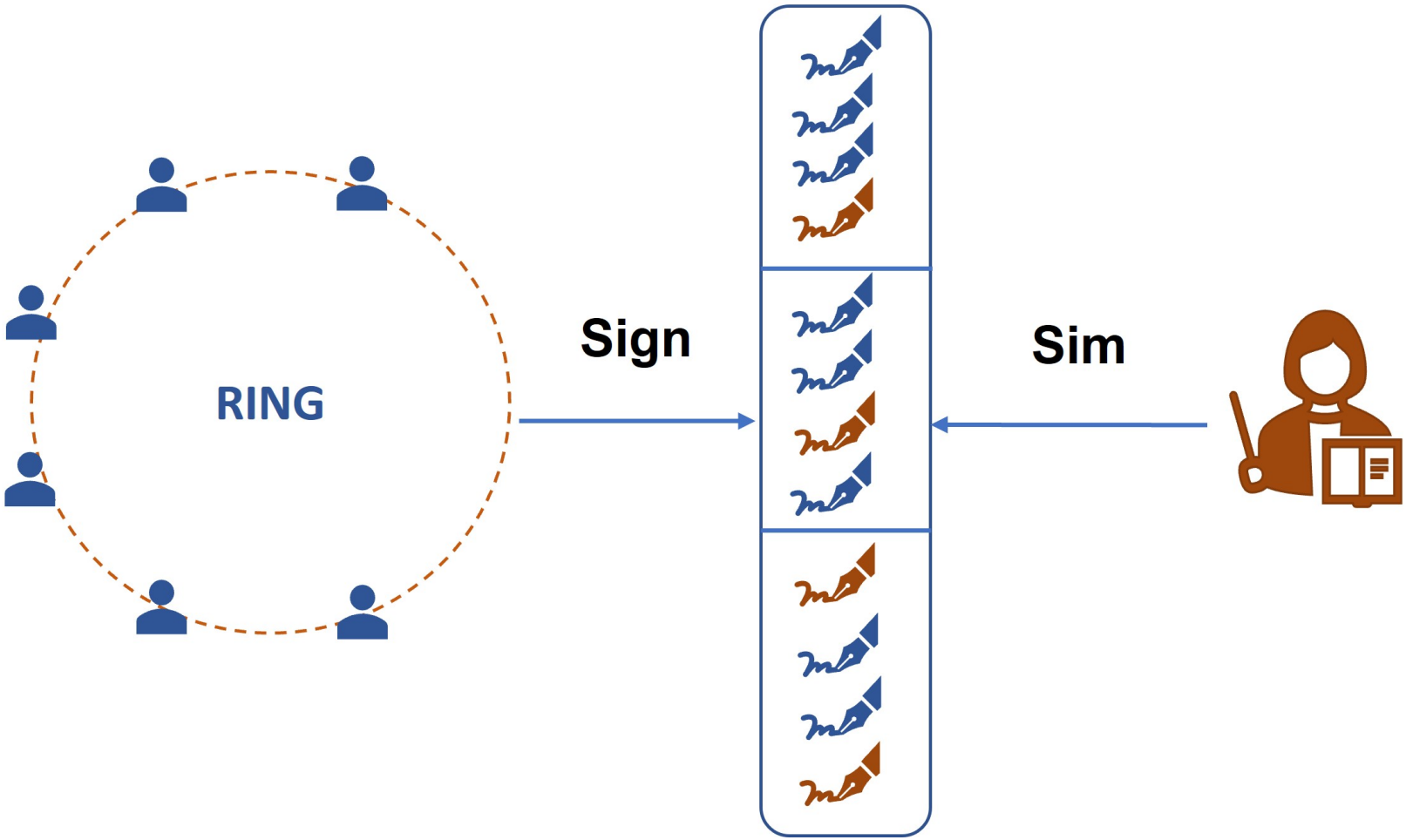
Designated-Verifier Signatures



- (Strong) Designated Verifier Signatures [JSI96]

[JSI96] Jakobsson, Sako, Impagliazzo. Designated Verifier Proofs and Their Applications

DVLRS Model



UDVLRS

- UDVLRS combines DVLRS [Beh+21] and ULRS [Liu+14]
- UDVLRS enhances the **anonymity** of DVLRS by making it unconditional.

[Beh+21] Behrouz, Grontas, Konstantakakos, Pagourtzis, Spyrakou. Designated Verifier Linkable Ring Signatures

[Liu+14] Liu, Au, Susilo, Zhou. Linkable Ring Signatures with Unconditional Anonymity.

UDVLRS Syntax

- $\mathsf{params} \leftarrow \mathsf{Setup}(\lambda)$
- $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}()$
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_\pi)$
- $\mathsf{pid} \leftarrow \mathsf{Extract}(\sigma)$
- $\sigma \leftarrow \mathsf{Sim}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \mathsf{sk}_D, \mathsf{pid})$
- $\{0,1\} \leftarrow \mathsf{Vrfy}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \sigma)$
- $\{0,1\} \leftarrow \mathsf{Link}(\sigma_1, \mathsf{ev}_1, \sigma_2, \mathsf{ev}_2)$

Adversarial Capabilities

Strong adaptive adversary

- Can add users to the system
- Can corrupt (take full control of) users
- Can request Signatures and Simulations

Security Properties

Unforgeability:
No one should be able to produce a valid signature except a member of the ring and the designated-verifier.

Anonymity:
No one, including the designated-verifier, should be able to identify the signer of a signature.
(Computationally unbounded $\mathcal{A}$)

Linkability:
If two signatures are signed with the same private key, they must be linked.

Non-slanderability:
No one should be able to maliciously link a signature to a specific ring member.

Non-transferability:
Signatures and simulations are indistinguishable.
(Computationally Unbounded $\mathcal{A}$)

Security Properties

Unforgeability:
No one should be able to produce a valid signature except a member of the ring and the designated-verifier.

Anonymity:
No one, including the designated-verifier, should be able to identify the signer of a signature.
(Computationally unbounded $\mathcal{A}$)

Linkability:
If two signatures are signed with the same private key, they must be linked.

Non-slanderability:
No one should be able to maliciously link a signature to a specific ring member.

Non-transferability:
Signatures and simulations are indistinguishable.
(Computationally Unbounded $\mathcal{A}$)

Security Properties

Unforgeability:
No one should be able to produce a valid signature except a member of the ring and the designated-verifier.

Anonymity:
No one, including the designated-verifier, should be able to identify the signer of a signature.
(Computationally unbounded $\mathcal{A}$)

Linkability:
If two signatures are signed with the same private key, they must be linked.

Non-slanderability:
No one should be able to maliciously link a signature to a specific ring member.

Non-transferability:
Signatures and simulations are indistinguishable.
(Computationally Unbounded $\mathcal{A}$)

Security Properties

Unforgeability:
No one should be able to produce a valid signature except a member of the ring and the designated-verifier.

Anonymity:
No one, including the designated-verifier, should be able to identify the signer of a signature.
(Computationally unbounded $\mathcal{A}$)

Linkability:
If two signatures are signed with the same private key, they must be linked.

Non-slanderability:
No one should be able to maliciously link a signature to a specific ring member.

Non-transferability:
Signatures and simulations are indistinguishable.
(Computationally Unbounded $\mathcal{A}$)

Security Properties

Unforgeability:
No one should be able to produce a valid signature except a member of the ring and the designated-verifier.

Anonymity:
No one, including the designated-verifier, should be able to identify the signer of a signature.
(Computationally unbounded $\mathcal{A}$)

Linkability:
If two signatures are signed with the same private key, they must be linked.

Non-slanderability:
No one should be able to maliciously link a signature to a specific ring member.

Non-transferability:
Signatures and simulations are indistinguishable.
(Computationally Unbounded $\mathcal{A}$)

Construction

- $\mathbb{G}$, ord($\mathbb{G}$)$= q$, DLOG is hard.
- g, h generators of $\mathbb{G}$.
- Private keys $(x_i, y_i) \in \mathbb{Z}_q^2$, $i \in [n_L]$.
- Public keys $Z_i = g^{x_i} h^{y_i} \in \mathbb{G}$, $i \in [n_L]$.
- $\mathsf{H}_{\mathbb{G}} : \{0,1\}^* \to \mathbb{G}$, $\mathsf{H}_q\{0,1\}^* \to \mathbb{Z}_q$.

$\mathsf{Sign}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_\pi)$

Signer π **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- t : linking tag
- K: uses the public keys of the ring
- K': uses the linking tag t
- K'': uses the DV's pk

- $t \leftarrow e^{x_\pi}$
- $K \leftarrow g^{r_x} h^{r_y} \cdot \prod_{\substack{i \in [n] \\ i \neq \pi}} Z_i{}^{c_i + w_i}$
- $K' \leftarrow e^{r_x} \cdot t^{\sum_{\substack{i \in [n] \\ i \neq \pi}} c_i + w_i}$
- $K'' \leftarrow h^s \cdot \mathsf{pk}_D{}^r \cdot \prod_{i=1}^{n} g^{w_i}$

Signer π **commits** on:

$c \leftarrow \mathsf{H}_q(m, L, \mathsf{ev}, t, K, K', K'')$

$$c_\pi \leftarrow c - \sum_{\substack{i=1, \\ i \neq \pi}}^{n} c_i$$
$$\tilde{x} \leftarrow (r_x - (c_\pi + w_\pi) x_\pi) \mod q$$
$$\tilde{y} \leftarrow (r_y - (c_\pi + w_\pi) y_\pi) \mod q$$

Signer π **computes**: $c_\pi, \tilde{x}, \tilde{y}$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \ldots, c_\pi, \ldots, c_n, \{w_i\}_{i=1}^{n})$$

$\mathsf{Sign}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_\pi)$

Signer π **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- t : linking tag
- K: uses the public keys of the ring
- K': uses the linking tag t
- K'': uses the DV's pk

- $t \leftarrow e^{x_\pi}$
- $K \leftarrow g^{r_x} h^{r_y} \cdot \prod_{\substack{i \in [n] \\ i \neq \pi}} {Z_i}^{c_i + w_i}$
- $K' \leftarrow e^{r_x} \cdot t^{\sum_{\substack{i \in [n] \\ i \neq \pi}} c_i + w_i}$
- $K'' \leftarrow h^s \cdot {\mathsf{pk}_D}^r \cdot \prod_{i=1}^{n} g^{w_i}$

Signer π **commits** on:

$c \leftarrow \mathsf{H}_q(m, L, \mathsf{ev}, t, K, K', K'')$

$c_\pi \leftarrow c - \sum_{\substack{i=1, \\ i \neq \pi}}^{n} c_i$

$\tilde{x} \leftarrow (r_x - (c_\pi + w_\pi) x_\pi) \mod q$

$\tilde{y} \leftarrow (r_y - (c_\pi + w_\pi) y_\pi) \mod q$

Signer π **computes**: $c_\pi, \tilde{x}, \tilde{y}$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \ldots, c_\pi, \ldots, c_n, \{w_i\}_{i=1}^{n})$$

$\mathsf{Sign}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_\pi)$

Signer π **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- t : linking tag
- K: uses the public keys of the ring
- K': uses the linking tag t
- K'': uses the DV's pk

- $t \leftarrow e^{x_\pi}$
- $K \leftarrow g^{r_x} h^{r_y} \cdot \prod_{\substack{i \in [n] \\ i \neq \pi}} {Z_i}^{c_i + w_i}$
- $K' \leftarrow e^{r_x} \cdot t^{\sum_{\substack{i \in [n] \\ i \neq \pi}} c_i + w_i}$
- $K'' \leftarrow h^s \cdot {\mathsf{pk}_D}^r \cdot \prod_{i=1}^{n} g^{w_i}$

Signer π **commits** on:
$c \leftarrow \mathsf{H}_q(m, L, \mathsf{ev}, t, K, K', K'')$

$$c_\pi \leftarrow c - \sum_{\substack{i=1, \\ i \neq \pi}}^{n} c_i$$
$$\tilde{x} \leftarrow (r_x - (c_\pi + w_\pi) x_\pi) \mod q$$
$$\tilde{y} \leftarrow (r_y - (c_\pi + w_\pi) y_\pi) \mod q$$

Signer π **computes**: $c_\pi, \tilde{x}, \tilde{y}$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \ldots, c_\pi, \ldots, c_n, \{w_i\}_{i=1}^{n})$$

$\mathsf{Sign}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_\pi)$

Signer π **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- t : linking tag
- K: uses the public keys of the ring
- K': uses the linking tag t
- K'': uses the DV's pk

- $t \leftarrow e^{x_\pi}$
- $K \leftarrow g^{r_x} h^{r_y} \cdot \prod_{\substack{i \in [n] \\ i \neq \pi}} {Z_i}^{c_i + w_i}$
- $K' \leftarrow e^{r_x} \cdot t^{\sum_{\substack{i \in [n] \\ i \neq \pi}} c_i + w_i}$
- $K'' \leftarrow h^s \cdot \mathsf{pk}_D{}^r \cdot \prod_{i=1}^{n} g^{w_i}$

Signer π **commits** on:
$c \leftarrow \mathsf{H}_q(m, L, \mathsf{ev}, t, K, K', K'')$

$$c_\pi \leftarrow c - \sum_{\substack{i=1, \\ i \neq \pi}}^{n} c_i$$
$$\tilde{x} \leftarrow (r_x - (c_\pi + w_\pi) x_\pi) \mod q$$
$$\tilde{y} \leftarrow (r_y - (c_\pi + w_\pi) y_\pi) \mod q$$

Signer π **computes**: $c_\pi, \tilde{x}, \tilde{y}$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \ldots, c_\pi, \ldots, c_n, \{w_i\}_{i=1}^{n})$$

$\mathsf{Sign}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_\pi)$

Signer π **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- t : linking tag
- K: uses the public keys of the ring
- K': uses the linking tag t
- K'': uses the DV's pk

- $t \leftarrow e^{x_\pi}$
- $K \leftarrow g^{r_x} h^{r_y} \cdot \prod_{\substack{i \in [n] \\ i \neq \pi}} {Z_i}^{c_i + w_i}$
- $K' \leftarrow e^{r_x} \cdot t^{\sum_{\substack{i \in [n] \\ i \neq \pi}} c_i + w_i}$
- $K'' \leftarrow h^s \cdot {\mathsf{pk}_D}^r \cdot \prod_{i=1}^{n} g^{w_i}$

Signer π **commits** on:

$c \leftarrow \mathsf{H}_q(m, L, \mathsf{ev}, t, K, K', K'')$

$$c_\pi \leftarrow c - \sum_{\substack{i=1, \\ i \neq \pi}}^{n} c_i$$

$$\tilde{x} \leftarrow (r_x - (c_\pi + w_\pi) x_\pi) \mod q$$

$$\tilde{y} \leftarrow (r_y - (c_\pi + w_\pi) y_\pi) \mod q$$

Signer π **computes**: $c_\pi, \tilde{x}, \tilde{y}$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \ldots, c_\pi, \ldots, c_n, \{w_i\}_{i=1}^{n})$$

$\mathsf{Sign}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_\pi)$

Signer π **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- t : linking tag
- K: uses the public keys of the ring
- K': uses the linking tag t
- K'': uses the DV's pk

- $t \leftarrow e^{x_\pi}$
- $K \leftarrow g^{r_x} h^{r_y} \cdot \prod_{\substack{i \in [n] \\ i \neq \pi}} {Z_i}^{c_i + w_i}$
- $K' \leftarrow e^{r_x} \cdot t^{\sum_{\substack{i \in [n] \\ i \neq \pi}} c_i + w_i}$
- $K'' \leftarrow h^s \cdot {\mathsf{pk}_D}^r \cdot \prod_{i=1}^{n} g^{w_i}$

Signer π **commits** on:

$c \leftarrow \mathsf{H}_q(m, L, \mathsf{ev}, t, K, K', K'')$

$$c_\pi \leftarrow c - \sum_{\substack{i=1, \\ i \neq \pi}}^{n} c_i$$

$$\tilde{x} \leftarrow (r_x - (c_\pi + w_\pi) x_\pi) \mod q$$

$$\tilde{y} \leftarrow (r_y - (c_\pi + w_\pi) y_\pi) \mod q$$

Signer π **computes**: $c_\pi, \tilde{x}, \tilde{y}$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \ldots, c_\pi, \ldots, c_n, \{w_i\}_{i=1}^{n})$$

$\mathsf{Sim}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_D)$

DV **chooses**: t linking tag

DV **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- K_D: uses the public keys of the ring
- K'_D: uses the linking tag
- K''_D: commit on random values

- $K_D \leftarrow g^{\chi} h^{\psi} \cdot {Z_1}^{\alpha} \cdot \prod_{i=2}^{n} {Z_i}^{c_i + w_i}$
- $K'_D \leftarrow e^{\chi} \cdot t^{\alpha + \sum_{i=2}^{n} c_i + w_i}$
- $K''_D \leftarrow g^{\beta} h^{\gamma} \cdot \prod_{i=2}^{n} g^{w_i}$

DV **commits** on:

$c = \mathsf{H}_q(m, L, \mathsf{ev}, t, K_D, K'_D, K''_D)$

$c_1 \leftarrow c - \sum_{i=2}^{n} c_i$

$w_1 \leftarrow \alpha - c_1 \mod q$

$r \leftarrow (\beta - w_1) \cdot {x_D}^{-1} \mod q$

$s \leftarrow \gamma - r \cdot y_D \mod q$

DV **computes**: c_1, w_1, r, s

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \{c_i\}_{i=2}^{n}, w_1, \{w_i\}_{i=2}^{n})$$

$\mathsf{Sim}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_D)$

DV **chooses**: t linking tag

DV **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- K_D: uses the public keys of the ring
- K'_D: uses the linking tag
- K''_D: commit on random values

- $K_D \leftarrow g^{\chi} h^{\psi} \cdot {Z_1}^{\alpha} \cdot \prod_{i=2}^{n} {Z_i}^{c_i + w_i}$
- $K'_D \leftarrow e^{\chi} \cdot t^{\alpha + \sum_{i=2}^{n} c_i + w_i}$
- $K''_D \leftarrow g^{\beta} h^{\gamma} \cdot \prod_{i=2}^{n} g^{w_i}$

DV **commits** on:

$c = \mathsf{H}_q(m, L, \mathsf{ev}, t, K_D, K'_D, K''_D)$

$c_1 \leftarrow c - \sum_{i=2}^{n} c_i$

$w_1 \leftarrow \alpha - c_1 \mod q$

$r \leftarrow (\beta - w_1) \cdot {x_D}^{-1} \mod q$

$s \leftarrow \gamma - r \cdot y_D \mod q$

DV **computes**: c_1, w_1, r, s

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \{c_i\}_{i=2}^{n}, w_1, \{w_i\}_{i=2}^{n})$$

$\mathsf{Sim}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_D)$

DV **chooses**: t linking tag

DV **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- K_D: uses the public keys of the ring
- K'_D: uses the linking tag
- K''_D: commit on random values

DV **commits** on:

$c = \mathsf{H}_q(m, L, \mathsf{ev}, t, K_D, K'_D, K''_D)$

DV **computes**: c_1, w_1, r, s

- $K_D \leftarrow g^{\chi} h^{\psi} \cdot {Z_1}^{\alpha} \cdot \prod_{i=2}^{n} {Z_i}^{c_i + w_i}$
- $K'_D \leftarrow e^{\chi} \cdot t^{\alpha + \sum_{i=2}^{n} c_i + w_i}$
- $K''_D \leftarrow g^{\beta} h^{\gamma} \cdot \prod_{i=2}^{n} g^{w_i}$

$c_1 \leftarrow c - \sum_{i=2}^{n} c_i$

$w_1 \leftarrow \alpha - c_1 \mod q$

$r \leftarrow (\beta - w_1) \cdot {x_D}^{-1} \mod q$

$s \leftarrow \gamma - r \cdot y_D \mod q$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \{c_i\}_{i=2}^{n}, w_1, \{w_i\}_{i=2}^{n})$$

$\mathsf{Sim}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_D)$

DV **chooses**: t linking tag

DV **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- K_D: uses the public keys of the ring
- K'_D: uses the linking tag
- K''_D: commit on random values

DV **commits** on:

$c = \mathsf{H}_q(m, L, \mathsf{ev}, t, K_D, K'_D, K''_D)$

DV **computes**: c_1, w_1, r, s

- $K_D \leftarrow g^{\chi} h^{\psi} \cdot {Z_1}^{\alpha} \cdot \prod_{i=2}^{n} {Z_i}^{c_i + w_i}$
- $K'_D \leftarrow e^{\chi} \cdot t^{\alpha + \sum_{i=2}^{n} c_i + w_i}$
- $K''_D \leftarrow g^{\beta} h^{\gamma} \cdot \prod_{i=2}^{n} g^{w_i}$

$c_1 \leftarrow c - \sum_{i=2}^{n} c_i$

$w_1 \leftarrow \alpha - c_1 \mod q$

$r \leftarrow (\beta - w_1) \cdot {x_D}^{-1} \mod q$

$s \leftarrow \gamma - r \cdot y_D \mod q$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \{c_i\}_{i=2}^{n}, w_1, \{w_i\}_{i=2}^{n})$$

$\mathsf{Sim}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_D)$

DV **chooses**: t linking tag

DV **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- K_D: uses the public keys of the ring
- K'_D: uses the linking tag
- K''_D: commit on random values

DV **commits** on:

$c = \mathsf{H}_q(m, L, \mathsf{ev}, t, K_D, K'_D, K''_D)$

DV **computes**: c_1, w_1, r, s

- $K_D \leftarrow g^{\chi} h^{\psi} \cdot {Z_1}^{\alpha} \cdot \prod_{i=2}^{n} {Z_i}^{c_i + w_i}$
- $K'_D \leftarrow e^{\chi} \cdot t^{\alpha + \sum_{i=2}^{n} c_i + w_i}$
- $K''_D \leftarrow g^{\beta} h^{\gamma} \cdot \prod_{i=2}^{n} g^{w_i}$

$$c_1 \leftarrow c - \sum_{i=2}^{n} c_i$$
$$w_1 \leftarrow \alpha - c_1 \mod q$$
$$r \leftarrow (\beta - w_1) \cdot {x_D}^{-1} \mod q$$
$$s \leftarrow \gamma - r \cdot y_D \mod q$$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \{c_i\}_{i=2}^{n}, w_1, \{w_i\}_{i=2}^{n})$$

$\mathsf{Sim}(\mathsf{ev}, L, m, \mathsf{pk}_D, \mathsf{sk}_D)$

DV **chooses**: t linking tag

DV **computes**:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- K_D: uses the public keys of the ring
- K'_D: uses the linking tag
- K''_D: commit on random values

DV **commits** on:

$c = \mathsf{H}_q(m, L, \mathsf{ev}, t, K_D, K'_D, K''_D)$

DV **computes**: c_1, w_1, r, s

- $K_D \leftarrow g^{\chi} h^{\psi} \cdot {Z_1}^{\alpha} \cdot \prod_{i=2}^{n} {Z_i}^{c_i + w_i}$
- $K'_D \leftarrow e^{\chi} \cdot t^{\alpha + \sum_{i=2}^{n} c_i + w_i}$
- $K''_D \leftarrow g^{\beta} h^{\gamma} \cdot \prod_{i=2}^{n} g^{w_i}$

$$c_1 \leftarrow c - \sum_{i=2}^{n} c_i$$
$$w_1 \leftarrow \alpha - c_1 \mod q$$
$$r \leftarrow (\beta - w_1) \cdot {x_D}^{-1} \mod q$$
$$s \leftarrow \gamma - r \cdot y_D \mod q$$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, c_1, \{c_i\}_{i=2}^{n}, w_1, \{w_i\}_{i=2}^{n})$$

$\mathsf{Vrfy}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \sigma)$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$$

compute:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- K: PoK of one of the secret keys of the ring
- K': proof of using the correct linking tag
- K'': PoK of the DV's secret key

- $K \leftarrow g^{\tilde{x}} h^{\tilde{y}} \cdot \prod_{i=1}^{n} Z_i{}^{c_i + w_i}$
- $K' \leftarrow e^{\tilde{x}} \cdot t^{+\sum_{i=1}^{n} c_i + w_i}$
- $K'' \leftarrow h^s \cdot \mathsf{pk}_D^r \cdot \prod_{i=2}^{n} g^{w_i}$

Verify that:

$$\sum_{i=1}^{n} c_i = \mathsf{H}_q(\mathtt{m}, L, \mathsf{ev}, t, K, K', K'')$$

$\mathsf{Vrfy}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \sigma)$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$$

compute:

- $e \leftarrow \mathsf{H}_G(\mathtt{ev})$
- K: PoK of one of the secret keys of the ring
- K': proof of using the correct linking tag
- K'': PoK of the DV's secret key

- $K \leftarrow g^{\tilde{x}} h^{\tilde{y}} \cdot \prod_{i=1}^{n} Z_i{}^{c_i + w_i}$
- $K' \leftarrow e^{\tilde{x}} \cdot t^{+\sum_{i=1}^{n} c_i + w_i}$
- $K'' \leftarrow h^s \cdot \mathsf{pk}_D^r \cdot \prod_{i=2}^{n} g^{w_i}$

Verify that:

$$\sum_{i=1}^{n} c_i = \mathsf{H}_q(\mathtt{m}, L, \mathsf{ev}, t, K, K', K'')$$

$\mathsf{Vrfy}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \sigma)$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$$

compute:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- K: PoK of one of the secret keys of the ring
- K': proof of using the correct linking tag
- K'': PoK of the DV's secret key

- $K \leftarrow g^{\tilde{x}} h^{\tilde{y}} \cdot \prod_{i=1}^{n} Z_i{}^{c_i + w_i}$
- $K' \leftarrow e^{\tilde{x}} \cdot t^{+\sum_{i=1}^{n} c_i + w_i}$
- $K'' \leftarrow h^s \cdot \mathsf{pk}_D^r \cdot \prod_{i=2}^{n} g^{w_i}$

Verify that:

$$\sum_{i=1}^{n} c_i = \mathsf{H}_q(\mathtt{m}, L, \mathsf{ev}, t, K, K', K'')$$

$\mathsf{Vrfy}(\mathsf{ev}, L, \mathtt{m}, \mathsf{pk}_D, \sigma)$

$$\sigma = (t, \tilde{x}, \tilde{y}, r, s, \{c_i\}_{i=1}^n, \{w_i\}_{i=1}^n)$$

compute:

- $e \leftarrow \mathsf{H}_G(\mathsf{ev})$
- K: PoK of one of the secret keys of the ring
- K': proof of using the correct linking tag
- K'': PoK of the DV's secret key

- $K \leftarrow g^{\tilde{x}} h^{\tilde{y}} \cdot \prod_{i=1}^{n} Z_i{}^{c_i + w_i}$
- $K' \leftarrow e^{\tilde{x}} \cdot t^{+\sum_{i=1}^{n} c_i + w_i}$
- $K'' \leftarrow h^s \cdot \mathsf{pk}_D^r \cdot \prod_{i=2}^{n} g^{w_i}$

Verify that:

$$\sum_{i=1}^{n} c_i = \mathsf{H}_q(\mathtt{m}, L, \mathsf{ev}, t, K, K', K'')$$

Security Analysis (Proof Sketch)

Unforgeability

- Assume adversary $\mathcal{A}$ can forge with non negligible probability
- Use forking lemma
- Solve the MDLR problem
- The MDLR problem:
  Let $\mathbb{G}$ be a cyclic group of prime order q, $\mathbb{G} =< g >$ and $Y_1, Y_2, \ldots, Y_n \leftarrow \mathbb{G}, Y_1 \neq 1_{\mathbb{G}}$. A solution to the MDLR problem is a tuple $(\phi_1, \phi_2, \ldots, \phi_n) \in \mathbb{Z}_q^n$ such that $Y_1 \cdot Y_2^{\phi_2} \cdots Y_n^{\phi_n} = g^{\phi_1}$ and $\sum_{i=1}^{n} \phi_i \neq 0 \pmod{q}$
- MDLR is equivalent to DLOG, which yields contradiction

Security Analysis (Proof Sketch)

Unforgeability

Anonymity

- Let σ be a signature and t its linking tag.
- Note that only the linking tag can leak out information about the identity of the signer.
- Assume $\mathcal{A}$ can solve DLOG and find x such that $e^x = t$
- $\mathcal{A}$ cannot tell to which public key the linking tag t corresponds

Security Analysis (Proof Sketch)

Unforgeability

Anonymity

Linkability

- Assume adversary $\mathcal{A}$ owns a pair of secret key in the ring L and can produce 2 pairwise unlinkable signatures
- Use forking lemma
- Solve the MDLR problem, which yields contradiction

Security Analysis (Proof Sketch)

Unforgeability

Anonymity

Linkability

Non-slanderability

- Assume adversary $\mathcal{A}$ is given a signature σ and can produce a signature σ' s.t. $\mathsf{Link}(\sigma) = \mathsf{Link}(\sigma')$
- Use forking lemma
- Solve the DLOG problem, which yields contradiction.

Security Analysis (Proof Sketch)

Unforgeability

Anonymity

Linkability

Non-slanderability

Non-transferability

- Given a $\sigma \leftarrow$ Sign and a $\sigma' \leftarrow$ Sim on the same $\mathtt{ev}, L, DV, t$ the components of σ, σ' follow the same distributions.

Comparison of Ring Signature Schemes

Signature	Unforgeability	Anonymity	Linkability	Non-Slanderability	Non-Transferability
RS[AOS02]	DLOG	Unconditional	–	–	–
LRS [LWW04]	DLOG	DDH	DLOG	DLOG	–
ULRS [Liu+14]	DLOG	Unconditional	MDLR	DLOG	–
DVLRS [Beh+21]	DLOG	DDH	DLOG	DLOG	Unconditional
UDVLRS	MDLR/DLOG	Unconditional	MDLR	DLOG	Unconditional

- DVLRS inherits the anonymity of LRS, that is weaker than RS
- UDVLRS achieves unconditional anonymity, inherited by ULRS

[AOS02] Abe, Ohkubo, Suzuki. 1-out-of-n Signatures from a Variety of Keys.

[LWW04] Liu, Wei, Wong. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups

[Liu+14] Liu, Au, Susilo, Zhou. Linkable Ring Signatures with Unconditional Anonymity.

[Beh+21] Behrouz, Grontas, Konstantakakos, Pagourtzis, Spyrakou. Designated Verifier Linkable Ring Signatures


Thank
you