Designated-Verifier Ring Signatures: Strong Definitions, Generic Constructions and Efficient Instantiations

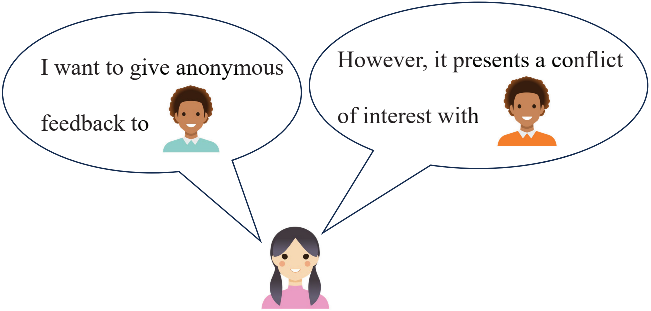
Jiaming Wen, Willy Susilo, Yanhua Zhang, Fuchun Guo, Huanguo Zhang

ICISC 2024, Seoul, South Korea

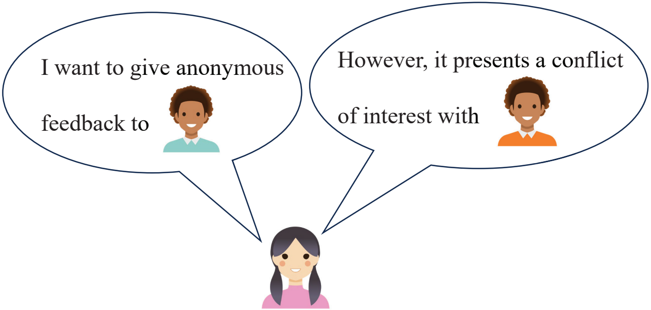
Outline

Motivation & Definitions

Motivation – Anonymous Feedback



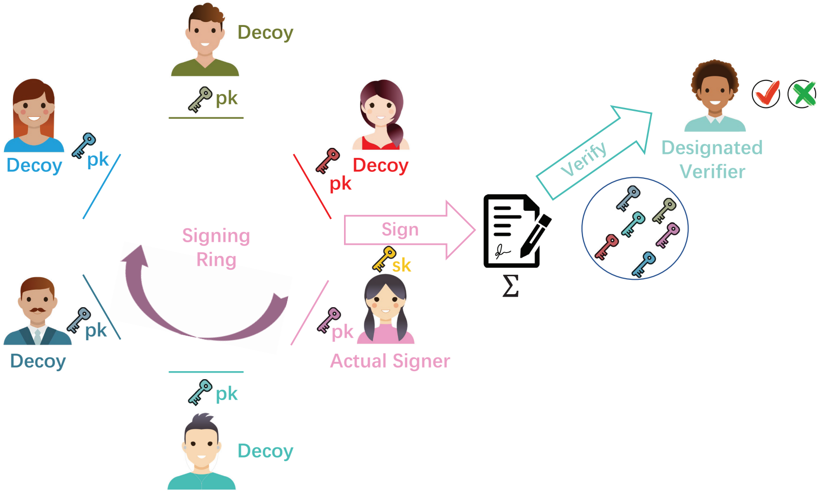
Motivation – Anonymous Feedback



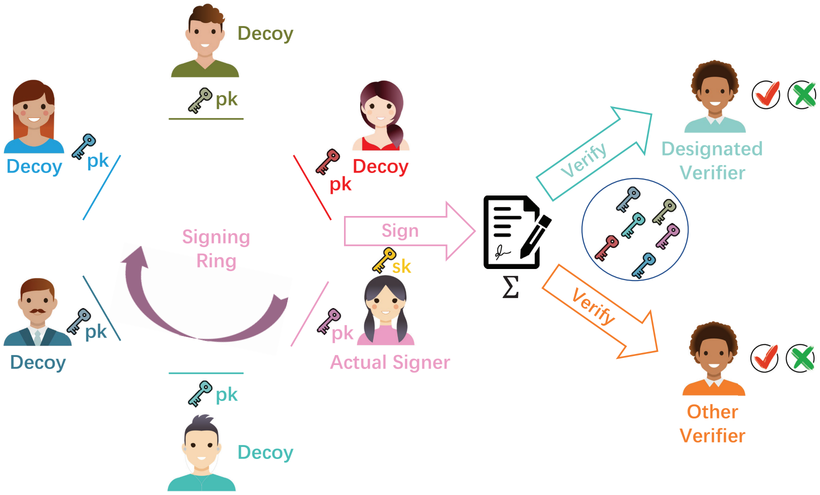
Requirements:

1. Feedback must remain anonymous
2. Feedback can be only provided by registered users
3. Feedback is exclusively to the specific user, even this user is forced to give away information, it cannot succeed

Can we use Ring Signature ?

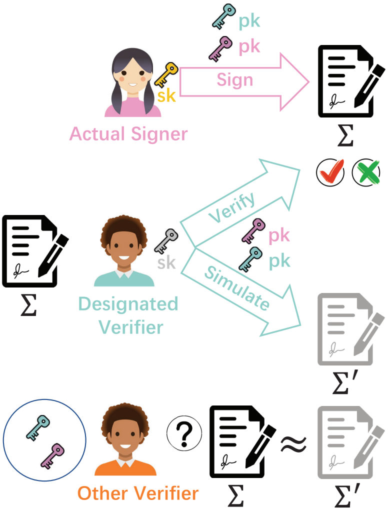


Can we use Ring Signature ?



However, the Requirement 3 cannot be addressed!

Borrow the idea of Designated-Verifier Signature [JSI96]



For Other Verifier:

- **Weak:** It can verify Σ and Σ', but cannot distinguish them.
- **Strong:** It cannot verify and distinguish Σ and Σ'.

[JSI96] Jakobsson, M., Sako, K., Impagliazzo, R.: Designated verifier proofs and their applications. In: EUROCRYPT 1996.

Related Work and Our Goal

Limitations of existing Designated-Verifier Ring Signature (DVRS):

- **Weak Definition:** DVRS schemes [BGKPS21, BBGPSV22] only achieve the Weak Designated-Verifier Property.
- **Increased Sizes:** Signature sizes linearly scale with ring sizes.
- **Pre-Quantum:** Based on pre-quantum assumptions like DL.

Goal: Strong Definition, Shorter Sizes, and Post-Quantum!

[BGKPS21] Behrouz, P., Grontas, P., Konstantakatos, V., Pagourtzis, A., Spyrakou, M.: Designated-Verifier Linkable Ring Signatures. In: ICISC 2021.

[BBGPSV22] Balla, D., Behrouz, P., Grontas, P., Pagourtzis, A., Spyrakou, M., Vrettos, G.: Designated-Verifier Linkable Ring Signatures with unconditional anonymity. In: International Conference on Algebraic Informatics 2022.

Algorithm Definitions

$\mathsf{DVRS} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify}, \mathsf{Sim})$

- $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$: Initializes public parameters pp using the security parameter λ.
- $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$: Generates a key pair $(\mathsf{pk}, \mathsf{sk})$.
- $\Sigma \leftarrow \mathsf{Sign}(\mathsf{R}, \mathsf{pk}_D, \mathsf{sk}_\pi, M)$: Generates a signature Σ for the designated-verifier, regarding the ring R and the message M.
- $\{0,1\} \leftarrow \mathsf{Verify}(\mathsf{R}, \mathsf{pk}_D, \mathsf{sk}_D, M, \Sigma)$: Verifies a signature Σ.
- $\Sigma' \leftarrow \mathsf{Sim}(\mathsf{R}, \mathsf{pk}_D, \mathsf{sk}_D, M)$: Simulates a signature Σ' by the designated-verifier, regarding the ring R and the message M.

Security Definitions

Unforgeability (UF)

No one can produce a valid signature except a ring member and the designated-verifier.

Signer Anonymity (SA)

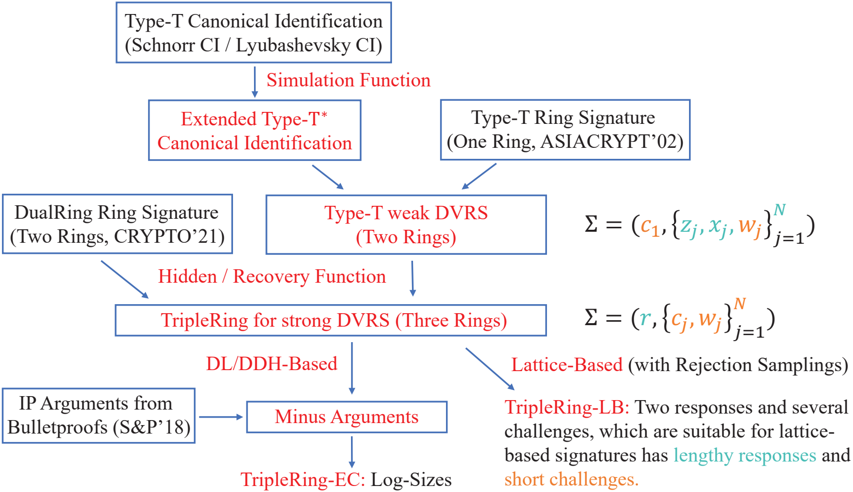
No one, including the designate-verifier, should be able to identify the signer of a signature.

Non-Transferability (NT)

Signatures from a ring member and Simulated Signatures from the designated-verifier are indistinguishable.

Constructions & Instantiations

Technical Overview

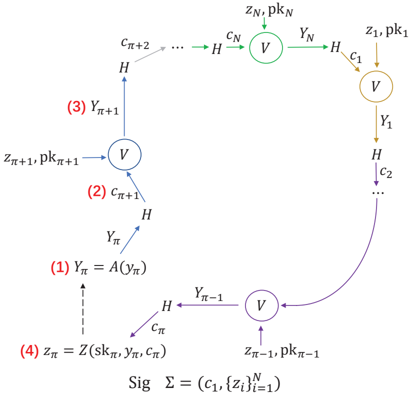


Type-T Canonical Identification and Signature

Type-T Canonical Identification and Signature $\langle$e.g. Schnorr$\rangle$

1. A commit function Y that outputs a commitment Y
   $A(y) \rightarrow Y = g^y$
2. A hash function H that outputs a challenge $c \in \mathcal{S}_c$
   $H(M, Y) \rightarrow c$
3. A response function Z that outputs a response z
   $Z(\mathsf{sk}, y, c) \rightarrow z = y - c \cdot \mathsf{sk}$
4. A verification function V that reconstruct Y from $\Sigma = (c, z)$, and runs H to check whether c is correct
   $V(\mathsf{pk}, z, c) \rightarrow Y = g^z \cdot \mathsf{pk}^c,\ c = H(M, Y)$

Type-T Ring Signature [AOS02]



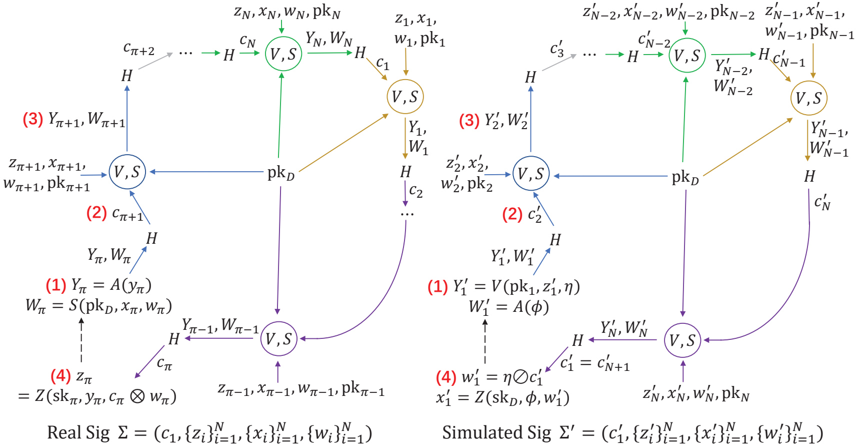
Signer runs as follows:

1. Picks r_π to generate Y_π via the commit function A
2. Computes next challenge $c_{\pi+1}$ via the hash function H
3. Uses a random response $z_{\pi+1}$ and $\mathrm{pk}_{\pi+1}$ to reconstruct $Y_{\pi+1}$ via the verification function V
   A ring is formed sequentially
4. Closes the ring by computing z_π via the response function Z

[AOS02] Abe, M., Ohkubo, M., Suzuki, K.: 1-out-of-n Signatures from a Variety of Keys. In: ASIACRYPT 2002.

Our first attempt: Type-T weak DVRS

- add a simulation function S $S(\mathrm{pk}_D, x, w) \rightarrow W = g^x \cdot \mathrm{pk}_D^w$



From Type-T to Type-T* – commutative group operations

Hash functions H in the ring, making it difficult to shorten sizes

Goal: Separate it via commutative group operations, then compress

- A verification function V can be rewritten as:

  $V(\mathrm{pk}, z, c) = V_1(z) \odot V_2(\mathrm{pk}, c) \quad V(\mathrm{pk}, z, c) \rightarrow Y = g^z \cdot \mathrm{pk}^c$
- A simulation function S can be rewritten as:

  $S(\mathrm{pk}_D, x, w) = S_1(x) \odot S_2(\mathrm{pk}_D, w) \quad S(\mathrm{pk}_D, x, w) \rightarrow W = g^x \cdot \mathrm{pk}_D^w$
- V_1 and S_1 are additive/multiplicative homomorphic
- Given sk and c, there exists a function $\mathcal{I}_V$ can compute

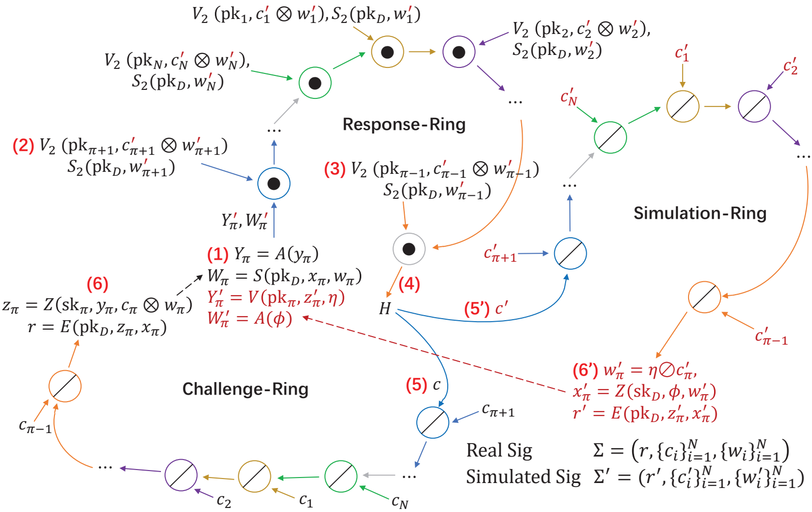
$$V_1(\mathcal{I}_V(\mathrm{sk}, c)) = V_2(\mathrm{pk}, c)$$

- Given sk_D and c, there exists a function $\mathcal{I}_S$ can compute

$$S_1(\mathcal{I}_S(\mathrm{sk}_D, w)) = S_2(\mathrm{pk}_D, w)$$

[YELAD21] Yuen, T.H., Esgin, M.F., Liu, J.K., Au, M.H., Ding, Z.: DualRing: Generic Construction of Ring Signatures with Efficient Instantiations. In: CRYPTO 2021.

TripleRing: A Generic Construction for strong DVRS



TripleRing-EC: A Logarithmic-Size Instance from DL and DDH

- A commit function $A(y) := g^y$ for $y \leftarrow_\$ \mathcal{S}_y = \mathbb{Z}_p$
- A hash function $H : \{0,1\}^* \to \mathcal{S}_c = \mathbb{Z}_p$
- A response function $Z(\mathsf{sk}, y, c) := y - c \cdot \mathsf{sk}$
- A verification function $V = V_1(z) \cdot V_2(\mathsf{pk}, c) = g^z \cdot \mathsf{pk}^c$
- A simulation function $S = S_1(x) \cdot S_2(\mathsf{pk}_D, w) = g^x \cdot \mathsf{pk}_D^w$
- A hidden function E and a recovery function F. Similar with ElGamal PKE

Remarks: Minus Arguments, adapted from the Inner Product (IP) Arguments used in Bulletproofs, enable logarithmic signature sizes

TripleRing-EC: A Logarithmic-Size Instance from DL and DDH

Table 1: Comparison of Signature Sizes for DL-based DVRS schemes

Scheme	# Elements in Signature		Signature Sizes for Ring Sizes N				Asymptotic Signature Sizes	Designated Verifier Property
	$\mathbb{G}$ (33 Bytes)	$\mathbb{Z}_p$ (32 Bytes)	2^4	2^8	2^{12}	2^{16}		
[BBGPSV22]	1	$2N+4$	1.1 KB	16.2 KB	256.2 KB	4.0 GB	$O(N)$	Weak
[BGKPS21]	1	$3N+1$	1.6 KB	24.1 KB	384.1 KB	6.0 GB	$O(N)$	Weak
TripleRing-EC (This work)	$4\log N+6$	5	0.9 KB	1.4 KB	1.9 KB	2.4 KB	$O(\log N)$	Strong

[BGKPS21] Behrouz, P., Grontas, P., Konstantakatos, V., Pagourtzis, A., Spyrakou, M.: Designated-Verifier Linkable Ring Signatures. In: ICISC 2021.

[BBGPSV22] Balla, D., Behrouz, P., Grontas, P., Pagourtzis, A., Spyrakou, M., Vrettos, G.: Designated-Verifier Linkable Ring Signatures with unconditional anonymity. In: International Conference on Algebraic Informatics 2022.

TripleRing-LB: A Post-Quantum Instance from Lattice

- A commit function $A(y) := \mathbf{A}\mathbf{y}$ for $y = \mathbf{y} \leftarrow_{\$} D_{\sigma}^{m}$
- A hash function $H : \{0,1\}^* \rightarrow \mathcal{S}_c = \{\mathbf{v} : \mathbf{v} \in \{-1,0,1\}^k, \|\mathbf{v}\|_1 \leq \kappa\}$
- A response function $Z(\mathsf{sk}, y, c) := \mathbf{S} \cdot \mathbf{c} - \mathbf{y}$
- A verification function $V = V_1(z) + V_2(\mathsf{pk}, c) = -\mathbf{A} \cdot \mathbf{z} + \mathbf{T} \cdot \mathbf{c}$
- A simulation function $S = S_1(x) + S_2(\mathsf{pk}_D, w) = -\mathbf{A} \cdot \mathbf{x} + \mathbf{T}_D \cdot \mathbf{w}$
- A hidden function E and a recovery function F. Similar with MP lattice trapdoor function

Remarks: This instance based on assumptions that believed to be post-quantum secure. Each signature includes two responses and several challenges, making it suitable for lattice-based signatures where responses are lengthy and challenges are short

Conclusion

Conclusion and Future Work

Conclusion:

- Give a strong model for Designated-Verifier Ring Signature
- Propose a generic construction for this model
- Provide an instantiation based on DL and DDH – log-size
- Provide an instantiation based on lattice – post-quantum

Future Work:

- Develop more efficient (post-quantum) designs
- Extend the model to support Multiple Designated Verifiers

Thanks!

Jiaming Wen

Website: https://jiamiwen.github.io

E-mail: wenjm@whu.edu.cn