On the Black-Box Impossibility of Multi-Designated Verifiers Signature Schemes from Ring Signature Schemes

Kyosuke Yamashita[1,2] and Keisuke Hara[2,3]

[1] Osaka University
[2] National Institute of Advanced Industrial Science and Technology
[3] Yokohama National University

Abstract. From the work by Laguillaumie and Vergnaud in ICICS'04, it has been widely believed that multi-designated verifier signature schemes (MDVS) can be constructed from ring signature schemes in general. However in this paper, somewhat surprisingly, we prove that it is impossible to construct an MDVS scheme from a ring signature scheme in a black-box sense (in the standard model). The impossibility stems from the difference between the definitions of unforgeability. To the best of our knowledge, existing works demonstrating the constructions do not provide formal reduction from an MDVS scheme to a ring signature scheme, and thus the impossibility has been overlooked for a long time.

Keywords: multi-designated verifier signature · ring signature · black-box separation.

1 Introduction

A multi-designated verifiers signature scheme (MDVS) [15] is a special variant of a (standard) digital signature scheme. Its prominent property is the *off-the-record* (OTR) [3], a.k.a. source hiding, which guarantees that a set of verifiers designated by a signer is able to simulate the signer's signature. Due to this property, it is useless for non-designated verifiers to verify a signature, as they cannot decide if it is created by a signer or simulated by a set of designated verifiers. Recently, as an important application, MDVS is expected to be used in messaging applications [7].

Prior to MDVS, a (single) designated verifier signature scheme is proposed by Chaum [17], and by Jakobsson et al. [13]. Desmedt asks the question if we can construct MDVS at CRYPTO'03 ramp session. Then, Laguillaumie and Vergnaud [15] demonstrate the first construction of an MDVS scheme based on a ring signature scheme under the computational Diffie-Hellman assumption. Since then, several MDVS schemes have been proposed based on ring signature schemes [15, 16, 24, 26], and it is said that an MDVS scheme can be constructed from a ring signature scheme in general.

It seems that such a construction has been widely believed because MDVS has similar structures with ring signature. Roughly, a ring signature scheme is

an extension of a digital signature scheme which provides anonymity for signers, meaning that a verifier who receives a ring signature cannot decide which ring member created the signature. In other words, any ring member is able to create a valid ring signature. Therefore, intuitively, if we regard a ring as a set of a signer and designated verifiers, it seems that we can construct an MDVS scheme from a ring signature scheme.

However, to the best of our knowledge, it is still unclear if such a construction is possible, as the existing works do not provide formal discussion on it. That is, they only propose the constructions in natural language, and never show formal security proofs by providing a reduction from an MDVS scheme to a ring signature scheme. For instance, the previous work [15], which proposes an MDVS scheme from a ring signature scheme for the first time, only discusses security as follows: *"The unforgeability of MDVS is guaranteed by the unforgeability of the underlying ring signature scheme. The source hiding property comes naturally from the source hiding of the ring signature."*

To the best of our knowledge, it is Zhang et al. [26] who formalize the security definitions of MDVS for the first time (in 2012), whereas they do not formally demonstrate the reduction from an MDVS scheme to a ring signature scheme. We further mention the recent formalization by Damgård et al. [7], which considers simulation by a subset of designated verifiers and claims that consistency is one of the standard requirements for MDVS. Since the desirable security requirements for MDVS are formalized, we are now ready to demonstrate the reduction formally by following them.

1.1 Our Contribution

Somewhat surprisingly, we demonstrate that it is impossible to construct an MDVS scheme from a ring signature scheme in a black-box manner in the standard model (in other words, we prove that there is no generic construction of an MDVS scheme based on a ring signature scheme). This counterintuitive result stems from the difference between the definitions of the unforgeability of MDVS and ring signature: A designated verifier in an MDVS scheme can be corrupted in the experiment, whereas a ring member in a ring signature scheme cannot be. (For formal definitions, see Section 2.)

While the formal proof is provided in Section 3, we provide its overview here. We follow the meta-reduction paradigm [9] to show the impossibility on unforgeability. If we want to formally show that the MDVS construction is unforgeable, we should demonstrate a reduction algorithm R, who is given a PPT adversary $\mathcal{A}$ against the unforgeability of the MDVS scheme, then breaks the unforgeability of the underlying ring signature scheme. That is, R plays the unforgeability game of the ring signature scheme as an adversary, along with simulating the unforgeability game of the MDVS scheme between $\mathcal{A}$. In this reduction, R should deal with a query made by $\mathcal{A}$ that corrupts a designated verifier in the simulated game. If we regard a ring of the ring signature scheme as a set of a signer and designated verifiers of the MDVS scheme, R cannot forward the corruption query to the challenger of the unforgeability game of the ring signature scheme, as it

leads to corrupt a ring member. Therefore, R should answer the query without relying on the challenger. However, if this is possible, R is able to break the unforgeability of the ring signature scheme without $\mathcal{A}$, which contradicts the security of the ring signature scheme.

We emphasize that it is an important task to give a formal proof even on a seemingly trivial matter, because it might be a case that it could not be established. We believe that this work is a prime example.

1.2 Related Work

The seminal work by Impagliazzo and Rudich [12] demonstrates a separation between a key agreement and a one-way function. This line of research has been successful, and there are a lot of follow-up works [10, 19, 22, 23]. We emphasize that a black-box impossibility only denies a generic construction of a primitive based on another primitive. Thus, if we rely on a concrete assumption, e.g. the RSA assumption and the discrete logarithm assumption, we might be able to circumvent such an impossibility.

We note that in spite of our result, it is known that a single designated verifier signature scheme (DVS) is equivalent to a ring signature scheme where a ring consists of two members. More precisely, Brendel et al. [4] show the construction of DVS from ring signature, and Hashimoto et al. [11] prove the inverse direction. However, we claim that this fact does not contradict our result. This is because the designated verifier in a DVS is not allowed to be corrupted, because a single secret key of the designated verifier is sufficient for a simulator. In other words, it leads to an obvious attack against unforgeability of the MDVS scheme. Therefore, our observation does not work for DVS.

Several constructions of MDVS from primitives rather than ring signature have been proposed so far. Chow [6] demonstrates a construction from multi-chameleon hash, whereas he does not define MDVS formally. Further, Damgård et al. [7] propose two generic constructions of MDVS; one is from a pseudorandom function, a pseudorandom generator, a key agreement, and an NIZK; and the other is from a functional encryption.

We mention recent works related to MDVS. It is used as a building block for a multi-designated receiver signed public key encryption scheme [5, 20]. Further, a new (M)DVS, a designated verifier linkable ring signature scheme [1], has been proposed.

Finally, ring signature schemes with additional properties have been proposed so far, such as accountable ring signature [25], linkable ring signature [18], traceable ring signature [8], deniable ring signature [14], claimable ring signature and repudiable ring signature [21]. We might be able to circumvent the impossibility that is exposed by this work by using these ring signature schemes with additional properties. We leave it as an open problem.

2 Preliminaries

Throughout this paper, we let $\lambda \in \mathbb{N}$ be a security parameter. We abbreviate a probabilistic polynomial time algorithm as a PPT algorithm. We denote a polynomial function and a negligible function by $\mathsf{poly}(\cdot)$ and $\mathsf{negl}(\cdot)$, respectively. For any $n \in \mathbb{N}$, let $[n] \coloneqq \{1, 2, \cdots, n\}$. A subroutine X of an algorithm Π is denoted by $\Pi.X$. A security property is defined by a game (or an experiment) between a challenger and an adversary. If the result of the game is 1, we say that the adversary wins the game.

2.1 Multi-Designated Verifier Signature

In this section, we recall the definition of multi-designated verifier signature (MDVS). We follow the most standard definition of MDVS by [7] except that all designated verifiers are required to participate to simulate a signature[4], rather than the definition by Zhang et al. [26]. The work [7] claims that the basic security requirements for MDVS are unforgeability, OTR, and consistency. Namely, consistency is a property which guarantees that verification results are the same among designated verifiers, which is not required in [26].

Let $\mathcal{I}$ denote a set of users' identities and we use $\mathcal{I}$ in the definition of an MDVS scheme. The formal definition is as follows. [5]

Definition 1 (MDVS). *A multi-designated verifier signature scheme (MDVS) scheme consists of the following six algorithms* $(\mathsf{Set}, \mathsf{SKG}, \mathsf{VKG}, \mathsf{Sig}, \mathsf{Vrf}, \mathsf{Sim})$*:*

- $\mathsf{Set}(1^\lambda) \to (\mathsf{pp}, \mathsf{msk})$: *Given a security parameter* 1^λ*, it outputs a public parameter* pp *and a master secret key* msk*.*
- $\mathsf{SKG}(\mathsf{pp}, \mathsf{msk}, \mathsf{id}_\mathsf{S}) \to (\mathsf{spk}_{\mathsf{id}_\mathsf{S}}, \mathsf{ssk}_{\mathsf{id}_\mathsf{S}})$: *Given a public parameter* pp*, a master secret key* msk*, and an identity* $\mathsf{id}_\mathsf{S} \in \mathcal{I}$*, it outputs the signer's public key* $\mathsf{spk}_{\mathsf{id}_\mathsf{S}}$ *and secret key* $\mathsf{ssk}_{\mathsf{id}_\mathsf{S}}$*.*
- $\mathsf{VKG}(\mathsf{pp}, \mathsf{msk}, \mathsf{id}_\mathsf{V}) \to (\mathsf{vpk}_{\mathsf{id}_\mathsf{V}}, \mathsf{vsk}_{\mathsf{id}_\mathsf{V}})$: *Given a public parameter* pp*, a master secret key* msk*, and an identity* $\mathsf{id}_\mathsf{V} \in \mathcal{I}$*, it outputs the verifier's public key* $\mathsf{vpk}_{\mathsf{id}_\mathsf{V}}$ *and secret key* $\mathsf{vsk}_{\mathsf{id}_\mathsf{V}}$*.*
- $\mathsf{Sig}(\mathsf{pp}, \mathsf{ssk}_{\mathsf{id}_\mathsf{S}}, \{\mathsf{vpk}_{\mathsf{id}_\mathsf{V}}\}_{\mathsf{id}_\mathsf{V} \in \mathcal{D}}, \mathsf{m}) \to \sigma$: *Given a public parameter* pp*, a signer's secret key* $\mathsf{ssk}_{\mathsf{id}_\mathsf{S}}$*, a set of verifiers' public keys* $\{\mathsf{vpk}_{\mathsf{id}_\mathsf{V}}\}_{\mathsf{id}_\mathsf{V} \in \mathcal{D}}$ *of designated verifiers* $\mathcal{D}$*, and a message* $\mathsf{m} \in \mathcal{M}$*, it outputs a signature* σ*.*
- $\mathsf{Vrf}(\mathsf{pp}, \{\mathsf{vpk}_{\mathsf{id}_\mathsf{V}}\}_{\mathsf{id}_\mathsf{V} \in \mathcal{D}}, \mathsf{vsk}_{\mathsf{id}'_\mathsf{V}}, \mathsf{spk}_{\mathsf{id}_\mathsf{S}}, \mathsf{m}, \sigma) \to 1/0$: *Given a public parameter* pp*, a set of public keys* $\{\mathsf{vpk}_{\mathsf{id}_\mathsf{V}}\}_{\mathsf{id}_\mathsf{V} \in \mathcal{D}}$ *of designated verifiers* $\mathcal{D}$*, a verifier's secret key* $\mathsf{vsk}_{\mathsf{id}'_\mathsf{V}}$*, a signer's public key* $\mathsf{spk}_{\mathsf{id}_\mathsf{S}}$*, a message* m*, and a signature* σ*, it outputs* 1 *(meaning accept) or* 0 *(meaning reject).*

[4] Note that this setting is limited compared to one by [7] in the sense that their definition considers simulation by any subset of designated verifiers. However, we stress that adopting a weaker definition makes our result better since our goal is to show a black-box impossibility from a ring signature scheme to an MDVS scheme.

[5] Note that, using $\mathcal{I}$, we give each algorithm an identifier only to make a user explicit. That is, we do not consider so-called "identity-based" primitives (e.g., identity-based signature).

– $\mathsf{Sim}(\mathsf{pp}, \{\mathsf{vpk}_{\mathsf{id_V}}\}_{\mathsf{id_V}\in\mathcal{D}}, \{\mathsf{vsk}_{\mathsf{id_V}}\}_{\mathsf{id_V}\in\mathcal{D}}, \mathsf{spk}_{\mathsf{id_S}}, \mathsf{m}) \to \sigma$: *Given a public parameter* pp*, a set of public keys* $\{\mathsf{vpk}_{\mathsf{id_V}}\}_{\mathsf{id_V}\in\mathcal{D}}$ *of designated verifiers* $\mathcal{D}$*, a set of secret keys* $\{\mathsf{vsk}_{\mathsf{id_V}}\}_{\mathsf{id}\in\mathcal{D}}$ *of designated verifiers* $\mathcal{D}$*, a signer's public key* $\mathsf{spk}_{\mathsf{id_S}}$*, and a message* m*, it outputs a simulated signature* σ*.*

Definition 2 (Correctness). *An MDVS scheme* $\Pi = (\mathsf{Set}, \mathsf{SKG}, \mathsf{VKG}, \mathsf{Sig}, \mathsf{Vrf}, \mathsf{Sim})$ *satisfies correctness if for any security parameter* $\lambda \in \mathbb{N}$*, any* $(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Set}(1^\lambda)$*, any set of verifiers' identities* $\mathcal{D} \subseteq \mathcal{I}$*, any verifier's identity* $\mathsf{id}'_{\mathsf{V}} \in \mathcal{D}$*, any signer's identity* $\mathsf{id_S} \in \mathcal{I}$*, and any message* $\mathsf{m} \in \mathcal{M}$*, it holds that*

$$\mathsf{Vrf}(\mathsf{pp}, \{\mathsf{vpk}_{\mathsf{id_V}}\}_{\mathsf{id_V}\in\mathcal{D}}, \mathsf{vsk}_{\mathsf{id}'_{\mathsf{V}}}, \mathsf{spk}_{\mathsf{id_S}}, \mathsf{m}, \mathsf{Sig}(\mathsf{pp}, \mathsf{ssk}_{\mathsf{id_S}}, \{\mathsf{vpk}_{\mathsf{id_V}}\}_{\mathsf{id_V}\in\mathcal{D}}, \mathsf{m})) = 1,$$

where $(\mathsf{spk}_{\mathsf{id_S}}, \mathsf{ssk}_{\mathsf{id_S}}) \leftarrow \mathsf{SKG}(\mathsf{pp}, \mathsf{msk}, \mathsf{id_S})$ *and* $(\mathsf{vpk}_{\mathsf{id_V}}, \mathsf{vsk}_{\mathsf{id_V}}) \leftarrow \mathsf{VKG}(\mathsf{pp}, \mathsf{msk}, \mathsf{id_V})$ *for all* $\mathsf{id_V} \in \mathcal{D}$*.*

We require an MDVS scheme to satisfy unforgeability, consistency, and off-the-record (OTR) as security requirements, as discussed in [7]. However, since our paper uses only the definition of unforgeability, we here introduce only it formally. The formal definitions of consistency and OTR are provided in Appendix A.1 for completeness.

Definition 3 (EUF-CMA). *An MDVS scheme* $\Pi = (\mathsf{Set}, \mathsf{SKG}, \mathsf{VKG}, \mathsf{Sig}, \mathsf{Vrf}, \mathsf{Sim})$ *is existentially unforgeable under an adaptive chosen-message attack (EUF-CMA) if for any security parameter* $\lambda \in \mathbb{N}$*, and any PPT adversary* $\mathcal{A}$*, it holds that* $\Pr[\mathsf{ExpEUFDVS}_{\Pi,\mathcal{A}}(1^\lambda) = 1] \leq \mathsf{negl}(\lambda)$ *where* $\mathsf{ExpEUFDVS}$ *is defined as follows:*

$\mathsf{ExpEUFDVS}_{\Pi,\mathcal{A}}(1^\lambda)$

$L_{\mathsf{VPK}} \coloneqq \emptyset; L_{\mathsf{SPK}} \coloneqq \emptyset; L_{\mathsf{VSK}} \coloneqq \emptyset; L_{\mathsf{SSK}} \coloneqq \emptyset; L_{\mathsf{Sign}} \coloneqq \emptyset; L_{\mathsf{Vrf}} \coloneqq \emptyset;$
$(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Set}(1^\lambda);$
$(\mathsf{id}^*_{\mathsf{S}}, \mathcal{D}^*, \mathsf{m}^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{O_{SPK}},\mathsf{O_{SSK}},\mathsf{O_{VPK}},\mathsf{O_{VSK}},\mathsf{O_{Sig}},\mathsf{O_{Vrf}}}(\mathsf{pp})$:
output 1 if $(\exists \mathsf{id}'_{\mathsf{V}} \in \mathcal{D}^* \setminus L_{\mathsf{VSK}}$ s.t. $\mathsf{Vrf}(\mathsf{pp}, \{\mathsf{vpk}_{\mathsf{id_V}}\}_{\mathsf{id_V}\in\mathcal{D}}, \mathsf{vsk}_{\mathsf{id}'_{\mathsf{V}}}, \mathsf{spk}_{\mathsf{id}^*_{\mathsf{S}}}, m^*, \sigma^*) = 1)$
$\wedge (\mathsf{id}^*_{\mathsf{S}} \notin L_{\mathsf{SSK}}) \wedge ((\mathcal{D}^*, \mathsf{id}^*_{\mathsf{S}}, \mathsf{m}^*) \notin L_{\mathsf{Sign}})$
otherwise 0

where $\mathsf{O_{SPK}}, \mathsf{O_{SSK}}, \mathsf{O_{VPK}}, \mathsf{O_{VSK}}, \mathsf{O_{Sig}}$*, and* $\mathsf{O_{Vrf}}$ *work as follows:*

$\mathsf{O_{SPK}}$**:** *Given* $\mathsf{id_S} \in \mathcal{I}$*, if* $\mathsf{id_S}$ *has already been queried previously, then it picks* $(\mathsf{id_S}, \mathsf{spk}_{\mathsf{id_S}}, \mathsf{ssk}_{\mathsf{id_S}})$ *from* L_{SPK} *and returns* $\mathsf{spk}_{\mathsf{id_S}}$*. Otherwise, it computes* $(\mathsf{spk}_{\mathsf{id_S}}, \mathsf{ssk}_{\mathsf{id_S}}) \leftarrow \mathsf{SKG}(\mathsf{pp}, \mathsf{msk}, \mathsf{id_S})$*, returns* $\mathsf{spk}_{\mathsf{id_S}}$*, and updates* $L_{\mathsf{SPK}} \coloneqq L_{\mathsf{SPK}} \cup \{(\mathsf{id_S}, \mathsf{spk}_{\mathsf{id_S}}, \mathsf{ssk}_{\mathsf{id_S}})\}$*.*

$\mathsf{O_{SSK}}$**:** *Given* $\mathsf{id_S} \in \mathcal{I}$*, if* $(\mathsf{id_S}, \mathsf{spk}_{\mathsf{id_S}}, \mathsf{ssk}_{\mathsf{id_S}}) \in L_{\mathsf{SPK}}$*, then it returns* $\mathsf{ssk}_{\mathsf{id_S}}$*, and updates* $L_{\mathsf{SSK}} \coloneqq L_{\mathsf{SSK}} \cup \{\mathsf{id_S}\}$*. Otherwise, it calls* $\mathsf{O_{SPK}}(\mathsf{id_S})$ *to generate* $(\mathsf{spk}_{\mathsf{id_S}}, \mathsf{ssk}_{\mathsf{id_S}})$ *along with updating* $L_{\mathsf{SPK}} \coloneqq L_{\mathsf{SPK}} \cup \{(\mathsf{id_S}, \mathsf{spk}_{\mathsf{id_S}}, \mathsf{ssk}_{\mathsf{id_S}})\}$*, returns* $(\mathsf{spk}_{\mathsf{id_S}}, \mathsf{ssk}_{\mathsf{id_S}})$*, and updates* $L_{\mathsf{SSK}} \coloneqq L_{\mathsf{SSK}} \cup \{\mathsf{id_S}\}$*. Note that we regard the signer corresponding to* $\mathsf{id_S} \in L_{\mathsf{SSK}}$ *as a corrupted signer.*

$\mathsf{O}_{\mathsf{VPK}}$: *Given* $\mathsf{id}_{\mathsf{V}} \in \mathcal{I}$, *if* id_{V} *has already been queried previously, then it picks* $(\mathsf{id}_{\mathsf{V}}, \mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}, \mathsf{vsk}_{\mathsf{id}_{\mathsf{V}}})$ *from* L_{VPK} *and returns* $\mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}$. *Otherwise, it computes* $(\mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}, \mathsf{vsk}_{\mathsf{id}_{\mathsf{V}}}) \leftarrow \mathsf{VKG}(\mathsf{pp}, \mathsf{msk}, \mathsf{id}_{\mathsf{V}})$, *returns* $\mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}$, *and updates* $L_{\mathsf{VPK}} := L_{\mathsf{VPK}} \cup \{(\mathsf{id}_{\mathsf{V}}, \mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}, \mathsf{vsk}_{\mathsf{id}_{\mathsf{V}}})\}$.

$\mathsf{O}_{\mathsf{VSK}}$: *Given* $\mathsf{id}_{\mathsf{V}} \in \mathcal{I}$, *if* $(\mathsf{id}_{\mathsf{V}}, \mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}, \mathsf{vsk}_{\mathsf{id}_{\mathsf{V}}}) \in L_{\mathsf{VPK}}$, *then it returns* $\mathsf{vsk}_{\mathsf{id}_{\mathsf{V}}}$, *and updates* $L_{\mathsf{VSK}} := L_{\mathsf{VSK}} \cup \{\mathsf{id}_{\mathsf{V}}\}$. *Otherwise, it calls* $\mathsf{O}_{\mathsf{VPK}}(\mathsf{id}_{\mathsf{V}})$ *to generate* $(\mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}, \mathsf{vsk}_{\mathsf{id}_{\mathsf{V}}})$ *along with* $L_{\mathsf{VPK}} := L_{\mathsf{VPK}} \cup \{(\mathsf{id}_{\mathsf{V}}, \mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}, \mathsf{vsk}_{\mathsf{id}_{\mathsf{V}}})\}$, *returns* $(\mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}, \mathsf{vsk}_{\mathsf{id}_{\mathsf{V}}})$, *and updates* $L_{\mathsf{VSK}} := L_{\mathsf{VSK}} \cup \{\mathsf{id}_{\mathsf{V}}\}$. *Note that we regard the verifier corresponding to* $\mathsf{id}_{\mathsf{V}} \in L_{\mathsf{VSK}}$ *as a corrupted verifier.*

$\mathsf{O}_{\mathsf{Sig}}$: *Given* $\mathcal{D} \subseteq \mathcal{I}, \mathsf{id}_{\mathsf{S}} \in \mathcal{I}$, *and* $\mathsf{m} \in \mathcal{M}$, *it does the followings:*

- *If* $(\mathsf{id}_{\mathsf{S}}, \cdot, \cdot) \notin L_{\mathsf{SPK}}$, *then call* $\mathsf{O}_{\mathsf{SPK}}$ *on* id_{S} *to generate* $(\mathsf{spk}_{\mathsf{id}_{\mathsf{S}}}, \mathsf{ssk}_{\mathsf{id}_{\mathsf{S}}})$.
- *For all* $\mathsf{id}_{\mathsf{V}} \in \mathcal{D}$ *s.t.* $(\mathsf{id}_{\mathsf{V}}, \cdot, \cdot) \notin L_{\mathsf{VPK}}$, *call* $\mathsf{O}_{\mathsf{VPK}}$ *on* id_{V} *to generate* $(\mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}, \mathsf{vsk}_{\mathsf{id}_{\mathsf{V}}})$.
- *Return* $\sigma \leftarrow \mathsf{Sig}(\mathsf{pp}, \mathsf{ssk}_{\mathsf{id}_{\mathsf{S}}}, \{\mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}\}_{\mathsf{id}_{\mathsf{V}} \in \mathcal{D}}, \mathsf{m})$, *and update* $L_{\mathsf{Sign}} := L_{\mathsf{Sign}} \cup \{(\mathcal{D}, \mathsf{id}_{\mathsf{S}}, \mathsf{m})\}$.

$\mathsf{O}_{\mathsf{Vrf}}$: *Given* $\mathsf{id}'_{\mathsf{V}}, \mathsf{id}_{\mathsf{S}} \in \mathcal{I}, \mathsf{m} \in \mathcal{M}$, $\mathcal{D} \subseteq \mathcal{I}$ *where* $\mathsf{id}'_{\mathsf{V}} \in \mathcal{D}$, *and* σ, *it does the followings:*

- *If* $\mathsf{id}'_{\mathsf{V}} \notin \mathcal{D}$, *then return* 0.
- *If* $(\mathsf{id}_{\mathsf{S}}, \cdot, \cdot) \notin L_{\mathsf{SPK}}$, *then call* $\mathsf{O}_{\mathsf{SPK}}$ *on* id_{S} *to generate* $(\mathsf{spk}_{\mathsf{id}_{\mathsf{S}}}, \mathsf{ssk}_{\mathsf{id}_{\mathsf{S}}})$.
- *For all* $\mathsf{id}_{\mathsf{V}} \in \mathcal{D}$, *if* $(\mathsf{id}_{\mathsf{V}}, \cdot, \cdot) \notin L_{\mathsf{VPK}}$, *then call* $\mathsf{O}_{\mathsf{VPK}}$ *on* id_{V} *to generate* $(\mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}, \mathsf{vsk}_{\mathsf{id}_{\mathsf{V}}})$.
- *Return* $b = \mathsf{Vrf}(\mathsf{pp}, \{\mathsf{vpk}_{\mathsf{id}_{\mathsf{V}}}\}_{\mathsf{id}_{\mathsf{V}} \in \mathcal{D}}, \mathsf{vsk}_{\mathsf{id}'_{\mathsf{V}}}, \mathsf{spk}_{\mathsf{id}_{\mathsf{S}}}, \mathsf{m}, \sigma)$ *and update* $L_{\mathsf{Vrf}} := L_{\mathsf{Vrf}} \cup \{(\mathcal{D}, \mathsf{id}'_{\mathsf{V}}, \mathsf{id}_{\mathsf{S}}, \mathsf{m}, \sigma)\}$.

2.2 Ring Signature

In this section, we review the definition of ring signature. We follow the strongest definition by [2]. Namely, as security properties for ring signature, we require unforgeability w.r.t. insider corruptions and anonymity against full key exposure. We remark that this stronger definition makes our result better, as it means an MDVS scheme cannot be obtained from such a stronger ring signature scheme in a black-box manner.

Definition 4 (Ring Signature). *A ring signature scheme consists of four PPT algorithms* $(\mathsf{Set}, \mathsf{KG}, \mathsf{Sig}, \mathsf{Vrf})$ *that work as follows:*

- $\mathsf{Set}(1^\lambda) \to \mathsf{pp}$: *Given a security parameter* 1^λ, *it outputs a public parameter* pp.
- $\mathsf{KG}(\mathsf{pp}) \to (\mathsf{pk}, \mathsf{sk})$: *Given a public parameter* pp, *it outputs a public key* pk *and a secret key* sk.
- $\mathsf{Sig}(\mathsf{pp}, \mathsf{sk}, \{\mathsf{pk}_i\}_{i \in [n]}, \mathsf{m}) \to \sigma$: *Given a public parameter* pp, *a secret key* sk, *a set of public keys (or a ring)* $\{\mathsf{pk}_i\}_{i \in [n]}$ *where* $n = \mathsf{poly}(\lambda)$, *and a message* m, *it outputs a signature* σ. *If there is no* $i \in [n]$ *s.t.* $(\mathsf{pk}_i, \mathsf{sk}) \leftarrow \mathsf{Set}(\mathsf{pp})$, *then it returns* $\perp$.
- $\mathsf{Vrf}(\mathsf{pp}, \{\mathsf{pk}_i\}_{i \in [n]}, \mathsf{m}, \sigma) = 1/0$: *Given a public parameter* pp, *a set of public keys* $\{\mathsf{pk}_i\}_{i \in [n]}$ *where* $n = \mathsf{poly}(\lambda)$, *a message* m, *and a signature* σ, *it outputs* 1 *(meaning accept) or* 0 *(meaning reject).*

A ring signature scheme $(\mathsf{Set}, \mathsf{KG}, \mathsf{Sig}, \mathsf{Vrf})$ *satisfies correctness if for any security parameter* λ*, any* $\mathsf{pp} \leftarrow \mathsf{Set}(1^\lambda)$*, and any message* $\mathsf{m} \in \mathcal{M}$*, it holds that*

$$\mathsf{Vrf}(\mathsf{pp}, \{\mathsf{pk}_i\}_{i\in[n]}, \mathsf{m}, \mathsf{Sig}(\mathsf{pp}, \mathsf{sk}, \{\mathsf{pk}_i\}_{i\in[n]}, \mathsf{m})) = 1,$$

where for any $i \in [n]$*,* pk_i *is generated by* KG*, and in particular, there exists* $i \in [n]$ *s.t.* $(\mathsf{pk}_i, \mathsf{sk}) \leftarrow \mathsf{KG}(\mathsf{pp})$*.*

Next, we define the unforgeability w.r.t. insider corruption as follows. Similar to MDVS, Anonymity is provided in Appendix A.2, as it does not appear in our discussion.

Definition 5 (Unforgeability w.r.t. Insider Corruptions). *A ring signature scheme* $\Pi_{\mathrm{RS}} = (\mathsf{Set}, \mathsf{KG}, \mathsf{Sig}, \mathsf{Vrf})$ *satisfies unforgeability w.r.t. insider corruptions if for any security parameter* λ *and any PPT adversary* $\mathcal{A}$ *who is allowed to make at most* $q = \mathsf{poly}(\lambda)$ *queries to oracles,* $\Pr[\mathsf{ExpEUFRS}_{\Pi_{\mathrm{RS}},\mathcal{A}}(1^\lambda) = 1] \leq \mathsf{negl}(\lambda)$ *where the experiment* $\mathsf{ExpEUFRS}_{\Pi_{\mathrm{RS}},\mathcal{A}}(1^\lambda)$ *is defined as follows:*

$\mathsf{ExpEUFRS}_{\Pi_{\mathrm{RS}},\mathcal{A}}(1^\lambda)$

$L_{\mathsf{PK}} := \emptyset; L_{\mathsf{SK}} := \emptyset; L_{\mathsf{Sign}} := \emptyset; \mathsf{pp} \leftarrow \mathsf{Set}(1^\lambda);$
$(\{\mathsf{pk}_i^*\}_{i\in[n]}, \mathsf{m}^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{O}_{\mathsf{PK}},\mathsf{O}_{\mathsf{SK}},\mathsf{O}_{\mathsf{RSig}}}(\mathsf{pp})$:
Output 1 if $(\mathsf{Vrf}(\mathsf{pp}, \{\mathsf{pk}_i^*\}_{i\in[n]}, \mathsf{m}^*, \sigma^*) = 1) \wedge (\forall i \in [n], (\mathsf{pk}_i^*, \mathsf{sk}_i^*) \in L_{\mathsf{PK}})$
$\wedge(\forall i \in [n], (\mathsf{pk}_i^*, \mathsf{sk}_i^*) \notin L_{\mathsf{SK}}) \wedge (\forall j \in [n], (\mathsf{pk}_j^*, \{\mathsf{pk}_i^*\}_{i\in[n]\setminus\{j\}}, \mathsf{m}^*, \sigma^*) \notin L_{\mathsf{Sign}})$,
otherwise 0

where $n = \mathsf{poly}(\lambda)$ *s.t.* $n \leq q$*, and* $\mathsf{O}_{\mathsf{PK}}, \mathsf{O}_{\mathsf{SK}}$ *and* $\mathsf{O}_{\mathsf{RSig}}$ *work as follows:*

O_{PK}**:** *Given* pp*, it computes* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KG}(\mathsf{pp})$*, returns* pk*, and updates* $L_{\mathsf{PK}} := L_{\mathsf{PK}} \cup \{(\mathsf{pk}, \mathsf{sk})\}$*.*

O_{SK}**:** *Given* pk*, if* $(\mathsf{pk}, \mathsf{sk}) \in L_{\mathsf{PK}}$*, then it returns* sk*, and updates* $L_{\mathsf{SK}} := L_{\mathsf{SK}} \cup \{(\mathsf{pk}, \mathsf{sk})\}$*. Otherwise, it returns* $\perp$*. Note that we regard* L_{SK} *as a set of corrupted entities.*

$\mathsf{O}_{\mathsf{RSig}}$**:** *Given a signer's public key* pk*, a set of public keys* $\{\mathsf{pk}_i\}_{i\in[n']}$ *where* $n' = \mathsf{poly}(\lambda)$*, and a message* m*, it does the followings:*

- *If* $(\mathsf{pk}, \mathsf{sk}) \notin L_{\mathsf{PK}}$*, then returns* $\perp$*.*
- *If* $(\mathsf{pk}, \{\mathsf{pk}_i\}_{i\in[n']}, \mathsf{m}, \sigma) \in L_{\mathsf{Sign}}$*, then returns* σ*.*
- *Returns* $\sigma \leftarrow \mathsf{Sig}(\mathsf{pp}, \mathsf{sk}, \{\mathsf{pk}\} \cup \{\mathsf{pk}_i\}_{i\in[n']}, \mathsf{m})$ *and updates* $L_{\mathsf{Sign}} := L_{\mathsf{Sign}} \cup \{(\mathsf{pk}, \{\mathsf{pk}_i\}_{i\in[n']}, \mathsf{m}, \sigma)\}$*.*

In the following, for simplicity, we say that a ring signature scheme satisfies EUF-CMA security if it satisfies the above definition.

3 Main Result

Now we provide the black-box impossibility of an MDVS scheme from a ring signature scheme. Formally, we assume that EUF-CMA security of the MDVS scheme can be based on EUF-CMA security of the ring signature scheme, i.e.

there exists a PPT reduction algorithm R that reduces EUF-CMA security of the MDVS scheme to EUF-CMA security of the ring signature scheme. (We remark that all existing constructions follow this reduction.) Then, we demonstrate that such an R contradicts the security of the ring signature scheme.

Shortly, the impossibility stems from the difference between their EUF-CMA security notions. That is, in $\mathsf{ExpEUFRS}$ a public key in the challenge ring should not be corrupted, whereas in $\mathsf{ExpEUFDVS}$ a part of (but not all) designated verifiers can be corrupted. Recall that existing constructions of MDVSs from ring signature schemes regard a ring as a set of a signer and designated verifiers. Thus the difference between the two security definitions is problematic when we consider such a construction.

Despite the above intuitive discussion, we should consider the case that a ring and a set of a signer and designated verifiers are distinct. In other words, it might be the case that such a construction is possible. Thus, we should deal with this counterintuitive construction.

Before demonstrating the separation formally, we describe our idea below. We have to deal with the following two cases.

We first prove that if $\mathsf{R}^{\mathcal{A}}$ breaks EUF-CMA security of the underlying ring signature scheme with non-negligible probability, then $\mathcal{A}$ should request R to make a query that corrupts a public key in R^* that is output by $\mathsf{R}^{\mathcal{A}}$ in $\mathsf{ExpEUFRS}$. Intuitively, if this is not the case, we can break EUF-CMA security of the underlying ring signature scheme without corrupting the members in the ring at all, which contradicts the existence of the ring signature scheme.

Secondly, in the case of regarding a ring as a set of a signer and designated verifiers, we follow the meta reduction paradigm [9]: Let $\mathcal{A}$ be a PPT adversary that breaks EUF-CMA security of the MDVS scheme with non-negligible probability. Then, we assume that $\mathsf{R}^{\mathcal{A}}$ breaks EUF-CMA security of the ring signature scheme with non-negligible probability. If $\mathcal{A}$ wants to corrupt a designated verifier and makes a corruption query, R should simulate the answer by itself without accessing its corruption oracle, because corrupting a ring member immediately violates the winning condition in $\mathsf{ExpEUFRS}$. However, if such a simulation is possible, then R is able to break EUF-CMA security of the ring signature scheme without $\mathcal{A}$.

Theorem 1. *Let* $\Pi_{\mathrm{RS}} = (\mathsf{Set}, \mathsf{KG}, \mathsf{Sig}, \mathsf{Vrf})$ *be a ring signature scheme. There is no black-box construction* $\Pi_{\mathrm{MDVS}}^{\Pi_{\mathrm{RS}}} = (\mathsf{Set}, \mathsf{SKG}, \mathsf{VKG}, \mathsf{Sig}, \mathsf{Vrf}, \mathsf{Sim})$ *of an MDVS scheme based on* Π_{RS}*, whose EUF-CMA security is reduced to EUF-CMA security of* Π_{RS}*.*

Proof. Suppose that there exists a PPT adversary $\mathcal{A}$ that breaks the EUF-CMA security of $\Pi_{\mathrm{MDVS}}^{\Pi_{\mathrm{RS}}}$ with non-negligible probability, and let R be a PPT reduction algorithm from the EUF-CMA security of $\Pi_{\mathrm{MDVS}}^{\Pi_{\mathrm{RS}}}$ to the EUF-CMA security of Π_{RS}. In other words, $\mathsf{R}^{\mathcal{A}}$ breaks the EUF-CMA security of Π_{RS} with non-negligible probability. Note that $\mathsf{R}^{\mathcal{A}}$ plays the experiment $\mathsf{ExpEUFRS}_{\Pi_{\mathrm{RS}},\mathsf{R}^{\mathcal{A}}}(1^\lambda)$ as an adversary, while simulating the experiment $\mathsf{ExpEUFDVS}_{\Pi_{\mathrm{MDVS}},\mathcal{A}}(1^\lambda)$ to $\mathcal{A}$ as a challenger. We demonstrate that we can construct a PPT reduction algorithm

that is able to break EUF-CMA security of Π_{RS} with non-negligible probability. The algorithm $\mathsf{R}^{\mathcal{A}}$ works in $\mathsf{ExpEUFRS}_{\Pi_{\mathrm{RS}},\mathsf{R}^{\mathcal{A}}}(1^\lambda)$ as follows:

Setup Phase: The challenger computes a public parameter $\mathsf{pp}_{\mathsf{RS}} \leftarrow \Pi_{\mathrm{RS}}.\mathsf{Set}(1^\lambda)$ and gives it to R.

Challenge Phase: Given $\mathsf{pp}_{\mathsf{RS}}$, R computes $(\mathsf{pp}_{\mathsf{MDVS}}, \mathsf{msk}_{\mathsf{MDVS}})$ and gives $\mathsf{pp}_{\mathsf{MDVS}}$ to $\mathcal{A}$. In other words, R and $\mathcal{A}$ play $\mathsf{ExpEUFDVS}_{\Pi^{\Pi_{\mathrm{RS}}}_{\mathrm{MDVS}},\mathcal{A}}(1^\lambda)$. As already mentioned, R could ask the challenger of $\mathsf{ExpEUFRS}_{\Pi_{\mathrm{RS}},\mathsf{R}^{\mathcal{A}}}(\lambda)$ to call an oracle if necessary. When $\mathcal{A}$ outputs $(\mathsf{id}^*_{\mathsf{S}}, \mathcal{D}^*, \mathsf{m}^*_{\mathsf{MDVS}}, \sigma^*_{\mathsf{MDVS}})$, R returns $(R^*, \mathsf{m}^*_{\mathsf{RS}}, \sigma^*_{\mathsf{RS}})$ to the challenger, where $R^* = \{\mathsf{pk}^*_i\}_{i\in[n]}$ be a set of public keys (or a ring) and $n = \mathsf{poly}(\lambda)$.

Verification Phase: The adversary $\mathsf{R}^{\mathcal{A}}$ wins the game if all the following conditions are satisfied.

- $\Pi_{\mathrm{RS}}.\mathsf{Vrf}(\mathsf{pp}_{\mathsf{RS}}, R^*, \mathsf{m}^*_{\mathsf{RS}}, \sigma^*_{\mathsf{RS}}) = 1$.
- Every pk^*_i is created via the oracle O_{PK}.
- Every pk^*_i is not queried to O_{SK}.
- The signature σ^*_{RS} is not created via $\mathsf{O}_{\mathsf{RSig}}$ on $(\mathsf{pk}^*_j, R^*, \mathsf{m}^*_{\mathsf{RS}})$.

The third condition means that every public key in R^* should not be corrupted when $\mathsf{R}^{\mathcal{A}}$ wins the game. Let `CorMember` be an event that $\mathcal{A}$, during the execution of $\mathsf{R}^{\mathcal{A}}$, makes a query that results in the corruption of a public key in R^*.

We first argue in Claim 3 that if $\mathsf{R}^{\mathcal{A}}$ wins the game with non-negligible probability under the condition that `CorMember` does not occur, then Π_{RS} is not EUF-CMA secure. In the proof, we first show that $\mathcal{A}$ cannot make a query that necessitates R to call $\mathsf{O}_{\mathsf{RSig}}$ on $(\mathsf{pk}^*_j, R^*, \mathsf{m}^*_{\mathsf{RS}})$ where $\mathsf{pk}^*_j \in R^*$. Now, $\mathcal{A}$ does not ask R to make queries that result in the corruption of a public key in R^* or a signature with respect to R^*. In other words, $\mathsf{R}^{\mathcal{A}}$ is able to break EUF-CMA security of Π_{RS} by using only somewhat public information, i.e. corrupting public keys that are outside of R^* or obtaining signatures with respect to rings rather than R^*. However, if EUF-CMA security of Π_{RS} is compromised with non-negligible probability under such conditions, then there must be a PPT algorithm R' (without depending on $\mathcal{A}$) that breaks EUF-CMA security of Π_{RS} with non-negligible probability.

Further, we prove that, if $\mathsf{R}^{\mathcal{A}}$ wins the game under the condition that `CorMember` occurs, then we can use the power of R to break EUF-CMA security of Π_{RS}. Our idea is that if `CorMember` occurs, then R should answer it without asking the challenger to call O_{SK}, since otherwise the third winning condition is immediately violated. In other words, R is able to create a valid secret key (of a ring member) without relying on O_{SK}. Therefore, we can use such an R to break EUF-CMA security of Π_{RS}.

Claim. If $\mathsf{R}^{\mathcal{A}}$ breaks EUF-CMA security of Π_{RS} with non-negligible probability without `CorMember`, then there exists a PPT algorithm R', which does not rely on $\mathcal{A}$, that breaks EUF-CMA security of Π_{RS} with non-negligible probability.

Proof. Although we do not know how $\Pi_{\mathrm{MDVS}}^{\Pi_{\mathrm{RS}}}$ is constructed, we put very natural assumptions on it. Overall, a subroutine of Π_{RS} should be used in a "corresponding" subroutine in $\Pi_{\mathrm{MDVS}}^{\Pi_{\mathrm{RS}}}$. The public parameter $\mathsf{pp}_{\mathsf{MDVS}}$ is created based on $\mathsf{pp}_{\mathsf{RS}}$. To construct public keys $\mathsf{spk}_{\mathsf{id_s}}$ and $\mathsf{vpk}_{\mathsf{id_v}}$, public keys generated by O_{PK} should be used. Similarly, secret keys that are created by O_{PK} should be used to create secret keys $\mathsf{ssk}_{\mathsf{id_s}}$ and $\mathsf{vsk}_{\mathsf{id_v}}$. (We note that it might be the case that multiple underlying keys are used to construct a key of $\Pi_{\mathsf{MDVS}}^{\Pi_{\mathsf{RS}}}$. However, we do not discuss this point in detail, as we do not know how $\Pi_{\mathsf{MDVS}}^{\Pi_{\mathsf{RS}}}$ is constructed.) Further, during the creation of a signature by $\Pi_{\mathrm{MDVS}}^{\Pi_{\mathrm{RS}}}$, regardless of whether it is real or simulated, $\Pi_{\mathrm{RS}}.\mathsf{Sig}$ is used. Similary, $\Pi_{\mathrm{MDVS}}^{\Pi_{\mathrm{RS}}}.\mathsf{Vrf}$ uses $\Pi_{\mathrm{RS}}.\mathsf{Vrf}$.

While we are under the assumption that `CorMember` does not happen, it might be the case that $\mathsf{R}^{\mathcal{A}}$ forges a ring signature by using $\mathsf{O}_{\mathsf{RSig}}$. Here, we need to further consider two cases, i.e. if $\mathcal{A}$ asks R a query that necessitates the query $(\mathsf{pk}_j^*, R^*, \mathsf{m}_{\mathsf{RS}}^*)$ where $\mathsf{pk}_j^* \in R^*$ to $\mathsf{O}_{\mathsf{RSig}}$ (i.e. $\Pi_{\mathrm{RS}}.\mathsf{Sig}$) or not.

Firstly, suppose that $\mathcal{A}$ makes such a query. In this case, R cannot call $\mathsf{O}_{\mathsf{RSig}}$ on $(\mathsf{pk}_j^*, R^*, \mathsf{m}_{\mathsf{RS}}^*)$ as it immediately violates the winning condition of $\mathsf{ExpEUFRS}_{\Pi_{\mathrm{RS}},\mathsf{R}^{\mathcal{A}}}(1^\lambda)$. Therefore, R should somehow compute and return a valid signature to $\mathcal{A}$ by itself, which immediately violates the EUF-CMA security of Π_{RS}. Here, R might make a query to $\mathsf{O}_{\mathsf{RSig}}$ on another input, and return it to $\mathcal{A}$. However, if such a "substitutional" answer, say $\sigma^\dagger$, works well, then Π_{RS} is no longer EUF-CMA secure. That is, it does not change the view of $\mathcal{A}$ and thus it holds that $\Pi_{\mathrm{RS}}.\mathsf{Vrf}(\mathsf{pp}_{\mathsf{RS}}, R^*, \mathsf{m}^*, \sigma^\dagger) = 1$. However, it contradicts the EUF-CMA security of Π_{RS} if there exists a PPT algorithm that finds such a substitution with non-negligible probability. Furthermore, if R computes a substitutional answer without relying on $\mathsf{O}_{\mathsf{RSig}}$, such an R is able to break the EUF-CMA security of Π_{RS} without relying on $\mathcal{A}$, which also contradicts the security of Π_{RS}.

Secondly, we assume that $\mathcal{A}$ never makes a query that necessitates R the query $(\mathsf{pk}_j^*, R^*, \mathsf{m}_{\mathsf{RS}}^*)$ to $\mathsf{O}_{\mathsf{RSig}}$. Suppose that $\mathsf{R}^{\mathcal{A}}$ breaks EUF-CMA security of Π_{RS} with non-negligible probability under such conditions, i.e. `CorMember` does not happen and $\mathcal{A}$ never makes a query that necessitates R the query $(\mathsf{pk}_j^*, R^*, \mathsf{m}_{\mathsf{RS}}^*)$ to $\mathsf{O}_{\mathsf{RSig}}$. They guarantee that the winning conditions "every pk_i^* is not queried to O_{SK}" and "the signature σ_{RS}^* is not created via $\mathsf{O}_{\mathsf{RSig}}$ on $(\mathsf{pk}_j^*, R^*, \mathsf{m}_{\mathsf{RS}}^*)$" are satisfied. Further, by the assumption on the construction of Π_{MDVS}, the winning condition "every pk_i^* is created via the oracle O_{PK}" is satisfied. Therefore, $\mathsf{R}^{\mathcal{A}}$ creates a ring signature along with a message and a ring that passes the verification of $\Pi_{\mathsf{RS}}.\mathsf{Vrf}$ without making queries that would result in the violation of the winning conditions at all. However, it indicates the existence of a PPT algorithm R' that breaks EUF-CMA security of Π_{RS} with non-negligible probability. This contradicts the assumption that Π_{RS} is EUF-CMA secure.

Now, we consider the case where `CorMember` happens. We first observe what happens if `CorMember` occurs. When $\mathcal{A}$ makes a query that necessitates R to corrupt a public key pk_i^* in R^*, R cannot ask the challenger to call O_{SK} on pk_i^*, because it immediately violates the winning condition for $\mathsf{R}^{\mathcal{A}}$. Therefore, R somehow manages to create the corresponding secret key sk_i^* and returns it to

$\mathcal{A}$, without calling O_{SK}. We exploit this power and construct a PPT algorithm R' that breaks EUF-CMA security of Π_{RS}, without relying on $\mathcal{A}$, as follows.

- Given a public parameter $\mathsf{pp}_{\mathsf{RS}}$ from the challenger, R' creates $R^* = \{\mathsf{pk}_i^*\}_{i\in[n]}$ via calling O_{PK}, where $n = \mathsf{poly}(\lambda)$.
- For each $i \in [n]$, R' tries to create the secret key sk_i^* by exploiting the above mentioned capability. Once such a key is obtained, then R' moves to the next step.
- R' chooses a message m^*, and computes $\sigma^* \leftarrow \Pi_{\mathrm{RS}}.\mathsf{Sig}(\mathsf{pp}, \mathsf{sk}_i^*, R^*, \mathsf{m}^*)$ where sk_i^* is the secret key that is obtained in the previous step. Note that this computation is not recorded in L_{Sign}, as it is conducted locally by R'.
- R' returns $(R^*, \mathsf{m}^*, \sigma^*)$ to the challenger.

Observe that it holds that $\Pi_{\mathrm{RS}}.\mathsf{Vrf}(\mathsf{pp}, \{\mathsf{pk}_i^*\}_{i\in[n]}, \mathsf{m}^*, \sigma^*) = 1$ due to the correctness of Π_{RS} if sk_i^* is a valid secret key. Further, the remaining conditions for R' to win $\mathsf{ExpEUFRS}_{\Pi_{\mathrm{RS}},\mathsf{R}'}(\lambda)$ are satisfied, as every pk_i^* is created via O_{PK}, every pk_i^* is not corrupted by O_{SK}, and the signature σ^* is not created via $\mathsf{O}_{\mathsf{RSig}}$. As R' is able to create sk_i^* with non-negligible probability, R' wins $\mathsf{ExpEUFRS}_{\Pi_{\mathrm{RS}},\mathsf{R}'}(\lambda)$ with non-negligible probability, which contradicts the existence of Π_{RS}.

4 Conclusion

In this paper, we demonstrated that it is impossible to construct an MDVS scheme from a ring signature scheme in a black-box manner, whereas such a construction has been widely believed for a long time. It seems that such folklore has spread due to a lack of formal discussion. Therefore, we claim that having a formal discussion is important even on a seemingly trivial matter.

One of our future works is to consider the construction in the random oracle model, as we showed the impossibility only in the standard model. Further, we might be able to circumvent the impossibility if we consider stronger ring signature schemes.

acknowledgement

This research was in part conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)," which was supported by the Ministry of Internal Affairs and Communications, Japan. This research was also supported by Grant-in-Aid for Scientific Research (A) (JP23H00468).

References

1. Behrouz, P., Grontas, P., Konstantakatos, V., Pagourtzis, A., Spyrakou, M.: Designated-verifier linkable ring signatures. In: Park, J.H., Seo, S.H. (eds.) Information Security and Cryptology – ICISC 2021. pp. 51–70. Springer International Publishing, Cham (2022)

2. Bender, A., Katz, J., Morselli, R.: Ring signatures: Stronger definitions, and constructions without random oracles. In: Halevi, S., Rabin, T. (eds.) Theory of Cryptography. pp. 60–79. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
3. Borisov, N., Goldberg, I., Brewer, E.: Off-the-record communication, or, why not to use pgp. In: Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society. p. 77–84. WPES '04, Association for Computing Machinery, New York, NY, USA (2004)
4. Brendel, J., Fiedler, R., Günther, F., Janson, C., Stebila, D.: Post-quantum asynchronous deniable key exchange and the signal handshake. In: Hanaoka, G., Shikata, J., Watanabe, Y. (eds.) Public-Key Cryptography – PKC 2022. pp. 3–34. Springer International Publishing, Cham (2022)
5. Chakraborty, S., Hofheinz, D., Maurer, U., Rito, G.: Deniable authentication when signing keys leak. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 69–100. Springer Nature Switzerland, Cham (2023)
6. Chow, S.: Multi-designated verifiers signatures revisited. International Journal of Network Security **7** (01 2008)
7. Damgård, I., Haagh, H., Mercer, R., Nitulescu, A., Orlandi, C., Yakoubov, S.: Stronger security and constructions of multi-designated verifier signatures. In: Pass, R., Pietrzak, K. (eds.) Theory of Cryptography. pp. 229–260. Springer International Publishing, Cham (2020)
8. Fujisaki, E., Suzuki, K.: Traceable ring signature. In: Public Key Cryptography – PKC 2007. pp. 181–200 (2007)
9. Gennaro, R., Trevisan, L.: Lower bounds on the efficiency of generic cryptographic constructions. In: Proceedings of the 41st Annual Symposium on Foundations of Computer Science. p. 305. FOCS '00, IEEE Computer Society, USA (2000)
10. Gertner, Y., Kannan, S., Malkin, T., Reingold, O., Viswanathan, M.: The relationship between public key encryption and oblivious transfer. In: Proceedings 41st Annual Symposium on Foundations of Computer Science. pp. 325–335 (2000)
11. Hashimoto, K., Katsumata, S., Kwiatkowski, K., Prest, T.: An efficient and generic construction for signal's handshake (x3dh): Post-quantum, state leakage secure, and deniable. In: Garay, J.A. (ed.) Public-Key Cryptography – PKC 2021. pp. 410–440. Springer International Publishing, Cham (2021)
12. Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: Goldwasser, S. (ed.) Advances in Cryptology — CRYPTO' 88. pp. 8–26. Springer New York, New York, NY (1990)
13. Jakobsson, M., Sako, K., Impagliazzo, R.: Designated verifier proofs and their applications. In: Maurer, U. (ed.) Advances in Cryptology — EUROCRYPT '96. pp. 143–154. Springer Berlin Heidelberg, Berlin, Heidelberg (1996)
14. Komano, Y., Ohta, K., Shimbo, A., Kawamura, S.: Toward the fair anonymous signatures: Deniable ring signatures. In: Pointcheval, D. (ed.) Topics in Cryptology – CT-RSA 2006. pp. 174–191. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
15. Laguillaumie, F., Vergnaud, D.: Multi-designated verifiers signatures. In: Lopez, J., Qing, S., Okamoto, E. (eds.) Information and Communications Security. pp. 495–507. Springer Berlin Heidelberg, Berlin, Heidelberg (2004)
16. Laguillaumie, F., Vergnaud, D.: Multi-designated verifiers signatures: anonymity without encryption. Information Processing Letters **102**(2), 127–132 (2007)
17. Lee, B., Choo, K.K.R., Yang, J., Yoo, S.: Secret signatures: How to achieve business privacy efficiently? In: Kim, S., Yung, M., Lee, H.W. (eds.) Information Security Applications. pp. 30–47. Springer Berlin Heidelberg, Berlin, Heidelberg (2007)

18. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable spontaneous anonymous group signature for ad hoc groups. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) Information Security and Privacy. pp. 325–335. Springer Berlin Heidelberg, Berlin, Heidelberg (2004)
19. Mahmoody, M., Mohammed, A., Nematihaji, S.: On the impossibility of virtual black-box obfuscation in idealized models. In: Kushilevitz, E., Malkin, T. (eds.) Theory of Cryptography. pp. 18–48. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
20. Maurer, U., Portmann, C., Rito, G.: Multi-designated receiver signed public key encryption. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022. pp. 644–673. Springer International Publishing, Cham (2022)
21. Park, S., Sealfon, A.: It wasn't me! repudiability and unclaimability of ring signatures. In: Annual International Cryptology Conference. pp. 159–190. Springer (2019)
22. Pass, R.: Unprovable security of perfect nizk and non-interactive non-malleable commitments. In: Sahai, A. (ed.) Theory of Cryptography. pp. 334–354. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
23. Simon, D.R.: Finding collisions on a one-way street: Can secure hash functions be based on general assumptions? In: Nyberg, K. (ed.) Advances in Cryptology — EUROCRYPT'98. pp. 334–345. Springer Berlin Heidelberg, Berlin, Heidelberg (1998)
24. Vergnaud, D.: New extensions of pairing-based signatures into universal designated verifier signatures. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) Automata, Languages and Programming. pp. 58–69. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
25. Xu, S., Yung, M.: Accountable ring signatures: A smart card approach. In: Smart Card Research and Advanced Applications VI. pp. 271–286 (2004)
26. Zhang, Y., Au, M.H., Yang, G., Susilo, W.: (strong) multi-designated verifiers signatures secure against rogue key attack. In: Xu, L., Bertino, E., Mu, Y. (eds.) Network and System Security. pp. 334–347. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)

A Omitted Security Properties for MDVS and Ring Signature

A.1 Consistency and OTR for MDVS

In this section, we review the definition of consistency and OTR for MDVS. Regarding OTR, compared to the work in [7], we recall a weaker definition for OTR that a simulator requires all secret keys of designated verifiers for simplicity. In [7], they define "OTR for any subset," which means that a part of the secret keys of designated verifiers is sufficient for a simulator. We note that requiring a weaker OTR for MDVS makes our result better, as we want to show a black-box impossibility of an MDVS scheme from a ring signature scheme. That is, even such a weaker MDVS scheme cannot be obtained based on a ring signature scheme in a black-box manner.

Definition 6 (Consistency). *An MDVS scheme* $\Pi = (\mathsf{Set}, \mathsf{SKG}, \mathsf{VKG}, \mathsf{Sig}, \mathsf{Vrf}, \mathsf{Sim})$ *is consistent if for any security parameter* $\lambda \in \mathbb{N}$*, and a stateful PPT*

adversary $\mathcal{A}$, it holds that $\Pr[\mathsf{ExpConst}_{\Pi,\mathcal{A}} = 1] \leq \mathsf{negl}(\lambda)$ *where* $\mathsf{ExpConst}$ *is defined as follows:*

$\mathsf{ExpConst}_{\Pi,\mathcal{A}}(1^\lambda)$

$L_{\mathsf{VPK}} := \emptyset; L_{\mathsf{SPK}} := \emptyset; L_{\mathsf{VSK}} := \emptyset; L_{\mathsf{SSK}} := \emptyset; L_{\mathsf{Sign}} := \emptyset; L_{\mathsf{Vrf}} := \emptyset;$
$(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Set}(1^\lambda);$
$(\mathsf{id}^*_{\mathsf{S}}, \mathcal{D}^*, \mathsf{m}^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{O}_{\mathsf{SPK}},\mathsf{O}_{\mathsf{SSK}},\mathsf{O}_{\mathsf{VPK}},\mathsf{O}_{\mathsf{VSK}},\mathsf{O}_{\mathsf{Sig}},\mathsf{O}_{\mathsf{Vrf}}}(\mathsf{pp}, \mathsf{spk}_{\mathsf{id}_\mathsf{S}}, \mathsf{id}_\mathsf{S}) :$
Output 1 if $((\mathsf{spk}_{\mathsf{id}^*_\mathsf{S}}, \mathsf{ssk}_{\mathsf{id}^*_\mathsf{S}}) \in L_{\mathsf{SPK}}) \wedge (\forall \mathsf{id}_\mathsf{V} \in \mathcal{D}^*, (\mathsf{vpk}_{\mathsf{id}_\mathsf{V}}, \mathsf{vsk}_{\mathsf{id}_\mathsf{V}} \in L_{\mathsf{VPK}}))$
$\wedge(\exists \mathsf{id}_\mathsf{V}, \mathsf{id}'_\mathsf{V} \in \mathcal{D}^* \text{ s.t. } \mathsf{id}_\mathsf{V} \neq \mathsf{id}'_\mathsf{V} \wedge (\mathsf{vpk}_{\mathsf{id}_\mathsf{V}}, \mathsf{vsk}_{\mathsf{id}_\mathsf{V}}), (\mathsf{vpk}_{\mathsf{id}'_\mathsf{V}}, \mathsf{vsk}_{\mathsf{id}'_\mathsf{V}}) \notin L_{\mathsf{VSK}}$
$\wedge \mathsf{Vrf}(\mathsf{pp}, \{\mathsf{vpk}_{\mathsf{id}_\mathsf{V}}\}_{\mathsf{id}_\mathsf{V} \in \mathcal{D}^*}, \mathsf{vsk}_{\mathsf{id}_\mathsf{V}}, \mathsf{spk}_{\mathsf{id}^*_\mathsf{S}}, m^*, \sigma^*) = 1$
$\wedge \mathsf{Vrf}(\mathsf{pp}, \{\mathsf{vpk}_{\mathsf{id}_\mathsf{V}}\}_{\mathsf{id}_\mathsf{V} \in \mathcal{D}^*}, \mathsf{vsk}_{\mathsf{id}'_\mathsf{V}}, \mathsf{spk}_{\mathsf{id}^*_\mathsf{S}}, m^*, \sigma^*) = 0)$
otherwise 0

where $\mathsf{O}_{\mathsf{SPK}}, \mathsf{O}_{\mathsf{SSK}}, \mathsf{O}_{\mathsf{VPK}}, \mathsf{O}_{\mathsf{VSK}}, \mathsf{O}_{\mathsf{Sig}}$ *and,* $\mathsf{O}_{\mathsf{Vrf}}$ *are defines as in Definition 3.*

Definition 7 (OTR). *An MDVS scheme* $\Pi = (\mathsf{Set}, \mathsf{SKG}, \mathsf{VKG}, \mathsf{Sig}, \mathsf{Vrf}, \mathsf{Sim})$ *is off-the-record (OTR) if for any security parameter* $\lambda \in \mathbb{N}$*, and a stateful PPT adversary* $\mathcal{A}$*, it holds that* $\Pr[\mathsf{ExpOTR}_{\Pi,\mathcal{A}} = 1] \leq \mathsf{negl}(\lambda)$ *where* ExpOTR *is defined as follows:*

$\mathsf{ExpOTR}_{\Pi,\mathcal{A}}(1^\lambda)$

$L_{\mathsf{VPK}} := \emptyset; L_{\mathsf{SPK}} := \emptyset; L_{\mathsf{VSK}} := \emptyset; L_{\mathsf{SSK}} := \emptyset; L_{\mathsf{Sign}} := \emptyset; L_{\mathsf{Vrf}} := \emptyset;$
$(\mathsf{pp}, \mathsf{msk}) \leftarrow \mathsf{Set}(1^\lambda); (\mathsf{spk}_{\mathsf{id}_\mathsf{S}}, \mathsf{ssk}_{\mathsf{id}_\mathsf{S}}) \leftarrow \mathsf{SKG}(\mathsf{pp}, \mathsf{msk}, \mathsf{id}_\mathsf{S});$
$(\mathcal{D}^*, \mathsf{m}^*) \leftarrow \mathcal{A}^{\mathsf{O}_{\mathsf{SPK}},\mathsf{O}_{\mathsf{SSK}},\mathsf{O}_{\mathsf{VPK}},\mathsf{O}_{\mathsf{VSK}},\mathsf{O}_{\mathsf{Sig}},\mathsf{O}_{\mathsf{Vrf}}}(\mathsf{pp}, \mathsf{spk}_{\mathsf{id}_\mathsf{S}}, \mathsf{id}_\mathsf{S});$
$\sigma_0 \leftarrow \mathsf{Sig}(\mathsf{pp}, \mathsf{ssk}_{\mathsf{id}_\mathsf{S}}, \{\mathsf{vpk}_{\mathsf{id}}\}_{\mathsf{id} \in \mathcal{D}^*}, \mathsf{m}^*);$
$\sigma_1 \leftarrow \mathsf{Sim}(\mathsf{pp}, \{\mathsf{vpk}_{\mathsf{id}}\}_{\mathsf{id} \in \mathcal{D}^*}, \{\mathsf{vsk}_{\mathsf{id}}\}_{\mathsf{id} \in \mathcal{D}^*}, \mathsf{spk}_{\mathsf{id}_\mathsf{S}}, \mathsf{m}^*); b \leftarrow \{0,1\};$
$b' \leftarrow \mathcal{A}^{\mathsf{O}_{\mathsf{SPK}},\mathsf{O}_{\mathsf{SSK}},\mathsf{O}_{\mathsf{VPK}},\mathsf{O}_{\mathsf{VSK}},\mathsf{O}_{\mathsf{Sig}},\mathsf{O}_{\mathsf{Vrf}}}(\sigma_b) :$
Output 1
if $(b' = b) \wedge (\mathsf{id}_\mathsf{S} \notin L_{\mathsf{SSK}}) \wedge (\exists \mathsf{id}_\mathsf{V} \in \mathcal{D}^* \text{ s.t. } \mathsf{id}_\mathsf{V} \notin L_{\mathsf{VSK}}) \wedge ((\cdot,\cdot,\cdot,\cdot,\sigma_b) \notin L_{\mathsf{Vrf}})$
otherwise 0

where $\mathsf{O}_{\mathsf{SPK}}, \mathsf{O}_{\mathsf{SSK}}, \mathsf{O}_{\mathsf{VPK}}, \mathsf{O}_{\mathsf{VSK}}, \mathsf{O}_{\mathsf{Sig}}$*, and* $\mathsf{O}_{\mathsf{Vrf}}$ *are defines as in Definition 3.*

A.2 Anonymity for Ring Signature

Here, we recall the definition of anonymity against full key exposure of a ring signature scheme as follows.

Definition 8 (Anonymity). *A ring signature scheme* $\Pi_{\mathrm{RS}} = (\mathsf{Set}, \mathsf{KG}, \mathsf{Sig}, \mathsf{Vrf})$ *satisfies anonymity if for any security parameter* λ*, and any PPT adversary* $\mathcal{A}$ *who is allowed to make at most* q *queries to oracles,* $|\Pr[\mathsf{ExpAno}_{\Pi_{\mathrm{RS}},\mathcal{A}}(1^\lambda) = 1] - 1/2| \leq \mathsf{negl}(\lambda)$*, where* $\mathsf{ExpAno}_{\Pi_{\mathrm{RS}},\mathcal{A}}(1^\lambda)$ *is defined as follows:*

$\mathsf{ExpAno}_{\Pi_{\mathrm{RS}},\mathcal{A}}(1^\lambda)$

$L_{\mathsf{PK}} := \emptyset; L_{\mathsf{SK}} := \emptyset; L_{\mathsf{Sign}} := \emptyset; \mathsf{pp} \leftarrow \mathsf{Set}(1^\lambda);$
$(\mathsf{m}^*, \mathsf{pk}_0, \mathsf{pk}_1, \{\mathsf{pk}^*_i\}_{i \in [n]}) \leftarrow \mathcal{A}^{\mathsf{O}_{\mathsf{PK}},\mathsf{O}_{\mathsf{SK}},\mathsf{O}_{\mathsf{RSig}}}(\mathsf{pp});$
output $\perp$ if $(\mathsf{pk}_0, \mathsf{sk}_0), (\mathsf{pk}_1, \mathsf{sk}_1) \notin L_{\mathsf{PK}};$
$b \leftarrow \{0,1\}; \sigma_b \leftarrow \mathsf{Sig}(\mathsf{pp}, \mathsf{sk}_b, \{\mathsf{pk}_0, \mathsf{pk}_1\} \cup \{\mathsf{pk}^*_i\}_{i \in [n]}, \mathsf{m}^*);$
$b' \leftarrow \mathcal{A}^{\mathsf{O}_{\mathsf{PK}},\mathsf{O}_{\mathsf{SK}},\mathsf{O}_{\mathsf{RSig}}}(\sigma_b) :$
output 1 if $b' = b$, otherwise 0.

where $n = \mathsf{poly}(\lambda)$ *s.t.* $n \leq q$*, and the oracles* O_{SK} *and* $\mathsf{O}_{\mathsf{RSig}}$ *are defined as in Definition 5.*