On the Anonymity of Linkable Ring Signatures[⋆]

Xavier Bultel[1][0000−0002−8309−8984] and Charles Olivier-Anclin[1,2,3][0000−0002−9365−3259]

[1] LIFO, Université d'Orléans, INSA Centre Val de Loire, Inria, France
[2] LIMOS, Université Clermont Auvergne, CNRS, France
[3] be ys Pay

Abstract. Security models provide a way of formalising security properties in a rigorous way, but it is sometimes difficult to ensure that the model really fits the concept that we are trying to formalise. In this paper, we illustrate this fact by showing the discrepancies between the security model of anonymity of linkable ring signatures and the security that is actually expected for this kind of signature. These signatures allow a user to sign anonymously within an ad hoc group generated from the public keys of the group members, but all their signatures can be linked together. Reading the related literature, it seems obvious that users' identities must remain hidden even when their signatures are linked, but we show that, surprisingly, almost none have adopted a security model that guarantees it. We illustrate this by presenting two counter-examples which are secure in most anonymity model of linkable ring signatures, but which trivially leak a signer's identity after only two signatures.

A natural fix to this model, already introduced in some previous work, is proposed in a corruption model where the attacker can generate the keys of certain users themselves, which seems much more coherent in a context where the group of users can be constructed in an ad hoc way at the time of signing. We believe that these two changes make the security model more realistic. Indeed, within the framework of this model, our counter-examples becomes insecure. Furthermore, we show that most of the schemes in the literature we surveyed appear to have been designed to achieve the security guaranteed by the latest model, which reinforces the idea that the model is closer to the informal intuition of what anonymity should be in linkable ring signatures.

1 Introduction

Ring signatures [33], digital signatures on behalf of *ad hoc* groups hiding which of the entities created them, are amongst the most studied privacy-preserving signatures. Over the years, they have been used in many real-world applications, making them one, if not the most widely deployed type of privacy-preserving signatures. Their applications are numerous and include blockchains (Monero, based on CryptoNote [38]), electronic voting [35], attestation [35], *etc.* These applications regularly require a mitigation of the powerful property of anonymity brought by the original concept.

Anonymity Mitigation. To adapt to its use cases, variations of the original concept have been developed to mitigate its full anonymity. These mitigations, introduced as new properties, are, amongst others, *traceability* of the signer if it produces more than one signature [23], *repudiation* of the signature for non-signers or *claimability* for signers [31] and *revocability* of the signer's anonymity by a revocation authority [42]. We focus on yet another property: *linkability* of the signature produced by the same signer, and its implications on anonymity. Introduced by Liu *et al.* [27], linkable ring signatures (LRS) have been the subject of many research papers and allows any verifier to link signatures produced by the same signer while concealing the signer's identity under the names of the ring members. A list of existing works is provided in Table 1. We give an example to illustrate its application and functionality: consider the certification of ballot in an election. Here, each voter signs its ballot paper not only under its identity but also under the identities of all the voters, which allows him to sign its ballot paper without disclosing its identity. This is done by generating a ring signature. In this case, linkable ring signatures would allow an auditor to link the signatures of two

[⋆] This is paper appeared in the proceedings of CANS 2024.
Author contracts Xavier Bultel: xavier.bultel@insa-cvl.fr, Charles Olivier-Anclin charlesolivier@outlook.fr.

electronic ballots from the same entity. This prevents voters from voting multiple times without manipulating the identity of voters, and allows voting to be modified during the elections (as in the Estonian electronic voting system [37]).

In the definition of linkable ring signatures, just like ring signatures, include a key generation algorithm, a signature algorithm, and a verification algorithm. Unlike traditional ring signatures, they allow for the verification of whether two signatures were produced by the same signer based on a linking algorithm, while still concealing the signer's identity. This preservation of privacy for the signer is often referred to as *pseudonymity*, *partial anonymity*, or *anonymity.* In the existing literature, the term *anonymity* has been preferred, but we highlight that for linkable ring signatures it represents a weaker property than when applied to ring signatures.

Security Considerations. Four security properties have been defined to model what is expected from linkable ring signatures:

Unforgeability of signatures: it is computationally unfeasible for anyone who is not part of the ring to produce a valid signature that would be accepted as legitimate.

Anonymity of signer: given a signature, it is unfeasible to determine which member signed.

Linkability of signatures: it is unfeasible to generate two unlinked signatures from the same key.

Non-slanderability of signatures: it is unfeasible to create a situation where a valid signature is falsely claimed to be generated by another member of the ring.

Of these properties, *unforgeability* and *anonymity* are derived from the properties of ring signatures, while the other two are necessary to guarantee the security of the linkability property. Although supposedly adapted from ring signatures, the level of anonymity formalised by most previous works, even the most recent ones, is insufficient. In fact, the associated constructions could suffer from a total lack of anonymity. What is more, the environments in which they could suffer concrete breaches in the anonymity of entities. In recent works such as [9] and the other schemes of Table 1 (except for [1]), *Anonymity* (ano) is informally characterised by the following statement:

> *"Anonymity, demands that an adversary cannot tell which of a ring's secret keys was used to produce a signature."*

Despite the accurate informal descriptions, we show that the definitions for all schemes listed in Table 1a essentially formalise this same concept as follows ([1] in Table 1b does it purposely):

> *Anonymity demands that an adversary cannot tell which of a ring's secret keys was used to produce* ***an entity's first signature****.*

We see a direct implication of the second statement by the first one. Throughout this paper, we refer to the second quote and weaker notion as *One-time Anonymity* (1-ano).

And, while it may be a feature of some schemes, as in [35], which main caracteristics are described in Table 1b, this statement does not model the actual expectation formulated for linkable ring signatures in the literature. Figure 1 shows a schematic comparison of the experiment of anonymity of ring signatures and the most frequently used one-time anonymity (1-ano) of linkable ring signatures. In Figure 1b, the one depicting the anonymity of linkable ring signatures, there is no guarantee regarding what the second signature might reveal about the identity of the signer, as we elucidate below. This is why we refer to this definitions of anonymity as *one-time anonymity* in order to better reflect the actual guarantees provided by the formalisation of this property. In looking for the rationale behind such a definition, one might speculate that it is linked to a statement made in Bender *et al.*'s seminal paper [7], whose provided a security framework for ring signatures. The statement in question is as follows:

[4] DL: Discrete logarithm; DDH: Differential Diffie Hellman, distinguishing between (g^x, g^y, g^{xy}) and (g^x, g^x, g^z) for some generator g and random values $x, y, z \in \mathbb{Z}_p^*$.

[5] ROM, which stands for *Random Oracle Model*

[6] CDL: Central Decoding Problem

[7] GSD: General Syndrome Decoding

Reference	Assumption	Model
Liu *et al.* [27]	DL[4] related	ROM[5]
Tsang *et al.* [36]	Strong RSA & DDH[1]	ROM
Liu and Wong [28]	DL related	ROM
Tsang and Wei [35]	DL related	ROM
Liu *et al.* [26]	DL related	ROM
Yuen *et al.* [40]	DL related	Standard
Boyen and Haines [11]	CDL[6]	ROM
Branco and Mateus [12]	GSDD[7]	ROM
Baum *et al.* [5]	SIS, LWE	ROM
Lu *et al.* [30]	SIS	ROM
Liu *et al.* [29]	M-SIS, D-MLWE	ROM
Zhang *et al.* [42]	DL related	ROM
Balla *et al.* [4]	DL related	ROM
Bootle *et al.* [9]	DL related	ROM
Xiangyu *et al.* [25]	DL related	ROM
Xue *et al.* [39]	Generic construction	ROM

(a) Existing Linkable Ring Signatures Proven Secure with Proven One-time Anonymity 1-ano.

Reference	Assumption	Model
Alberto *et al.* [1]	R-SIS	ROM

(b) Existing One-time Linkable Ring Signatures.

Reference	Assumption	Model
Backes *et al.* [3]	Generic construction	Standard
Beullens *et al.* [8]	SIDH, M-LWE	ROM

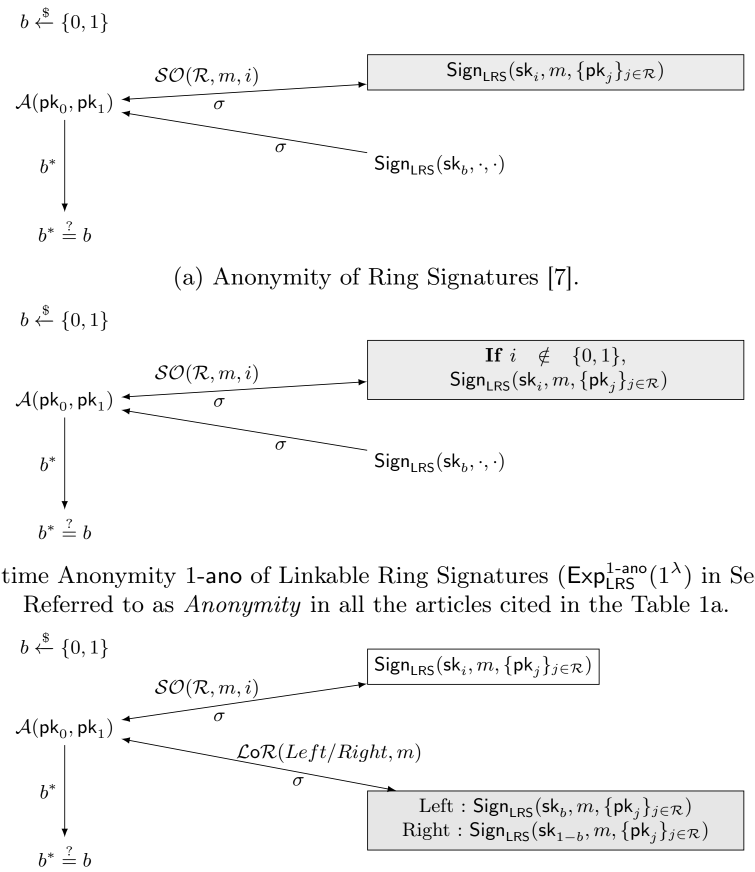
(c) Existing Linkable Ring Signatures with Proven Anonymity ano.

Table 1: Existing Linkable Ring Signatures.

> "*a weaker definition of anonymity* (one-time anonymity of Figure 1b) *whereby the adversary obtains only users' public keys and a single signature – but cannot obtain multiple other signatures via a signing oracle – does not imply unlinkability [of the signatures produced by the same signer]*" .

At first glance, removing the right to obtain multiple signatures in the experiment may seem like a reasonable way of defining anonymity with linkability. However, upon closer examination, this statement actually discusses the fact that unlinkability is not considered when only one signature is issued to the adversary. Therefore, all we can ascertain about the definition of anonymity is that this weak definition of one-time anonymity 1-ano appeared in the very first articles on linkable ring signatures and has persisted across most existing schemes (of Table 1a). Only two existing works [3,8], reported in Table 1c have formalised the anonymity of LRS with a more realistic experiment, schematically described in Figure 1c using a *Left or Right* challenge oracle. However, their model is left unconsidered in all subsequent works reported in Table 1a.

Our Contributions. We argue that the modelisation of the anonymity experiment for linkable ring signatures in all the schemes listed in Table 1a does not match the security expectations formalised in their respective works. This discrepancy means that 16 of the 18 existing linkable ring signatures may suffer from a deep lack of protection of the signer's identity after only the second signature. The most commonly used security model for linkable ring signatures, which we have referred to as one-time anonymity (1-ano) (above and in Figure 1b), remains broadly similar across all the works listed in Table 1a. The one-time anonymity


$b \xleftarrow{\$} \{0,1\}$
$\mathcal{SO}(\mathcal{R}, m, i)$
σ
$\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$
$\mathcal{A}(\mathsf{pk}_0, \mathsf{pk}_1)$
σ
$\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_b, \cdot, \cdot)$
b^*
$b^* \overset{?}{=} b$
$b \xleftarrow{\$} \{0,1\}$
$\mathcal{SO}(\mathcal{R}, m, i)$
σ
If $i \notin \{0,1\}$,
$\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$
$\mathcal{A}(\mathsf{pk}_0, \mathsf{pk}_1)$
σ
$\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_b, \cdot, \cdot)$
b^*
$b^* \overset{?}{=} b$
$b \xleftarrow{\$} \{0,1\}$
$\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$
$\mathcal{SO}(\mathcal{R}, m, i)$
σ
$\mathcal{A}(\mathsf{pk}_0, \mathsf{pk}_1)$
$\mathcal{L}o\mathcal{R}(Left/Right, m)$
σ
b^*
Left : $\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_b, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$
Right : $\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_{1-b}, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$
$b^* \overset{?}{=} b$

(a) Anonymity of Ring Signatures [7].

(b) One-time Anonymity 1-ano of Linkable Ring Signatures ($\mathsf{Exp}^{\mathsf{1\text{-}ano}}_{\mathsf{LRS}}(1^\lambda)$ in Section 2). Referred to as *Anonymity* in all the articles cited in the Table 1a.

(c) Anonymity ano of Linkable Ring Signatures ($\mathsf{Exp}^{\mathsf{ano}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ in Section 4 or A).

Fig. 1: Schematic Comparison of Anonymity Experiments for Ring and Linkable Ring Signatures. (Corruption models are not specified.)

experiment only hides the identity of the signer when they first sign, not necessarily on the second signature. This does not match the informal expectations described in all these works. Our main contribution is to highlight the absence of an appropriate formalism for anonymity, even in some of the most recent research.

Another model exists in the literature and has only been used for the schemes presented in Table 1c. This model takes better account of the anonymity expected from linkable ring signatures. It is based on an oracle and we called it anonymity (ano) as illustrated in Figure 1c. We recall it in Section 4 and show, by our upcoming counter-examples, that it is strictly stronger than 1-ano.

Linkable ring signatures admit two corruption models:

The Honest Key model: a scenario where all signature keys must have been generated honestly by the challenger in the experiment.

The Adversarially-chosen Keys Model: a scenario where signature keys may have been generated maliciously by the adversary.

After introducing both 1-ano and ano in each of the models, we can formulate a first counter-example, showing what we claimed above: in the one-time anonymity experiment 1-ano, there exist schemes revealing the identity of the signer on the second signature. We also propose a second counter-example based on existing literature [13]. These counter-examples are realised by proposing two constructions that could have been considered as "secure linkable ring signatures", in Section 5. We therefore argue for the stronger notions of anonymity ano. We discuss the insecurity of our counter-examples under this stronger model with ano-anonymity in Section 6. Next, we review all existing works citied in the Table 1a and initially based on the weaker notion of one-time anonymity 1-ano in Section 7. With this, we rule out a general lack of anonymity in existing constructions. By studying the proofs of existing schemes, we observed that many of them follow a similar proof pattern that can be extended by simple hybrid arguments. These results are summarised in Table 1.

Our final contribution is a complete classification of anonymity properties in the two corruption models for linkable ring signatures. For this, a second counter-example is needed to demonstrate the strict difference between the two corruption models. We construct it on the basis of an IND-CPA encryption scheme and any of the linkable ring signature scheme of the literature.

Related Work. Since 2004, numerous works have focused on linkable ring signature. In Table 1 we provide an exhaustive description of the existing linkable ring signatures in the literature, at the time of writing, while omitting signatures that have been attacked and thus provide insufficient security. These primitives claim either computational or unconditional anonymity. Most rely on discrete logarithm related assumptions, though few are based on lattice based assumptions [1,5,29,8] and could achieve some post-quantum security. Some of these schemes achieve additional properties, such as *threshold* [36] or *forward-security* [11]. Alberto *et al.* [1] proposed the only existing one-time linkable ring signature. However, their definition of anonymity is in fact the same as that of most linkable ring signatures. This should have given rise to concern.

All the signatures highlighted in the Table 1 are based on security models adapted for individual purposes. However, these models consistently encompass a weak formalisation of the anonymity experiment, with only two works standing out with a definition that is consistent with informal descriptions [3,8]. Similar realistic models have also been provided by Branco and Mateus [12] for *Same Ring Linkable Ring signature* and by Aranha *et al.* for *Same Message Linkable Ring Signature* [2]. Their signatures allow more anonymity than generally considered for linkable ring signature schemes, as it limits the possibility of linking signatures in scenarios in which two signatures were generated, respectively, for the same ring or the same message. Fujisaki and Suzuki introduced a security model for *Traceable Ring signatures* [23] that extends and is stronger than those considered for linkable ring signatures. Indeed, their model is similar to what was later proposed in [3] for linkable ring signatures, however, it includes additional failure conditions to prevent the adversary from trivially tracing the signer behind the challenges. All these related primitives are not strictly linkable ring signatures and their authors have not directly provided a model adapted to linkable ring signatures. Nonetheless the general idea behind their formalism is more accurate. In order to focus only on the existing model for linkable ring signatures, we leave aside their formalism and concentrate only on the definitions that aim to formalise the security of linkable ring signatures.

Other linkable signatures have been proposed, which are based on two types of privacy preserving signatures:

Group Signatures: such as *linkable group signatures* [41], from which LRS originate. They are its centralised version where an authority is responsible for managing the group. There also exist weaker linkability properties, for example *selective linkability* [24,22] which means that all signatures are unlinkable per default and only when needed, a set of signatures can be linked through the central authority. Unlike the case of ring signatures, it is possible (to use hybrid arguments in order) to show that providing one or more signatures to the adversary leads to the same property of anonymity, as the adversary has the secret signature keys of all the members of the group [6]. Their decentralised equivalent also exists [21] and their anonymity is formalised in a realistic way. Diaz and Lehmann [17] also introduced a *user-controlled Linkable Group Signature* for which signers can provide proof of links between their signatures. With such a property, the model differs from linkable group or ring signatures as the proof of a link must be produced by the signers before a connection can be established by a verifier, and is therefore not de facto accessible. The same weakness has not passed on to their security model.

Group and Ring signatures with User-controlled Linkability: A signer of a user-controled linkable signature scheme can produce a linking witness for any of its signatures. This type of linkability was introduced by Diaz and Lehmann [17] for group signatures and later extended to ring signatures by

Fiore *et al.* [21]. In the definitions, signatures are accompanied by a pseudonym within an event scope. Re-using the same scope leads to the same pseudonym allowing linking of signatures by the verifier. Signers can also provide explicit linking between signatures with different pseudonyms, hence allowing more linking that originally intended. In both works, the security provided by their experiment for the anonymity of the signer is analogous to the definition of anonymity ano, our arguments do not apply as they use strong anonymity notions, their schemes are not vulnerable to the exposed incorrect formulation of the anonymity experiment.

Attribute-based Signatures: *Attribute-based Signatures* [18,19] are a type of cryptographic signatures for which the signing capability is determined by the possession of certain attributes, rather than depending on the signer's public keys. This method enables the signer to demonstrate that they possess specific attributes. Attribute-based Signatures have also been proposed with user-controlled linkability. The same observation can be made as for user-controled linkable group signature. We found no weaknesses in the formalisation of anonymity in existing definitions of attribute-based signatures.

Outline. We start by presenting the most commonly used model of linkable ring signature in Section 2, thus formalising one-time anonymity $1\text{-}\mathsf{ano}$ in both corruption models. We provide an alternative model, derived from the model of Backes *et al.* [3] for anonymity $1\text{-}\mathsf{ano}$ in Section A in the *honest key* corruption model and present the model of Backes *et al.* [3] in a stronger model in Section 4. In Section 5, we show that the models of Section 2 are too weak to model what is expected from a linkable ring signature. In Section 6, we review our counter-examples and shown them unsecure in the stronger models of Section A and 4. Subsequently, we review all linkable ring signature schemes to determine whether they can satisfy the stronger security requirements of Section 4, in Section 7. Last, in Section 8, and before concluding in Section 9, we provide the full relation diragram between the two anonymity properties ($1\text{-}\mathsf{ano}$ and ano) in the two corruption models.

2 Review of Linkable Ring Signatures Definitions

Definitions of *linkable ring signatures* vary across the literature (see references given in Table 1). Despite that, the prescribed algorithms have been defined in the same way in almost all presented works. This is not always the case for their associated security definitions, even if they remain relatively similar.

Definition 1 (Linkable Ring Signature - LRS). *A* Linkable Ring Signature *scheme is composed of five algorithms defined as follows:*

$\mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$**:** *is a* PPT *algorithm that takes the security parameter* λ *and produces the* public parameters p*.*

We assume these parameters p *as common inputs to all the upcoming algorithms.*

$\mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$**:** *is a* PPT *algorithm that takes the security parameter* λ*, and it returns a pair of keys* $(\mathsf{pk}, \mathsf{sk})$*.*

$\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$**:** *is a* PPT *algorithm that takes a* public key set $\{\mathsf{pk}_i\}_{i\in\mathcal{R}}$ *for a ring set* $\mathcal{R}$*, a signer secret key* sk_i *(with* $i \in \mathcal{R}$*) and a message* m*. It returns a ring signature* σ*.*

$\mathsf{Verif}_{\mathsf{LRS}}(m, \sigma, \{\mathsf{pk}_i\}_{i\in\mathcal{R}})$**:** *is a deterministic polynomial-time algorithm that takes a public key set* $\{\mathsf{pk}_i\}_{i\in\mathcal{R}}$*, a signature* σ*, and a message* m*. If the signature* σ *is valid, then it returns 1, otherwise, it returns 0.*

$\mathsf{Link}_{\mathsf{LRS}}(\sigma, \sigma')$**:** *is a deterministic polynomial-time algorithm that takes two signatures* σ *and* σ'*, it returns 1 if they are linked, otherwise, it returns 0.*

A linkable ring signature must guarantee Correctness*,* Unforgeability*,* One-time Anonymity*,* Linkability *and* Non-slanderability *as defined below.*

Correctness. Honestly generated signatures on any message m should verify the equation:

$$\forall\lambda, \forall\mathcal{R} \subset \mathbb{N}, \forall i \in \mathcal{R}, \forall\mathsf{p} \in [\mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)], \forall(\mathsf{pk}_j, \mathsf{sk}_j)_{j\in\mathcal{R}} \in [\mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)]^{|\mathcal{R}|},$$
$$\forall\sigma \in [\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})], \mathsf{Verif}_{\mathsf{LRS}}(m, \sigma, \{\mathsf{pk}_j\}_{j\in\mathcal{R}}) = 1.$$

As discussed in depth in [7], the corruption model of RS, in particular the anonymity of the signer, can be based on different corruption setups, from the weakest to the strongest:

- **Honest Key Model (HK).** The *Honest Key Model* assumes that all the keys within the rings are generated honestly by the challenger. They may later be corrupted by the adversary. Consequently, no security is provided against keys generated maliciously.
- **Adversarially-Chosen Keys Model (ACK).** The *Adversarially-Chosen Keys Model* allows the adversary to supply maliciously generated keys to the signing oracle and the challenge signature ring, hence dropping the assumption that all keys need to be generated honestly. This model solves the problem of the honest key model by assuming that keys could have been generated maliciously by the signers. However, it does not guarantee that the entities in the ring are unable to identify the signer if they all collude, including the signer, *i.e.,* if all secret keys are revealed to the adversary.
- **Full Key Exposure Model (FKE).** The *Full Key Exposure Model* was proposed for ring signatures, assuming full disclosure of all secret keys to the adversary. In the context of ring signatures this model ensured anonymity even in case of leakage of all the secret keys. However, this level of security cannot be achieved for linkable ring signature schemes: given knowledge of all the secret key, the adversary can generate signatures with every single keys and use the $\mathsf{Link}_{\mathsf{LRS}}$ algorithm to identify the signers.

These corruption models, originally proposed for ring signatures, also apply to linkable ring signatures, with the exception of the full key exposure model. We elucidate on this fact at the end of this section, after presenting the property of anonymity.

Like in all the previous models proposed by the papers listed in Table 1a, the security of LRS is introduced here in the *honest key model*, *i.e.,* all keys must have been generated honestly by the challenger and only some of them can be corrupted based on a corruption oracle provided to the adversary. The honest key model leads to a weak corruption model, contradicting the *ad hoc* purpose of ring signatures, as any signer may generate its own key without any checks by other parties. We first introduce the definition of the required oracles before presenting the four game-based security requirements for *Secure Linkable Ring Signatures.* We discuss the model provided by Backes *et al.* [3] in Sections 4 and A and also discuss the more apropriate adversarially-chosen keys model.

Oracles. The adversary has access to the following oracles when it attempts to break the security of a linkable ring signature scheme.

- **$\mathcal{JO}$.** The *Joining Oracle.* Given the security parameter λ, runs $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$ and outputs the public key pk.
- **$\mathcal{CO}$.** The *Corruption Oracle.* Given a public key pk which is the output of a previous query to $\mathcal{JO}$, $\mathcal{CO}$ returns its corresponding secret key sk.
- **$\mathcal{SO}$.** The *Signature Oracle.* Given a public key vector $\{\mathsf{pk}_i\}_{i\in\mathcal{R}}$ an insider public key pk_i, for $i \in \mathcal{R}$ previously generated by $\mathcal{JO}$, and a message m, $\mathcal{SO}$ returns the signature $\sigma \leftarrow \mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_i\}_{i\in\mathcal{R}})$ and keeps record of the signed messages m in the set $\mathcal{SO}$.

For notation purposes, in our security experiments, we use the above oracle to designate the set of public keys of the entity that have been either introduced into the oracle or generated by it for $\mathcal{JO}$. The set $\mathcal{SO}$ records multiple types of elements:

- **Messages:** $\mathcal{SO}$ records the set of messages input to the oracle, when we write $m \in \mathcal{SO}$ for m a message, or;
- **Messages and signatures:** $\mathcal{SO}$ records the set of message-signature pairs input to the oracle, when we write $(m, \sigma) \in \mathcal{SO}$ for m a message and σ the associated signature, or;
- **Public keys of signers:** $\mathcal{SO}$ records the set of public keys of the signers which produced the linkable ring signatures when the oracle is called, when we write $\mathsf{pk} \in \mathcal{SO}$ for the public key pk of a signer.

Security Model. We now describe the properties expected for linkable ring signatures, namely *unforgeability*, *one-time anonymity*, *linkability* and *non-slanderability*. We denote by $\mathsf{Adv}^{\mathsf{prop}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ the advantage of $\mathcal{A}$ against the property prop of a linkable ring signature LRS for a given security parameter λ. Experiences are provided in the honest key model.

Unforgeability ($\mathsf{unf\text{-}HK}$). Constructing a valid signature without using the secret key should be unfeasible. Formally, the probability $\mathsf{Adv}^{\mathsf{unf\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ of a PPT adversary $\mathcal{A}$ winning (*i.e.,* making the challenger return 1) against the experiment $\mathsf{Exp}^{\mathsf{unf\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ should be negligible in the security parameter λ. Note that we could instead require a stronger variant, where a new signature on a signed messages would be accepted as a forgery. For that, a record of the messages input to the signature oracle and the output signature is kept in the set $\mathcal{SO}$, and line 5 of $\mathsf{Exp}^{\mathsf{unf\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ checks if $(m^*, \sigma^*) \in \mathcal{SO}$ instead.

$\mathsf{Exp}^{\mathsf{unf\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ - (Unforgeability Experiment in the Honest Key Model)

```
1 : $\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$
2 : $(m^*, \sigma^*, (\mathsf{pk}_i)_{i \in \mathcal{R}}) \leftarrow \mathcal{A}^{\mathcal{JO},\mathcal{CO},\mathcal{SO}}(\mathsf{p})$
3 : if $\{\mathsf{pk}_i\}_{i \in \mathcal{R}} \not\subset \mathcal{JO}$ : return 0
    // All of the public keys in $\{\mathsf{pk}_i\}_{i \in \mathcal{R}}$ were output by $\mathcal{JO}$.
4 : if $\{\mathsf{pk}_i\}_{i \in \mathcal{R}} \cap \mathcal{CO} \neq \emptyset$ : return 0   // No public key in $(\mathsf{pk}_i)_{i \in \mathcal{R}}$ were queried to $\mathcal{CO}$.
5 : if $m^* \in \mathcal{SO}$ : return 0   // The message $m^*$ was not an input to $\mathcal{SO}$.
6 : return $\mathsf{Verif}_{\mathsf{LRS}}(m^*, \sigma^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}}) = 1$
```

One-time Anonymity ($\mathsf{1\text{-}ano\text{-}HK}$) *(previously named anonymity)***.** It must be difficult to guess the public key corresponding to the secret key used to produce a signer's first signature. Here we present the property generally provided in the literature and call it *One-time Anonymity* whereas the property was previously given as *Anonymity*. Formally, for any PPT adversary $\mathcal{A}$, the experiment $\mathsf{Exp}^{\mathsf{1\text{-}ano\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ should have a negligible probability to output 1:

$$\mathsf{Adv}^{\mathsf{1\text{-}ano\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda) = |\Pr[\mathsf{Exp}^{\mathsf{1\text{-}ano\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda) = 1] - 1/2| \leq \epsilon(1^\lambda).$$

$\mathsf{Exp}^{\mathsf{1\text{-}ano\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ - (One-time Anonymity Experiment in the Honest Key Model)

```
1 : $\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$
2 : $(m^*, (\mathsf{pk}_i)_{i \in \mathcal{R}^*}, i_0, i_1) \leftarrow \mathcal{A}^{\mathcal{JO},\mathcal{CO},\mathcal{SO}}(\mathsf{p})$
3 : $b \xleftarrow{\$} \{0, 1\}^*$
4 : $\sigma \leftarrow \mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_{i_b}, m^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}^*} \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$
5 : $b^* \leftarrow \mathcal{A}^{\mathcal{JO},\mathcal{CO},\mathcal{SO}}(\sigma)$
6 : if $\{\mathsf{pk}_i\}_{i \in \mathcal{R}^*} \not\subset \mathcal{JO}$ : return $b$   // All of the public keys in $(\mathsf{pk}_i)_{i \in \mathcal{R}^*}$ are outputs of $\mathcal{JO}$.
7 : if $\{\mathsf{pk}_i\}_{i \in \mathcal{R}^*} \cap \mathcal{CO} \neq \emptyset$ : return $b$   // No public key in $(\mathsf{pk}_i)_{i \in \mathcal{R}^*}$ was queried to $\mathcal{CO}$.
8 : if $\{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\} \cap \mathcal{SO} \neq \emptyset$ : return $b$   // The oracle $\mathcal{SO}$ did not allow the link.
9 : return $b = b^*$
```

This property only allows the adversary $\mathcal{A}$ to obtain a single signature σ produced by the signer associated with the key pk_{i_b} and no signature from the signer associated with the key $\mathsf{pk}_{i_{(1-b)}}$ (line 4 and 5 of $\mathsf{Exp}^{\mathsf{1\text{-}ano\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$). Consequently, the property offers no guarantees on the anonymity of the signer when several signatures are produced with the same keys. This formalism contradicts the intended use for LRS, which is designed for different use cases than one-time LRS. In particular, the anonymity of the signer is expected to persist throughout the lifespan of the keys.

Some models, such as in [26], are even weaker and assume that none of the members of the challenge ring (*i.e.,* all entities associated with keys in $\{\mathsf{pk}_i\}_{i \in \mathcal{R}^*}$) have ever produced a signature with their keys. These definitions do not reflect the actual use of linkable ring signatures, as this primitive was designed to allow multiple anonymous signatures for a single entity. In Section 5, we give further arguments and two counter-examples for obtaining the above property, but without what was informally described as *anonymity* (see Section 1). This shows the limits of the experiment proposed above as $\mathsf{Exp}^{\mathsf{1\text{-}ano\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$.

Linkability ($\mathsf{link\text{-}HK}$). It must be difficult to generate two unlinked valid signatures from the same signer. To obtain linkability, the probability $\mathsf{Adv}^{\mathsf{link\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ of winning the experiment $\mathsf{Exp}^{\mathsf{link\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ must be negligible.

$\mathsf{Exp}^{\mathsf{link\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ - (Linkability Experiment in the Honest Key Model)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$
$(m_0^*, \sigma_0^*, (\mathsf{pk}_i)_{i \in \mathcal{R}_0^*}), (m_1^*, \sigma_1^*, (\mathsf{pk}_i)_{i \in \mathcal{R}_1^*}) \leftarrow \mathcal{A}^{\mathcal{JO},\mathcal{CO},\mathcal{SO}}(\mathsf{p})$
**if** $\{\mathsf{pk}_i\}_{i \in \mathcal{R}_0^* \cup \mathcal{R}_1^*} \not\subset \mathcal{JO}$ : **return** $0$
    // Public keys in $(\mathsf{pk}_i)_{i \in \mathcal{R}_0^* \cup \mathcal{R}_1^*}$ are honestly generated.
**if** $\exists i, j \in \mathcal{R}_0^* \cup \mathcal{R}_1^*, i \neq j, \mathsf{pk}_i, \mathsf{pk}_j \in \mathcal{CO}$ : **return** $0$
    // Max. one corrupted key in the rings.
**if** $\{\mathsf{pk}_i\}_{\mathcal{R}_0^* \cup \mathcal{R}_1^*} \cap \mathcal{SO} \neq \emptyset$ : **return** $0$
    // The oracle $\mathcal{SO}$ did not return a linked signature.
**return** $\mathsf{Verif}_{\mathsf{LRS}}(m_0^*, \sigma_0^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}_0^*}) = \mathsf{Verif}_{\mathsf{LRS}}(m_1^*, \sigma_1^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}_1^*}) = 1$
    $\wedge\ \mathsf{Link}_{\mathsf{LRS}}(\sigma_0^*, \sigma_1^*) = 0$
```

Non-slanderability ($\mathsf{slan\text{-}HK}$). It should be unfeasible to link two valid signatures correctly generated by different signers. To obtain non-slanderability, the probability $\mathsf{Adv}^{\mathsf{slan\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ of winning the experiment $\mathsf{Exp}^{\mathsf{slan\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ must be negligible.

$\mathsf{Exp}^{\mathsf{slan\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ - (Non-slanderability Experiment in the Honest Key Model)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$
$(\mathsf{pk}^*, m_0^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}_0^*}) \leftarrow \mathcal{A}^{\mathcal{JO},\mathcal{CO},\mathcal{SO}}(\mathsf{p})$
**if** $\{\mathsf{pk}^*\} \cup \{\mathsf{pk}_i\}_{i \in \mathcal{R}_0^*} \not\subset \mathcal{JO}$ : **return** $0$
    // The key $\mathsf{pk}^*$ is honestly generated and the set $\mathcal{R}_0^*$ only contains honestly generated keys.
$\sigma \leftarrow \mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}, m_0^*, \{\mathsf{pk}^*\} \cup \{\mathsf{pk}_i\}_{i \in \mathcal{R}_0^*})$   // $\mathsf{sk}$ is the secret key associated to $\mathsf{pk}$.
$(m_1^*, \sigma^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}_1^*}) \leftarrow \mathcal{A}^{\mathcal{JO},\mathcal{CO},\mathcal{SO}}(\sigma)$
**if** $\{\mathsf{pk}_i\}_{i \in \mathcal{R}_1^*} \not\subset \mathcal{JO}$ : **return** $0$   // The set $\mathcal{R}_1^*$ only contains honestly generated keys.
**if** $\mathsf{pk}^* \in \mathcal{CO}$ : **return** $0$   // The public key $\mathsf{pk}^*$ has not been requested from $\mathcal{CO}$.
**if** $\mathsf{pk}^* \in \mathcal{SO}$ : **return** $0$   // The oracle $\mathcal{SO}$ did not produce the signature $\sigma^*$.
**return** $\mathsf{Verif}_{\mathsf{LRS}}(m_1^*, \sigma^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}_1^*}) = 1 \wedge \mathsf{Link}_{\mathsf{LRS}}(\sigma, \sigma^*) = 1$
```

Some definitions of non-slanderability, such as the one in [1] require $\mathcal{A}$ to use specific keys to generate a signature. We deviate slightly from that definition by prohibiting corruption of the entity targeted by the attack, but follows the main idea of that formalisation.

From here on we can note that the correctness of the linking algorithm $\mathsf{Link}_{\mathsf{LRS}}$ is guaranteed by the properties of *linkability* and *non-slanderability.*

Unconditional Variant. We say that a property prop is obtained unconditionally if, for any unbounded probabilistic adversary $\mathcal{A}$, its advantage $\mathsf{Adv}^{\mathsf{prop}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ is equal to 0. Amongst existing work (see Table 1), only a few schemes, such as [26,11,1,4], have achieved unconditional one-time anonymity $\mathsf{1\text{-}ano}$.

Adversarially-chosen Keys Model. As stated above, most existing work listed in Table 1a sets unusually low security requirements. All of the security experiments presented in this section and in all previous work refered to in Table 1a are modelled within the framework of the honest key model HK, hence, failing to take into consideration the possibility of potentially malicious *adversarially generated keys*, the ACK model. This is inconsistent with informal security expectations for LRS as already stated. We present the experiment for one-time anonymity in the $\mathsf{1\text{-}ano}$ in the ACK corruption model below.

$\mathsf{Exp}^{\text{1-ano-ACK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n)$ - (One-time Anonymity experiment w.r.t. adversarially-chosen keys)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i=1}^{n} \leftarrow \mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$   // Abusing notations, the algorithm is executed $n$ times.
$(m^*, (\mathsf{pk}_i)_{i\in\mathcal{R}^*}, i_0, i_1) \leftarrow \mathcal{A}^{\mathcal{SO}}(\mathsf{p}, \{\mathsf{pk}_i\}_{i=1}^{n})$
// The set $\mathcal{R}$ for which $\mathcal{SO}$ is queried can also contain public keys picked by the adversary.
$b \xleftarrow{\$} \{0,1\}$
$\sigma \leftarrow \mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_{i_b}, m^*, \{\mathsf{pk}_i\}_{i\in\mathcal{R}^*} \cup \{\mathsf{pk}_0, \mathsf{pk}_1\})$
$b^* \leftarrow \mathcal{A}^{\mathcal{SO}}(\sigma)$
if $\{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\} \cap \mathcal{SO} \neq \emptyset$ : return $b$   // The oracle $\mathcal{SO}$ did not allow any link.
return $b = b^*$
```

The introduction of the other properties, unf-ACK, link-ACK, slan-ACK is postponed to Figure 2 in Section 4 with the introduction of Backes *et al.* [3]'s property of anonymity ano.

The full key exposure corruption model, which is stronger than the adversarially-chosen keys corruption model, cannot be achieved for linkable ring signatures. This is because anonymity of LRS cannot be achieved in the full key exposure corruption model. Linkable ring signature are always claimable, *e.g.,* by performing a signature for any given message and using the link algorithm anyone can test if they were both produced by the same signer. Therefore, revealing the challenger's secret key always breaks anonymity.

3 Usage of the Honest-Key Model and Anonymity

The security properties of ring signatures were formalised in a work by Bender *et al.* [7]. In particular, unforgeability and anonymity of ring signatures were extensively studied. Their models encompass three levels of corruptions. The honest key model is the most considered one for linkable ring signature and always with the flawed one-time anonymity experiments. Only two works [3,8] stand out and consider linkable ring signatures in the adversarially-chosen keys model that we will introduce later in Section 4. Moreover, their definition of anonymity, that of the second [8] resulting from the first [3], is the only one in the literature to consider a natural and stronger formalisation of anonymity for linkable ring signatures. They take advantage of what is sometimes called a *Left-or-Right* ($\mathcal{L}\mathsf{o}\mathcal{R}$) oracle. It acts as a challenge oracle providing signatures to the adversary for consistent unknown *left* and *right* signers. The adversary must uncover how the identity of the two signers are distributed in between the two challenger signers. The $\mathcal{L}\mathsf{o}\mathcal{R}^{\mathsf{HK}}$ oracles is defined in a context in which two key pairs $(\mathsf{pk}_{i_0}, \mathsf{sk}_{i_0})$ and $(\mathsf{pk}_{i_1}, \mathsf{sk}_{i_1})$ are known by the challenger, which also holds a bit $b \in \{0,1\}$. The oracle is defined as follows:

$\mathcal{L}\mathsf{o}\mathcal{R}^{\mathsf{HK}}$. The *Left-or-Right* oracle $\mathcal{L}\mathsf{o}\mathcal{R}_b^{\mathsf{HK}}(\cdot,\cdot)$ is such that for a call $\mathcal{L}\mathsf{o}\mathcal{R}_b^{\mathsf{HK}}(m, \{\mathsf{pk}_i\}_{i\in\mathcal{R}})$, it checks that all the public keys $\{\mathsf{pk}_i\}_{i\in\mathcal{R}}$ were honestly generated, hence belongs to $\mathcal{JO}$, and if so, it returns a signature $\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_{i_b}, m, \{\mathsf{pk}_i\}_{i\in\mathcal{R}} \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$.

The $\mathcal{L}\mathsf{o}\mathcal{R}^{\mathsf{HK}}$ oracle can be queried for any arbitrary set of registered keys $\{pk_i\}_{i\in\mathcal{R}}$. This set is always supplemented by the key of the two challengers, pk_{i_0} and pk_{i_1}, in order to avoid trivial identification attacks based on the failure of the oracles.

We introduce the definition of anonymity for linkable ring signatures as per [3] in the *honest-key model.* For the anonymity under the honest key model to hold against a PPT adversary $\mathcal{A}$, it should be computationally difficult to guess the public key corresponding to the secret key used during the production of the signatures of a signer. Formally, the experiment $\mathsf{Exp}^{\mathsf{ano}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n)$ should have a negligible probability $\mathsf{Adv}^{\mathsf{ano}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n)$ given by:

$$\mathsf{Adv}^{\mathsf{ano}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n) = |\Pr[\mathsf{Exp}^{\text{ano-HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n) = 1] - 1/2| \leq \epsilon(1^\lambda).$$

This bound must hold for every $n \in \mathbb{N}$ and the following experiment.

$\mathsf{Exp}^{\mathsf{ano\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n)$ - (Anonymity in the honest keys model)

```
$\mathsf{p} \leftarrow \mathsf{Setup}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i=1}^n \leftarrow \mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$
$(m^*, i_0, i_1) \leftarrow \mathcal{A}^{\mathcal{SO}}(\mathsf{p}, \{\mathsf{pk}_i\}_{i=1}^n)$   // Requests $\mathcal{SO}$ must be made using the provided keys.
$b \xleftarrow{\$} \{0,1\}$
$b^* \leftarrow \mathcal{A}^{\mathcal{SO}, \mathcal{L}o\mathcal{R}_b^{\mathsf{HK}}}(1^\lambda)$
if $\{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\} \cap \mathcal{SO} \neq \emptyset$ : return $b$
// The $\mathcal{SO}$ oracle did not output a signature for the signer $\mathsf{pk}_{i_b}$.
if $\mathcal{SO}$ was queried for a ring $\mathcal{R}$ with a public key which is not in $\{\mathsf{pk}_i\}_{i=1}^n$ :
    return $b$
if $\mathcal{L}o\mathcal{R}^{\mathsf{HK}}$ was queried for a ring $\mathcal{R}$ with a public key which is not in $\{\mathsf{pk}_i\}_{i=1}^n$ :
    return $b$
return $b = b^*$
```

In this experiment, the challenge is not directly sent to the adversary, but is deported to the answers of the $\mathcal{L}o\mathcal{R}^{\mathsf{HK}}$ oracle which provides challenges as output when called by the adversary. Therefore, when proving the anonymity of LRS under this model, every execution of the oracle $\mathcal{L}o\mathcal{R}^{\mathsf{HK}}$ would have to be considered by the reduction instead of just the first signature, which could lead to less tight reductions when these reductions are not unconditional. However, it does more accurately formalise the anonymity of the linkable ring signature than has previously been achieved in the literature.

Definition 2 (Linkable Ring Signature in the Honest-key Model). *A* Linkable Ring Signature *scheme is defined with algorithms described in Definition 1 and achieves security in the* honest-key model *if it achieves the properties of* Unforgeability $\mathsf{unf\text{-}HK}$*,* Linkability $\mathsf{link\text{-}HK}$ *and* Non-slanderability $\mathsf{slan\text{-}HK}$ *as described in Section 2 and* Anonymity $\mathsf{ano\text{-}HK}$ *as described above in this Section.*

This model with anonymity formalised in the honest key model can only be used when key generation is fully trusted. The use cases are then either (1) when it is possible to prove the honesty of the key generations, or (2) when all the members of the ring are honest. While this assumption may be realistic for some threat models, ring signatures are, by their nature, intended for use in contexts where there is no central authority responsible for verifying the validity of public keys, otherwise linkable group signatures could be used [41]. As a result, this definition does not always reflect the actual security requirements for linkable ring signatures, especially when used in decentralised scenarios such as blockchains [1]. This model leaves open possible attack scenarios in which (1) an adversary arbitrarily generates public keys (which may possibly depend on the public keys of honest users), and then (2) a legitimate signer generates a signature for a ring containing some of these adversary-generated public keys. Definition 7 offers no protection in these scenarios. This motivates the use of a stronger definition in the adversary-selected key model.

4 Anonymity of Linkable Ring Signatures

Despite more than 20 years of research in this area, misconceptions have persisted about the one-time anonymity experiment for linkable ring signatures. At the time of writing, only two works [3,8] have considered realistic models: in the adversarially-chosen keys model ACK and with anonymity formalised based on a *Left-or-Right* ($\mathcal{L}o\mathcal{R}$) signer oracle as a challenge. This oracle allows to provide multiple signatures from the challenger to the adversary. This accurate model has largely been overlooked in subsequent work, despite seemingly being achieved by most linkable ring signatures. We restate their definition, demonstrating its precision and that the introduction of the $\mathcal{L}o\mathcal{R}$ oracle excludes the counter-examples later presented in Section 5 and demonstrated our claim of weakness of the definition of one-time anonymity $\mathsf{1\text{-}ano}$.

For the formalisation of the security properties of linkable ring signatures in the adversarially-chosen keys model ACK, we instantiate two oracles: the $\mathcal{SO}^{\mathsf{ACK}}$ and the $\mathcal{L}o\mathcal{R}^{\mathsf{ACK}}$ oracles. They are both defined below. The $\mathcal{L}o\mathcal{R}^{\mathsf{ACK}}$ oracles is defined in a context where two key pairs $(\mathsf{pk}_{i_0}, \mathsf{sk}_{i_0})$ and $(\mathsf{pk}_{i_1}, \mathsf{sk}_{i_1})$ are known by the challenger as well as a bit $b \in \{0,1\}$.

$\mathsf{Exp}^{\mathsf{ano\text{-}ACK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n)$ - (Anonymity Experiment in the Adversarially-chosen Keys Model)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i=1}^{n} \leftarrow \mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$
$(i_0, i_1) \leftarrow \mathcal{A}^{\mathcal{SO}^{\mathsf{ACK}}}(\mathsf{p}, \{\mathsf{pk}_i\}_{i=1}^{n})$
    // The set $\mathcal{R}$ for which $\mathcal{SO}^{\mathsf{ACK}}$ is queried can also contain public keys picked by the adversary.
$b \xleftarrow{\$} \{0, 1\}$
$b^* \leftarrow \mathcal{A}^{\mathcal{SO}^{\mathsf{ACK}}, \mathcal{L}o\mathcal{R}_b^{\mathsf{ACK}}}(1^\lambda)$
if $\{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\} \cap \mathcal{SO}^{\mathsf{ACK}} \neq \emptyset$ : return $b$    // The oracle $\mathcal{SO}^{\mathsf{ACK}}$ did not allow any link.
return $b = b^*$
```

$\mathsf{Exp}^{\mathsf{unf\text{-}ACK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)$ - (Unforgeability Experiment in the Adversarially-chosen Keys Model)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i=1}^{n} \leftarrow \mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$
$(m^*, \sigma^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}}) \leftarrow \mathcal{A}^{\mathcal{SO}^{\mathsf{ACK}}}(\mathsf{p}, (\mathsf{pk}_i)_{1 \leq i \leq n})$
if $\mathcal{R} \not\subset \{1, \ldots, n\}$ : return 0    // No corrupted public key in the ring.
if $m^* \in \mathcal{SO}^{\mathsf{ACK}}$ : return 0    // The message $m^*$ has not been an input of $\mathcal{SO}^{\mathsf{ACK}}$.
return $\mathsf{Verif}_{\mathsf{LRS}}(m^*, \sigma^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}}) = 1$
```

$\mathsf{Exp}^{\mathsf{link\text{-}ACK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n)$ - (Linkability Experiment in the Adversarially-chosen Keys Model)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i=1}^{n} \leftarrow \mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$
$(m_0^*, \sigma_0^*, \{\mathsf{pk}_i^*\}_{i \in \mathcal{R}_0^*}), (m_1^*, \sigma_1^*, \{\mathsf{pk}_i^*\}_{i \in \mathcal{R}_1^*}) \leftarrow \mathcal{A}^{\mathcal{SO}^{\mathsf{ACK}}}(\mathsf{p}, \{\mathsf{pk}_i\}_{1 \leq i \leq n})$
if $\exists i \in \mathcal{R}_0^*, \exists j \in \mathcal{R}_1^*, \mathsf{pk}_i \neq \mathsf{pk}_j^*, \mathsf{pk}_i^*, \mathsf{pk}_j^* \notin \{\mathsf{pk}_i\}_{1 \leq i \leq n}$ : return 0
    // Only one common corrupted key or many in the same ring.
if $(m_0, \sigma_0^*)$ or $(m_1, \sigma_1^*) \in \mathcal{SO}^{\mathsf{ACK}}$ : return 0
    // The oracle $\mathcal{SO}^{\mathsf{ACK}}$ did not produce the signatures.
return $\mathsf{Verif}_{\mathsf{LRS}}(m_0^*, \sigma_0^*, \{\mathsf{pk}_i^*\}_{i \in \mathcal{R}_0^*}) = 1 \wedge \mathsf{Verif}_{\mathsf{LRS}}(m_1^*, \sigma_1^*, \{\mathsf{pk}_i^*\}_{i \in \mathcal{R}_1^*}) = 1$
    $\wedge\ \mathsf{Link}_{\mathsf{LRS}}(\sigma_0^*, \sigma_1^*) = 0$
```

$\mathsf{Exp}^{\mathsf{slan\text{-}ACK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n)$ - (Non-slanderability Experiment in the Adversarially-chosen Keys Model)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i=1}^{n} \leftarrow \mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$
$i^*, m_0^*, \{\mathsf{pk}_i^*\}_{\mathcal{R}_0^*} \leftarrow \mathcal{A}^{\mathcal{SO}^{\mathsf{ACK}}}(\mathsf{p}, \{\mathsf{pk}_k\}_{1 \leq k \leq n})$
if $i^* \notin \{1, \ldots, n\}$ : return 0    // The designated signer has been produced by the challenger.
$\sigma \leftarrow \mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_{i^*}, m_0^*, \{\mathsf{pk}_i^*\}_{i \in \mathcal{R}_0^*})$
$m_1^*, \sigma^*, \mathcal{R}_1^* \leftarrow \mathcal{A}^{\mathcal{SO}^{\mathsf{ACK}}}(\sigma)$
if $\mathsf{pk}_{i^*} \in \mathcal{SO}^{\mathsf{ACK}}$ : return 0
    // The oracle $\mathcal{SO}^{\mathsf{ACK}}$ did not allowed to produce the signature $\sigma^*$ for the key $\mathsf{pk}_{i^*}$.
return $\mathsf{Verif}_{\mathsf{LRS}}(m_1^*, \sigma^*, \{\mathsf{pk}_i^*\}_{i \in \mathcal{R}_1^*}) = 1 \wedge \mathsf{Link}_{\mathsf{LRS}}(\sigma, \sigma^*) = 1$
```

Fig. 2: Experiments for Anonymity, Unforgeability, Linlability and Non-slanderability in the Adversarially-chosen Keys Model.
(Similar to the one given in [3].)

$\mathcal{SO}^{\mathsf{ACK}}$. The oracle $\mathcal{SO}^{\mathsf{ACK}}(\cdot,\cdot,\cdot)$ is such that for a call $\mathcal{SO}^{\mathsf{ACK}}(i, m, \mathcal{R})$, it returns $\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_i\}_{i\in\mathcal{R}})$, where sk_i must be known by the challenger and $i \in \mathcal{R}$.

$\mathcal{L}o\mathcal{R}^{\mathsf{ACK}}$. For two honestly generated key pairs $(\mathsf{pk}_{i_0}, \mathsf{sk}_{i_0})$ and $(\mathsf{pk}_{i_1}, \mathsf{sk}_{i_1})$. The *Left-or-Right* oracle $\mathcal{L}o\mathcal{R}_b^{\mathsf{ACK}}(\cdot,\cdot)$ is such that for a call $\mathcal{L}o\mathcal{R}_b^{\mathsf{ACK}}(m, \{\mathsf{pk}_i\}_{i\in\mathcal{R}})$, it returns a signature $\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_{i_b}, m, \{\mathsf{pk}_i\}_{i\in\mathcal{R}} \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$.

In these security experiments the registration and corruption oracles $\mathcal{JO}$ and $\mathcal{CO}$ are removed to better reflect the *ad hoc* ring construction. Instead, arbitrary key input to the $\mathcal{SO}^{\mathsf{ACK}}$ and $\mathcal{L}o\mathcal{R}^{\mathsf{ACK}}$ oracles is allowed and provide alternatives to the corruption oracle. The same modification can be made for the other properties in a similar manner. We depict the alternative experiments in Figure 2.

Definition 3 (Linkable Ring Signature in the Adversarially-chosen Key Model). *A* Linkable Ring Signature *scheme is defined with algorithms described in Definition 1 and achieves a security in the* adversarially-chosen key model *if it achieves the properties of* Unforgeability unf-ACK*,* Anonymity ano-ACK*,* Linkability link-ACK *and* Non-slanderability slan-ACK*, described in Section 2 but, this time, on the basis of the experiments provided in Figure 2.*

Most linkable ring signatures have been proposed without regard to this model (see the other works in Table 1), although we believe that most linkable ring signatures could achieve this stronger properties in the adversarially-chosen key model, as it is not much more demanding on the design than the honest key model. Only two schemes in [3] and [8] stand out from the rest of the literature and have been shown to be secure within the framework of this model. Further work is needed to re-examine the security of existing schemes in these models. Table 1, column named *Anonymity* and Section 7 provide a literature review of the anonymity of the existing linkable ring signatures. Their we try to provide arguments towards the potential achievement of anonmity ano by most of the schemes of the literature.

4.1 Cryptographic Background

This section introduce two cryptographic primitives used to demonstrate the weaknesses in the linkable ring signature model of Section 2. First, let us introduce a primitive, called *Secret Sharing scheme*, an example of which is the well-known Shamir secret sharing scheme [34].

Definition 4 (Secret Sharing). *A* secret sharing *scheme amongst n participants is given by:*

$\mathsf{Split}(m, n)$**:** *is a* PPT *algorithm that takes parameters n and a message m, it returns a vector of shares $(s_i)_{1\leq i\leq n}$.*

$\mathsf{Recover}((s_i)_{1\leq i\leq n})$**:** *is a deterministic polynomial-time algorithm that takes a vector of shares $(s_i)_{1\leq i\leq n}$, it returns a message m.*

It must verify the *correctness* described by the equality $\mathsf{Recover}(\mathsf{Split}(m, n)) = m$ and achieve *perfect secrecy.*

Perfect Secrecy [34]. Recovering a message m split for a threshold of k with less than k shares is unfeasible.
The experiment $\mathsf{Exp}^{\mathcal{PS}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)\lambda$ for an adversary $\mathcal{A}$ and for a secret sharing scheme is defined as:

$\mathsf{Exp}^{\mathcal{PS}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)\lambda$ - (Perfect Secrecy)

```
$m_0, m_1, n, k \leftarrow \mathcal{A}(\lambda)$   // The value $k$ must be contained in the set $\{1, \ldots, n\}$.
$b \xleftarrow{\$} \{0, 1\}$
$(s_i)_{1\leq i\leq n} \leftarrow \mathsf{Split}(m_b, n)$   // Split one of the messages based on a uniform distribution.
$b' \leftarrow \mathcal{A}((s_i)_{1\leq i\leq n, i\neq k})$   // Here $\mathcal{A}$ must operate Recover with one less share than necessary.
return $(b = b')$
```

and for any adversary it should lead to

$$\mathsf{Adv}^{\mathcal{PS}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)\lambda = \left|\Pr[\mathsf{Exp}^{\mathcal{PS}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda)\lambda = 1] - 1/2\right| = 0.$$

This scheme is used for our first counter-example introduced in Section 5. We also need to introduce *non-interactive zero-knowledge proofs* for further investigation of a counter-example based on previously published work.

Definition 5 (Non-Interactive Zero-Knowledge proof). *A* Non-Interactive Zero-Knowledge proof *(*NIZK*) for a relation* $\mathcal{R}$ *is a pair of* PPT *algorithms. We use the Camenisch and Stadler [14] notation to describe the algorithms and their associated arguments.*

$\mathsf{ZK}\{w : (w, \phi) \in \mathcal{R}\}$**:** *is a* PPT *algorithm that takes a witness* w*, a statement* ϕ*, it returns a proof* π*.*
$\mathsf{Verif}_{\mathsf{ZK}}(\phi, \pi)$**:** *is a deterministic polynomial-time algorithm that takes a statement* ϕ *and a proof* π*, it returns a bit* 0 *or* 1*.*

A NIZK *requires* Completeness, Soundness *and* Zero-Knowledge*. A definition of these properties can be found in [15].*

5 Insecurity of the One-time Anonymity

Here, we demonstrate the weaknesses of signer's one-time anonymity $\mathsf{1\text{-}ano}$ in Section 2. Despite this, it is the model used by almost all existing works. In this section, we present two counter-examples showing that this definition lacks anonymity. Our first counter-example is a dedicated scheme, while the second comes from an existing work [13] which has different purposes. Both show the need to adopt a stricter definition of anonymity, as after the second signature the identity of the signer is purposely revealed. Nevertheless, these constructions are secure linkable ring signatures in the model of Section 2. This model was used to demonstrate the security of 16 linkable ring signatures out of the 18 existing schemes.

5.1 Toy Counter-example Scheme.

We start our dedicated construction from a secure linkable ring signature LRS, such any of the ones exposed in Table 1. From this LRS we instantiate a new linkable ring signature scheme CeLRS for *Counter-example linkable ring signature*, by combining LRS with a secret sharing scheme $(\mathsf{Split}, \mathsf{Recover})$ (Definition 4).

$\mathsf{CeLRS.Setup}_{\mathsf{LRS}}(1^\lambda)$**:** corresponds to the execution of $\mathsf{LRS.Setup}_{\mathsf{LRS}}(1^\lambda)$.
$\mathsf{CeLRS.Gen}_{\mathsf{LRS}}(1^\lambda)$**:** executes $(\mathsf{sk}_{\mathsf{LRS}}, \mathsf{pk}_{\mathsf{LRS}}) \leftarrow \mathsf{LRS.Gen}_{\mathsf{LRS}}(1^\lambda)$ and $s_1, s_2 \leftarrow \mathsf{Split}(\mathsf{pk}_{\mathsf{LRS}}, 2)$. Sets and returns $\mathsf{sk} = (\mathsf{sk}_{\mathsf{LRS}}, s_1, s_2)$, $\mathsf{pk} = \mathsf{pk}_{\mathsf{LRS}}$.
$\mathsf{CeLRS.Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$**:** parses sk_i into $(\mathsf{sk}_{\mathsf{LRS}}, s_1, s_2)$, randomly samples $b \xleftarrow{\$} \{1, 2\}$ and returns $\sigma_{\mathsf{LRS}} \leftarrow \mathsf{LRS.Sign}_{\mathsf{LRS}}(\mathsf{sk}_{\mathsf{LRS}}, m \| s_b, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$ and s_b as σ.
$\mathsf{CeLRS.Verif}_{\mathsf{LRS}}(m, \sigma, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$**:** parses σ into σ_{LRS} and s and executes $\mathsf{LRS.Verif}_{\mathsf{LRS}}(m\|s, \sigma_{\mathsf{LRS}}, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$ and returns its result.
$\mathsf{CeLRS.Link}_{\mathsf{LRS}}(\sigma, \sigma')$**:** parses σ into σ_{LRS} and s, and σ' into σ'_{LRS} and s'. Executes and returns the result of $\mathsf{LRS.Link}_{\mathsf{LRS}}(\sigma_{\mathsf{LRS}}, \sigma'_{\mathsf{LRS}})$.

The secret sharing share included in a single signature does not reveal any information about the signer's public key, since the secret sharing scheme is perfectly secret. On the other hand, we have considered a LRS scheme with one-time anonymity, which therefore does not reveal the identity of the signer. Nevertheless, a signer has a probability of at least $1/2$ of revealing its identity when it sends its second signature. Since one-time anonymity is modelled by a single signature disclosed to the adversary (see Section 2), this construction is proved secure as per Property 1 below and its proof. Moreover, the disclosure of the identity of the signer when more signatures can be claimed does not affect the other properties. This highlights limitations of the one-time anonymity $\mathsf{1\text{-}ano}$ property in ensuring the hiding of the identity of the signer to its first signature for all linkable ring signatures of Table 1a.

Property 1. Consider a secure linkable ring signature LRS and a secret sharing scheme with perfect secrecy. Then, the above toy counter-example scheme CeLRS is a linkable ring signature with correctness, unforgeability unf, one-time anonymity $\mathsf{1\text{-}ano}$, linkability link and non-slanderability slan under the definitions introduced in Section 2 in any of the corruption models HK or ACK.

Proof. The correctness is straightforward. To give an intuition of the following argument, anonymity of the CeLRS construction follows from the anonymity of the LRS and the perfect secrecy of the secret sharing scheme. The other properties of the CeLRS construction uniquely follow based on the security of the LRS scheme which has already been proven.

Unforgeability (unf*).* First, it should be noted that the LRS scheme is assumed to satisfy the unforgeability unf prescribed in Section 2, and that the share s_b is signed with the message. An adversary modifying s_b in the signature would cause the verification to fail because the wrong message would be introduced into the verification algorithm. Hence, the property follows from a direct reduction to unf of the LRS signature. A forgery against the CeLRS scheme for a message m would correspond to a forgery for a message $m\|s$ for a random s amongst s_1 or s_2.

One-time Anonymity ($1\text{-}\mathsf{ano}$*) (unconditional if unconditional for the* LRS*).* This is a two step proof. As only one signature is provided to the adversary for the public identities pk_{i_0} and pk_{i_1}, the first step is to replace the element s embedded in the signature σ by a random element based on the perfect secrecy, this is possible as one of the shares is never disclosed during the experiment. From then on, the signature σ of the CeLRS construction is just a LRS signature with a random elements concatenated to the signed message. The one-time anonymity $1\text{-}\mathsf{ano}$ of the LRS scheme guarantees that no identity related information would leak from the signature σ_{LRS}, hence from the signature σ provided to the adversary.

Linkability (link*) and Non-slanderability (*slan*).* As the linking algorithm only take into account the sub-signatures $\sigma_{\mathsf{LRS}_0^*}$, $\sigma_{\mathsf{LRS}_1^*}$, these experiments give the same answers for the CeLRS construction and the LRS scheme used as its base. Hence, linkability link and non-slanderability slan are both ensured under the hypothesis that the LRS scheme is secure.

5.2 Model of k-Times Full Traceable Ring Signatures

This section recalls the model for *k-Times Full Traceable Ring Signature* originally introduced by Bultel and Lafourcade [13]. Their construction is a linkable ring signature that can be traced back to the signer when it produces more than k authorised signatures. We define it here as it is used in Section 5 to show that the 1-time full traceable ring signature presented in [13] can be demonstrated secure under the model of linkable ring signature with one-time anonymity $1\text{-}\mathsf{ano}$ ilustrated in Section 2 despite the fact that it explicitly discloses the identity of the signer on the second signature. We chose to present this construction, we could also have presented the same arguments for the traceable ring signature in [23].

Definition 6 (*k*-Times Full Traceable Ring Signature ($\mathsf{k\text{-}FTRS}$)). *A k-Times Full Traceable Ring Signature scheme is composed of five algorithms defined as follows:*

$\mathsf{Setup}_{\mathsf{k\text{-}FTRS}}(1^\lambda)$**:** *is a* PPT *algorithm takes a security parameter* λ *and produces the* public parameters p.

We assume these parameters p *as common input to all the following algorithms.*

$\mathsf{Gen}_{\mathsf{k\text{-}FTRS}}(1^\lambda, k)$**:** *is a* PPT *algorithm that takes the security parameter* λ *and a* threshold value k *denoting the maximum number of anonymous signatures authorised, it returns a pair of keys* $(\mathsf{pk}, \mathsf{sk})$.

$\mathsf{Sign}_{\mathsf{k\text{-}FTRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}}, l)$**:** *is a* PPT *algorithm that takes a* vector $\{\mathsf{pk}_i\}_{i\in\mathcal{R}}$ *of public keys for a ring* $\mathcal{R}$*, a signer secret key* sk_i*, a the witness* $l \in \{1, \ldots, k\}$ *and a message* m*. It outputs a ring signature* σ.

$\mathsf{Verif}_{\mathsf{k\text{-}FTRS}}(m, \sigma, \{\mathsf{pk}_i\}_{i\in\mathcal{R}})$**:** *is a deterministic polynomial-time algorithm that takes a public key vector* $\{\mathsf{pk}_i\}_{i\in\mathcal{R}}$*, a signature* σ*, and a message* m*, if the signature* σ *is valid, it returns 1, else it returns 0.*

$\mathsf{Link}_{\mathsf{k\text{-}FTRS}}(\sigma, \sigma')$**:** *is a deterministic polynomial-time algorithm that takes two signatures* σ *and* σ'*, it returns 1, if they are linked, otherwise, it returns 0. Before running this algorithm, signatures must be verified.*

$\mathsf{Match}_{\mathsf{k\text{-}FTRS}}(\sigma, \sigma')$**:** *is a deterministic polynomial-time algorithm that takes two signatures* σ *and* σ'*, if* $\mathsf{Link}_{\mathsf{k\text{-}FTRS}}(\sigma, \sigma') = 1$*, it returns a public key* pk *and a* tracing element ω*, else it returns* $\perp$.

$\mathsf{Trace}_{\mathsf{k\text{-}FTRS}}(\sigma, \omega)$**:** *is a deterministic polynomial-time algorithm that takes a signature* σ *and a* tracing element ω*, it returns 1 if the signature* σ *was produced by the signer associated to* ω*, else it returns 0.*

A k-times full traceable ring signature $\mathsf{k\text{-}FTRS}$ must satisfy the properties of *Correctness*, *k-Unforgeability*, *k-Anonymity* and *k-Traceability.*

k-Unforgeability: constructing a valid signature without using the secret key should be unfeasible. The probability $\mathsf{Adv}^{\mathsf{k\text{-}unf}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ of a PPT adversary $\mathcal{A}$ winning against the experiment $\mathsf{Exp}^{\mathsf{k\text{-}unf}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ should be negligible for any integer $n \in \mathbb{N}$, any $k \leq n$ and any security parameter λ.

$\mathsf{Exp}^{\mathsf{k\text{-}unf}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ - (Unforgeability experiment for k-FTRS)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{k\text{-}FTRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{1 \leq i \leq n} \leftarrow \mathsf{Gen}_{\mathsf{k\text{-}FTRS}}(1^\lambda, k)$
$(m^*, \sigma^*, (\mathsf{pk}_i)_{i \in \mathcal{R}^*}) \leftarrow \mathcal{A}^{\mathsf{k}\mathcal{SO}_1}(\mathsf{p}, (\mathsf{pk}_i)_{1 \leq i \leq n})$
**if** $\mathcal{R} \not\subset \{1, \ldots, n\}$ : **return** $0$   // No corrupted public keys in the ring.
**if** $\sigma^* \notin \mathsf{k}\mathcal{SO}_1$ : **return** $0$   // The signature $\sigma^*$was not output by $\mathsf{k}\mathcal{SO}_1$.
**return** $\mathsf{Verif}_{\mathsf{k\text{-}FTRS}}(m^*, \sigma^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}^*}) = 1$
```

In this experiment, $\mathsf{k}\mathcal{SO}_1$ is a signing oracle that takes $(\mathsf{pk}_i, \{\mathsf{pk}_j\}_{j \in \mathcal{R}^*}, m, l)$ as input to sign it, a message m. If $\mathsf{pk}_i \notin \{\mathsf{pk}_i, \mathsf{sk}_i\}_{1 \leq i \leq n}$, it returns $\perp$, else it computes $\sigma \leftarrow \mathsf{Sign}_{\mathsf{k\text{-}FTRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, l)$ and returns σ.

k-Anonymity: guessing the public key corresponding to the secret key used to produce less than $(k + 1)$ signatures should be hard. Any PPT adversary $\mathcal{A}$ should have a negligible advantage to win the the experiment $\mathsf{Exp}^{\mathsf{k\text{-}ano}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$:

$$\mathsf{Adv}^{\mathsf{k\text{-}ano}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n) = |\Pr[\mathsf{Exp}^{\mathsf{k\text{-}ano}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n) = 1] - 1/2| \leq \epsilon(1^\lambda),$$

for any integer $n \in \mathbb{N}$, any $k \leq n$ and any security parameter λ.

$\mathsf{Exp}^{\mathsf{k\text{-}ano}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ - (Anonymity experiment for k-FTRS)

```
$b \xleftarrow{\$} \{0, 1\}$
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{k\text{-}FTRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i=1}^n \leftarrow \mathsf{Gen}_{\mathsf{k\text{-}FTRS}}(1^\lambda, k)$
$(m^*, i_0, i_1) \leftarrow \mathcal{A}^{\mathsf{k}\mathcal{SO}_2}(\mathsf{p}, \{\mathsf{pk}_i\}_{i=1}^n)$
$\sigma_0 \leftarrow \mathsf{k}\mathcal{SO}_2(m, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, \mathsf{sk}_{i_0}, l)$
$\sigma_1 \leftarrow \mathsf{k}\mathcal{SO}_2(m, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, \mathsf{sk}_{i_1}, l)$
$b^* \leftarrow \mathcal{A}^{\mathsf{k}\mathcal{SO}_2}(\sigma_b)$
**return** $b = b^*$
```

In this experiment $\mathsf{k}\mathcal{SO}_2$ is a signing oracle that takes $(\mathsf{pk}_i, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, m, l)$ in input to sign the message m. If $l > k$ or $\mathsf{pk}_i \notin \{\mathsf{pk}_j, \mathsf{sk}_j\}_{j=1}^n$ then it returns $\perp$ and aborts. If $l \in \{1, \ldots, k\}$ was already queried for pk_i, it also returns $\perp$. Else, it computes $\sigma \leftarrow \mathsf{Sign}_{\mathsf{k\text{-}FTRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, l)$ and returns σ.

k-Traceability: more than k signatures from the same signer are always (linkable and then) traceable. The probability $\mathsf{Adv}^{\mathsf{k\text{-}trace}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ of a PPT adversary $\mathcal{A}$ winning against the experiment $\mathsf{Exp}^{\mathsf{k\text{-}trace}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ should be negligible for any integer $n \in \mathbb{N}$, any $k \leq n$ and any security parameter λ.

$\mathsf{Exp}^{\mathsf{k\text{-}trace}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ - (Traceability experiment for k-FTRS)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{k\text{-}FTRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{1 \leq i \leq n} \leftarrow \mathsf{Gen}_{\mathsf{k\text{-}FTRS}}(1^\lambda, k)$
$i^* \leftarrow \mathcal{A}^{\mathsf{k}\mathcal{SO}_1}(\mathsf{p}, \{\mathsf{pk}_i\}_{1 \leq i \leq n})$
$(\{\mathsf{pk}_j\}_{j \in \mathcal{R}_i^*}, m_i^*, \sigma_i^*)_{1 \leq i \leq l} \leftarrow \mathcal{A}^{\mathsf{k}\mathcal{SO}_1}(\mathsf{sk}_{i^*})$
**if** $l \geq k \wedge (\forall i \in \{1, \ldots, k\}, \mathsf{Verif}_{\mathsf{k\text{-}FTRS}}(m_i^*, \sigma_i^*, \{\mathsf{pk}_j\}_{j \in \mathcal{R}_i^*}) = 1$
    $\wedge (\{\mathsf{pk}_j\}_{j \in \mathcal{R}_i^*}, m_i^*, \sigma_i^*) \notin \mathsf{k}\mathcal{SO}_1) \wedge \big((\forall 1 \leq a < b \leq k, \mathsf{Link}_{\mathsf{k\text{-}FTRS}}(\sigma_a, \sigma_b) \neq 1)$
      $\vee (\exists a, b, i, \mathsf{Match}_{\mathsf{k\text{-}FTRS}}(\sigma_a, \sigma_b) = (\mathsf{pk}, \omega), \mathsf{pk} \neq \mathsf{pk}_{i^*} \vee \mathsf{Trace}_{\mathsf{k\text{-}FTRS}}(\sigma_i, \omega_i) \neq 1)\big)$
        **return** $1$
**return** $0$
```

5.3 Concrete Counter-example

We present a second counter-example based on a construction which has been designed for a different purpose: revealing the public identity of signers overpassing a limit of k signatures. Originally proposed in [13], this primitive is called *k-times full traceable ring signature*. It is a ring signature that becomes linkable when the signer exceeds its limit of k allowed signatures. Once this limit has been exceeded, any verifier is capable of tracing the identity of the signer using an algorithm $\mathsf{pk} \leftarrow \mathsf{Trace}(\sigma, \sigma')$.

Here, we only consider *1-time full traceable ring signatures*, which allow a signer to produce one ring signature before disclosing their public key. Under the definition currently in use, we claim that this type of signature is also a linkable ring signature, even though a linkable ring signature should not reveal the identity of the signer, even after an arbitrary number of issued signatures. We now examine the instance of the scheme from [13] with $k = 1$.

$\mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$: generates three groups $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_t$ of prime order p with a pairing mapping $e \colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_t$ (a computable non-degenerate bilinear map). Chooses six random generators $g_1, h_0, h_1, h_2, h_3 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$ and a hash function H mapping to $\mathbb{Z}_p^*$.

$\mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$: the keys come in two parts, two secret discrete logarithms x and y constitute the secret key sk and the two associated elements of $\mathbb{G}_1$, $\mathsf{pk}_1 = g_1^x$ and $\mathsf{pk}_2 = g_1^y$ constitute the public key pk.

$\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_i\}_{i\in\mathcal{R}})$: samples a random $r \overset{\$}{\leftarrow} \mathbb{Z}_p^*$, computes $u = H(m, 0, g_2^r)$, $v = H(m, 1, g_2^r)$, $T_1 = h_1^y$, $T_2 = h_2^y \cdot g_1^{u\cdot x}$, $T_3 = h_3^y \cdot h_4^{v\cdot x}$, $T_4 = g_2^r$, $T_5 = e(h_4, T_4)^x$ and then generates a zero-knowledge proof to wrap up all the elements:

$$\mathit{\Pi} \leftarrow \mathsf{ZK}\left\{ x, y, r \colon \begin{array}{l} \left(\bigvee_{(\mathsf{pk}_1, \mathsf{pk}_2) \in \{\mathsf{pk}_i\}_{i\in\mathcal{R}}} (\mathsf{pk}_1 = g_1^x \wedge \mathsf{pk}_2 = g_1^y)\right) \\ \wedge T_1 = h_1^y \wedge T_2 = h_2^y \cdot g_1^{u\cdot x} \wedge T_3 = h_3^y \cdot h_4^{v\cdot x} \\ \wedge T_4 = g_2^r \wedge T_5 = e(h_4, T_4)^x \end{array} \right\}.$$

Returns $\sigma = (T_1, T_2, T_3, T_4, T_5, \mathit{\Pi})$ as the signature of the message m.

$\mathsf{Verif}_{\mathsf{LRS}}(m, \sigma, \{\mathsf{pk}_i\}_{i\in\mathcal{R}})$: parses the signature, computes $u = H(m, 0, T_4)$, $v = H(m, 1, T_4)$ and verifies the zero-knowledge proof.

$\mathsf{Link}_{\mathsf{LRS}}(\sigma, \sigma')$: parses the signatures, checks if $T_1 = T_1'$ and returns 1 if so, otherwise returns 0. We assume that the signatures have been verified before.

For the sake of completeness and the rest of our argument, we also provide the tracing algorithm that identify signers who have produced more than one signature. It also encompass the matching algorihm Match directly inside the tracing algorithm Trace.

$\mathsf{Trace}(\sigma, \sigma')$: checks the link between the two signatures by executing $\mathsf{Link}_{\mathsf{LRS}}(\sigma, \sigma')$ and stop if it fails. On two signatures σ, σ' being linked, computes u, u' and $\mathsf{id} = (T_2/T_2')^{1/(u-u')}$. Returns the identity id. A second element $w = (T_3/T_3')^{1/(v-v')}$ is also recovered in the construction presented in [13], this element is not useful in the case $k = 1$.

Property 2. The 1-time full traceable ring signature from Bultel and Lafourcade introduced in [13] and depicted above is a linkable ring signature and achieves correctness, unforgeability unf, one-time anonymity $\mathsf{1\text{-}ano}$, linkability link and non-slanderability slan under the definitions introduced in Section 2 in any of the corruption models HK or ACK.

Proof. Correctness is straightforward. Security proofs for the scheme are given for the associated model in [13], we rely on them to construct ours. Indeed, their model is quite similar to the security model of linkable ring signatures.

Unforgeability. The experiment unf presented in Section 2 matches the $\mathsf{k\text{-}unf}$ experiment in [13] (recalled in Section B): their an adversary has to return a valid signature, *i.e.,* $\mathsf{Verif}_{\mathsf{LRS}}(m^*, \sigma^*, \{\mathsf{pk}_i\}_{i\in\mathcal{R}}) = 1$, for a set of uncorrupted users with honestly generated keys $\{\mathsf{pk}_i\}_{i\in\mathcal{R}}$. Furthermore, this signature should not have been output by a call to the signature oracle. Thus, unforgeability unf is obtained directly from the proof of unforgeability $\mathsf{k\text{-}unf}$ given in [13]. It relies mainly on the soundness of the zero-knowledge proof Π.

One-time Anonymity. The experiment $\mathsf{Exp}^{\mathsf{k\text{-}ano}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda)$ (recalled in Section B) is stronger than the one-time anonymity $\mathsf{1\text{-}ano}$ introduced for the LRS schemes and presented in Section 2. In their model, the authors of [13] made it possible for the adversary to obtain multiple signatures from the same designated signer, with a limit of k signatures per signer. Here we have set the limit $k = 1$ which directly provides $\mathsf{1\text{-}ano}$. The model from [13] works in a static framework: the number of public keys in the ring is fixed to an integer n. Reducing our case to the static environment implies the introduction of a polynomial factor in the reduction. Consequently, $\mathsf{k\text{-}ano}$ implies one-time anonymity $\mathsf{1\text{-}ano}$.

Linkability. We are looking at the construction proposed in [13] using the setup $k = 1$, where k denotes the number of signatures that can be produced without being traced (linkability of all the produced signatures and identification of authors of the signatures). As the adversary can infer the identity of signers through its calls to the signing oracles, the ability to trace does not reveal any information. Hence, this property falls under the *traceability* of the 1-time full traceable ring signature as only one signature is queried for the challenger signers. Moreover, the proof Π is sound under the hardness of the DL problem (see [13] for the security proof). Since the adversary is unable to forge a signature for an honest and uncorrupted user under the soudness of π, linkability is an implication of the correctness of the Link algorithms.

Non-slanderability. In this experiment the condition $\mathsf{Link}_{\mathsf{LRS}}(\sigma, \sigma^*) = 1$ enforces that $T_1 = h_1^y = h_1^{y^*} = T_1^*$, hence $y = y^*$, where y and y^* are such that for $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ and $\mathsf{pk}^* = (\mathsf{pk}_1^*, \mathsf{pk}_2^*)$, $\mathsf{pk}_2 = g_1^y$ and $\mathsf{pk}_2^* = g_1^{y^*}$. Under the soundness of the proof Π, the adversary must know y^* (thus y too). And under the zero-knowledge property of Π, the security of the against non-slanderability is reduced to the hardness of the DL problem.

Therefore, the 1-time full traceable ring signature of [13] can also be considered as a linkable ring signature secure under the $\mathsf{1\text{-}ano}$ -HK model presented in Section 2. From these counter-examples, we have demonstrated the existence of a gap between the definition of anonymity provided in most of the literature and the informal and expected purposes of this property. We now provide the formalism which has only been used by [3,8]. Later, in Section 6, we demonstrate that these definitions bridge the anonymity gap in the definition.

6 Review of our Counter-examples

In this section, we evaluate the anonymity of our counter-examples.

Since it is now possible to obtain multiple signatures of the challenger signer based on the $\mathcal{L}\mathsf{o}\mathcal{R}$ oracle, our two counter-examples have become insecure for the new definition of anonymity. This is because a PPT adversary can claim more than one signature for one of the challenger signers when interacting with the challenger in one of the two $\mathsf{Exp}^{\mathsf{ano}}_{\mathsf{LRS}}(1^\lambda)$ experiments. As shown in Section 5, both schemes have non-negligible probabilities of revealing the identity of their signer after the second signature. For our counter-example construction, the probability of obtaining both secret sharing shares after the second signature is $1/2$, which allows identity recovery with a probability significantly different from $1/2$ (random guessing) even if we had obtained unconditional one-time anonymity based on an unconditionally anonymous LRS and a perfectly secret secret sharing scheme. This shows that even some schemes with unconditional one-time anonymity $\mathsf{1\text{-}ano}$ may reveal the identity of a signer after its second signature.

Regarding Bultel and Lafourcade's 1-time full traceable ring signature [13], their primitive is specifically designed to reveal the identity of the signer after a given number of signatures. We have set this value to 2 in Section 5. Thus, given a polynomial number of queries to the signature oracle, an adversary can always query the oracles twice and break the game by revealing the identity of the signer based on the Trace algorithm. The arguments above show that our two counter-examples cannot achieve the definitions of anonymity of Section 4 and this holds even under the honest key model provided in Section A. The above arguments imply the following property.

Property 3. Our *counter-example* of Section 5.1 and the 1-time full traceable ring signature from [13] do not guarantee anonymity ano in the adversary-chosen keys model, nor in the honest keys model.

Reference	One-time Anonymity (1-ano)	Anonymity (ano)
Liu *et al.* [27]	Computational	✗ → ✓
Tsang *et al.* [36]	Computational	✗ → ✓
Liu and Wong [28]	Computational	✗ → ✓
Tsang and Wei [35]	Computational	✗ → ✓
Liu *et al.* [26]	Unconditional	✗ → ✓ (Unconditional)
Yuen *et al.* [40]	Computational	✗ → ✓
Boyen and Haines [11]	Unconditional	?[9]
Branco and Mateus [12]	Computational	?[5]
Baum *et al.* [5]	Computational	✗ → ✓
Lu *et al.* [30]	Computational	?[5]
Liu *et al.* [29]	Computational	No Proof Found
Zhang *et al.* [42]	Computational	✗ → ✓
Balla *et al.* [4]	Unconditional	✗ → ✓(Unconditional)
Bootle *et al.* [9]	Computational	✗ → ✓
Xiangyu *et al.* [25]	Computational	✗ → ✓
Xue *et al.* [39]	Computational	✗ → ✓

(a) Existing Linkable Ring Signatures. "✗ → ✓" means that it seems possible to extend the existing proof. N.A. for "Not Applicable".

Reference	One-time Anonymity (1-ano)	Anonymity (ano)
Alberto *et al.* [1]	Unconditional	✗[10]

(b) Existing One-time Linkable Ring Signatures.

Reference	One-time Anonymity (1-ano)	Anonymity (ano)
Backes *et al.* [3]	N.A.	✓ (already proven)
Beullens *et al.* [8]	N.A.	✓ (already proven)

(c) Existing Linkable Ring Signatures with Proven Anonymity. N.A. for "Not Applicable".

Table 2: Anonymity of Existing Linkable Ring Signatures.

7 Literature Review

The results of these investigations regarding expected security, obtained after a broad review of the literature, are summarized in Table 2. We are expecting that most schemes verify the stronger definitions of Section 4 as they were constructed with this idea in mind, while schemes in [3] and [8] have already been proven secure by their authors in the model of Section 4. Furthermore, most security reductions of existing schemes were provided based on arguments applied to one signature and decorrelating it from the keys of the signer. Their security proofs, for most of them, can be generalised when these arguments can be applied independently using hybrid arguments. This is unlike the reduction we provided for our counter-examples[8].

In this section, we provide a systematic review of all existing schemes in the literature in term of the experiment introduced in Section 4. Given the arguments of Section 5 and 6, it becomes apparent that the security of linkable ring signatures with one-time anonymity 1-ano should be re-evaluated, even when one-time anonymity holds unconditionally. We give an overview of how the stronger security requirement of anonymity applies to existing systems. Yet, we do not seek to prove the security of existing schemes.

[8] Our counter-examples where purposely lacking security when more signature needed to be produced, but their reduction involved arguments that were not limited to a single signature each time (*e.g.,* the perfect secrecy of the Sharmir secret sharing apply to $k-1$ shares but does not holds anymore when the k^{th} shared is revealed).

[9] There is no direct argument one way or the other, we are leaving this question open.

[10] This scheme is a one-time LRS, in their case, one-time anonymity is expected.

Given their design choices, it seems that the authors of the schemes in the literature aimed to offer the security described in the stronger model, when one-time anonymity was not considered to be a feature of the scheme. Indeed, this is reflected in the informal description of anonymity provided in previous works. We stress however that, even if the quoted schemes seem to have been designed to achieve our security, it would be necessary to re-analyse their security in the model of Section 4.

All linkable ring signatures include the ability to link signatures generated from the secret key sk. In general, these signatures can be divided into two parts: σ the "signature" itself and a *tag*. The purpose of the *tag* is to link valid signatures by their direct comparison while being bound to the "signature" part. The tags are usually in the form $tag = h^{\mathsf{sk}}$, for some fixed element h when relying on DL related hypothesis, or similarly when relying on other mathematical bases. The "signature" part wraps everything together to avoid modification of the tag, it can for example be an "OR" proof over the Schnorr NIZK proof [16,20] over all the public keys $\mathsf{pk} = g^{\mathsf{sk}}$. This construction was studied in [36] with a proof in the model of Section 2. As part of the security reduction of the anonymity, these tags are being stripped of the signer's identity by applying decisional hypothesis, *e.g.,* the DDH hypothesis for tags formed as above, then, providing a random value g^z instead of $h^{\mathsf{sk}} = g^{x \cdot \mathsf{sk}}$ for some unknown x. The reduction for other parts of the signature is more specific to the design. We detail below existing lines of work and their methods.

General Idea of our Analysis. When investigating the anonymity proofs of existing signature schemes, it was common to be able to divide the proof into three parts: (1) an initial sequence of game hops, *e.g.,* programming the ROM, (2) a sequence involving the modification of elements limited to the signature part σ of the challenge decorrelating all but the tag from the signer's secret key, *e.g.,* simulation of the NIZK proof wrapping up the signature, (3) a sequence of game hops making it possible to decorrelate the signature tag of the signature σ from the signer's keys for example the one based on the DDH and mentioned above. Now, given steps 2 (associated with the challenge signature) and 3 (associated with the label value), a hybrid argument seems to be possible most of the time to apply independently these parts of the proof to the multiple challenges generated by the $\mathcal{L}o\mathcal{R}$ oracle. In particular, the proof of [8], for which the scheme is secure in the strong model of Section 4, mainly follows these steps. We therefore investigated whether it is possible to obtain a hybrid argument based on the reductions provided to decorrelate the multiple challenges of the signer's identity and summarised our results in Table 2.

Zero-knowledge Based LRS *Schemes.* As a prominent basis for LRS, the constructions from [36,28,35,40,12,9,25,39] are based on zero-knowledge proofs, zero-knowledge arguments, or signature of knowledge. These schemes are used to wrap up ring signatures and link them with tags. The reductions provided by the authors of the existing schemes are mainly based on the zero-knowledge security of their NIZK proofs. This leads us to believe that the security of the previous schemes can be extended to anonymity ano in the adversarially-chosen keys model. This is because the proofs corresponding to the signature can be simulated independently and, by virtue of the existing proof for one-time anonymity, it must be possible to decorrelated the tag from the signer's keys. This last reduction for the tag most likely applies to several signatures at the same time.

Pedersen Commitment Based LRS *Schemes for Unconditional Anonymity.* The Pedersen commitment [32] where two secret values r and s are sampled and form a public commitment $c = g^r h^s$, for two generators g and h of a group, was used to obtain unconditional anonymity for LRS. LRS scheme based on this commitment scheme uses the elements r and s as the secret key and c the public key. As multiple pairs (r, s) leads to the same public key pk, an unbounded adversary is unable to recover the secret from the public key. The anonymity reductions provided by the authors of these schemes [26,11,4] are essentially the same. For any signature, there is always a secret key pair leading to any public key involved and from which the same signature could result. Put differently, whatever secret key is used, the statistical distribution of the signature remains unchanged. Given the independence of the signatures from the secret keys, we claim that the proof for all three schemes can be generalised to prove the stronger notion of anonymity ano, at least under the honest key model.

Remaining LRS *Schemes.* Among the existing schemes, some do not fall into the previous two categories and their anonymity relies solely on decisional hypotheses, such as the DDH problem for [27,42] or the *Decisional Module-LWE problem* [10] for [5] and [29]. Another scheme [30] is based on the chameleon hash function. For the first two schemes [27,42], each of the provided arguments only apply to a single element in the signatures and the associated reductions can be performed an arbitrary polynomial number of times. We therefore believe that a hybrid argument could be carried out based on part of the provided reduction and generalise the proof for any number of signatures produced by a single signer. That is why anonymity ano seems possible to guarantee. As for the scheme [29], we cannot verify how the reduction is performed for this scheme as we were unable to find an obvious reference to the full proofs.

The security of the remaining [1] scheme does not need to be addressed because its authors have proposed a singleone-time linkable ring signature: a LRS that is intended to be used to produce a single signature for each generated key pair. In particular, this scheme is unforgeable only if a single signature has been produced with a key pair. There is therefore no need to consider more than one signature for each key pair in the anonymity experiment.

8 Relationship Between the Properties

All the relationships between the four anonymity properties are shown in Figure 3. Some of them have not yet been demonstrated, and we discuss them below.

$$\begin{tikzcd}
\mathsf{1\text{-}ano\text{-}ACK} \arrow[r, shift left, "Sec.\ 5", "/" marking] \arrow[d, shift right, "Sec.\ 8"'] \arrow[dr, shift right, "|" marking] & \mathsf{ano\text{-}ACK} \arrow[l, shift left] \arrow[d, shift right] \\
\mathsf{1\text{-}ano\text{-}HK} \arrow[u, shift right, "/" marking] \arrow[r, shift left, "/" marking] & \mathsf{ano\text{-}HK} \arrow[l, shift left, "Sec.\ 5"] \arrow[u, shift right, "Sec.\ 8"', "/" marking] \arrow[ul, shift right, "|" marking]
\end{tikzcd}$$

Fig. 3: Comparison of the Anonymity Levels in the Various Corruption Models.

The anonymity ano presented in Section 4 (*resp.* in Section A) in the ACK corruption model (*resp.* the HK) is stronger than the anonymity 1-ano, as it allows access to several challenge signatures whereas only one is provided to the adversary in the 1-ano-ACK model (*resp.* 1-ano-HK). This has been demonstrated in Section 5.

Now, we examine the relationship between the HK corruption model and the ACK corruption model. Consider an adversary $\mathcal{A}$ winning, with non-negligible probability, against the experiment 1-ano or ano in the honest key model HK. According to the prescriptions of the honest key model, in the case of experiment 1-ano, $\mathcal{A}$ did not query oracle $\mathcal{SO}$ and did not issue a public key vector $(\mathsf{pk}_i)_{i\in\mathcal{R}^*}$ with an unregistered or corrupted public key. Similarly for the case of the ano experiment, $\mathcal{A}$ did not query oracle $\mathcal{SO}$ or oracle $\mathcal{L}o\mathcal{R}$ with unregistered or corrupted public keys. Hence, the same answer provided in the ACK model would also be accepted by the respective decisional problems in the ACK model. Therefore, 1-ano-HK is weaker than the 1-ano-ACK experiment and ano-HK is weaker than the ano-ACK experiment. Let us now show that there is a scheme that achieves security in the HK model but not the ACK model. To do this, we provide a second toy scheme showing that the inequalities between the corruption models are strict.

Second Toy Counter-example Scheme. Consider a secure signature LRS in any of the corruption models and a IND-CPA secure encryption scheme $\mathcal{E}$. The following counter-example encrypts the signer's identity under all the other public encryption keys of the ring members. This allows anyone with the secret key associated with one of the public keys of any of the ring members to recover the identity of the signer, but not anyone outside the ring. We formalise below the linkable ring signature scheme with such a property and show that it fulfils all the properties of LRS schemes in the HK corruption model but not in the ACK corruption model.

$\mathsf{Setup}_{\mathsf{LRS}}(1^\lambda)$**:** corresponds to the execution of $\mathsf{LRS.Setup}_{\mathsf{LRS}}(1^\lambda)$.

$\mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$**:** executes $(\mathsf{sk}_{\mathsf{LRS}}, \mathsf{pk}_{\mathsf{LRS}}) \leftarrow \mathsf{LRS.Gen}_{\mathsf{LRS}}(1^\lambda)$ and $(\mathsf{sk}_{\mathcal{E}}, \mathsf{pk}_{\mathcal{E}}) \leftarrow \mathsf{Gen}_{\mathsf{Enc}}(1^\lambda)$. Sets and returns $\mathsf{sk} = (\mathsf{sk}_{\mathsf{LRS}}, \mathsf{sk}_{\mathcal{E}})$, $\mathsf{pk} = (\mathsf{pk}_{\mathsf{LRS}}, \mathsf{pk}_{\mathcal{E}})$.

$\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$**:** parses sk_i into $(\mathsf{sk}_{\mathsf{LRS}}, \mathsf{sk}_{\mathcal{E}})$ and for all i in the ring $\mathcal{R}$ parses $\mathsf{pk}_j \xrightarrow{p} (\mathsf{pk}_{\mathsf{LRS},j}, \mathsf{pk}_{\mathcal{E},j})$. It computes $e_j \leftarrow \mathsf{Enc}(\mathsf{pk}_{\mathcal{E},j}, \mathsf{pk}_i)$ and $\sigma_{\mathsf{LRS}} \leftarrow \mathsf{LRS.Sign}_{\mathsf{LRS}}(\mathsf{sk}_i, m\|(e_j)_{j\in\mathcal{R}}, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$. Then returns $(\sigma_{\mathsf{LRS}}, (e_j)_{j\in\mathcal{R}})$ as σ.

$\mathsf{Verif}_{\mathsf{LRS}}(m, \sigma, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$**:** parses σ into σ_{LRS} and $(e_j)_{j\in\mathcal{R}}$ and verifies σ_{LRS} by executing the verification $\mathsf{LRS.Verif}_{\mathsf{LRS}}(m\|(e_j)_{j\in\mathcal{R}}, \sigma_{\mathsf{LRS}}, \{\mathsf{pk}_j\}_{j\in\mathcal{R}})$ and returns its result.

$\mathsf{Link}_{\mathsf{LRS}}(\sigma, \sigma')$**:** parses σ into σ_{LRS} and $(e_j)_{j\in\mathcal{R}}$, and σ' into σ'_{LRS} and $(e'_j)_{j\in\mathcal{R}'}$. Executes and returns the result of $\mathsf{LRS.Link}_{\mathsf{LRS}}(\sigma_{\mathsf{LRS}}, \sigma'_{\mathsf{LRS}})$.

Property 4. Consider a secure linkable ring signature LRS with one-time anonymity 1-ano (*resp.* anonymity ano) and a IND-CPA secure encryption scheme $\mathcal{E}$. Then, the second toy counter-example scheme is a linkable ring signature with correctness, unforgeability unf, one-time anonymity 1-ano (*resp.* anonymity ano), linkability link and non-slanderability slan under the honest key model HK.

Proof. This proof follows an analogous path to the proof of the first toy counter-example, the proof of Property 1 but relyies on the IND-CPA security of the encryption scheme for the $|\mathcal{R}|$ encrypted elements e_j for $j \in \mathcal{R}$ instead of the perfect secrecy of the secret sharing scheme (for the element s_1 or s_2 in the proof of the first toy counter-example). We now only elaborte for the proof of the property of anonymity 1-ano-HK or ano-HK.

First, for all challenge signatures with a ring $\mathcal{R}$, we reduce to the IND-CPA security of the encryption scheme for all the elements e_j, for all $j \in \mathcal{R}$. This is possible as in the honest key model, the secret key associated to the public key used by the challenger to encrypt the signers' identities remains unknown by the adversary. After this reduction, all elements e_j, for any $j \in \mathcal{R}$ and for all $\mathcal{R}$ supplied by the adversary, are uniformly random. Thus, in a similar way to the proof of Property 1, the 1-ano-HK property (*resp.* the ano-HK property) of the LRS leads to the proof of the 1-ano-HK property (*resp.* the ano-HK property) of our second toy example.

Our arguments are valid for both the 1-ano-HK or link-HK experiment depending on the anonymity of the LRS scheme. And yet, it is clear that the ACK corruption model allows neither. Therefore, we conclude that the HK model is strictly weaker than the ACK model as presented in Figure 3.

The combination of the two counter-examples introduced in this Section and in Section 5, directly implies that there is no hierarchy between the 1-ano-ACK experiment and the ano-HK model. If we take any 1-ano-ACK secure linkable ring signature scheme and introduce it into our first toy counter-example, we still get a 1-ano-ACK secure linkable ring signature scheme. However, this time we ensure that it does not achieve ano anonymity, and therefore does not reach ano-HK. Similarly, if we consider a ano-HK secure linkable ring signature scheme and introduce it into our second toy counter-example, we still obtain a ano-HK secure linkable ring signature scheme, but we ensure that it does not achieve any type of anonymity in the ACK model. With these last elements, we conclude the comparison introduced in Figure 3.

9 Conclusion and Further work

We have demonstrated that most security analysis for existing linkable ring signatures lacked of any guarantee of anonymity, even for the most recent ones. To support our claim, we provided two constructions that can be proven secure under the most commonly used security model, despite clearly breaking the informal anonymity expected from such schemes. Indeed, these counter-examples leaked the identity of the signer after only two signatures.

Based on this observation, we highlighted the model proposed by Backes *et al.* [3] and subsequently used by Beullens *et al.* [8] which has been left out of subsequent works. We believe that the model presented, in the adversarially-chosen keys model, better reflects the use cases of linkable ring signatures unlike the currently used one. In particular, they leave out the two counter-example constructions as we demonstrate.

Finally, we reviewed the literature providing arguments in favor of existing schemes realising the new properties. Thus, we rule out a global lack of anonymity for existing schemes.

References

1. Alberto Torres, W.A., Steinfeld, R., Sakzad, A., Liu, J.K., Kuchta, V., Bhattacharjee, N., Au, M.H., Cheng, J.: Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice ringct v1. 0). In: Information Security and Privacy: 23rd Australasian Conference, ACISP (2018)
2. Aranha, D.F., Hall-Andersen, M., Nitulescu, A., Pagnin, E., Yakoubov, S.: Count me in! extendability for threshold ring signatures. In: IACR International Conference on Public-Key Cryptography (2022)
3. Backes, M., Döttling, N., Hanzlik, L., Kluczniak, K., Schneider, J.: Ring signatures: logarithmic-size, no setup—from standard assumptions. In: Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part III 38. pp. 281–311. Springer (2019)
4. 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)
5. Baum, C., Lin, H., Oechsner, S.: Towards practical lattice-based one-time linkable ring signatures. In: International Conference on Information and Communications Security. pp. 303–322. Springer (2018)
6. Bellare, M., Micciancio, D., Warinschi, B.: Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In: Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques (2003)
7. Bender, A., Katz, J., Morselli, R.: Ring signatures: Stronger definitions, and constructions without random oracles. In: Theory of Cryptography Conference (2006)
8. Beullens, W., Katsumata, S., Pintore, F.: Calamari and falafl: logarithmic (linkable) ring signatures from isogenies and lattices. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 464–492. Springer (2020)
9. Bootle, J., Elkhiyaoui, K., Hesse, J., Manevich, Y.: Dualdory: Logarithmic-verifier linkable ring signatures through preprocessing. In: European Symposium on Research in Computer Security (2022)
10. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-kyber: a cca-secure module-lattice-based kem. In: 2018 IEEE European Symposium on Security and Privacy (2018)
11. Boyen, X., Haines, T.: Forward-secure linkable ring signatures. In: Information Security and Privacy: 23rd Australasian Conference, ACISP (2018)
12. Branco, P., Mateus, P.: A code-based linkable ring signature scheme. In: Provable Security: 12th International Conference, ProvSec 2018 (2018)
13. Bultel, X., Lafourcade, P.: k-times full traceable ring signature. In: 2016 11th International Conference on Availability, Reliability and Security (ARES) (2016)
14. Camenisch, J., Stadler, M.: Efficient group signature schemes for large groups. In: Annual international cryptology conference (1997)
15. Chase, M., Lysyanskaya, A.: On signatures of knowledge. In: Advances in Cryptology-CRYPTO: 26th Annual International Cryptology Conference (2006)
16. Cramer, R., Damgård, I., Schoenmakers, B.: Proofs of partial knowledge and simplified design of witness hiding protocols. In: CRYPTO '94 (1994)
17. Diaz, J., Lehmann, A.: Group signatures with user-controlled and sequential linkability. In: IACR International Conference on Public-Key Cryptography (2021)
18. El Kaafarani, A., Chen, L., Ghadafi, E., Davenport, J.: Attribute-based signatures with user-controlled linkability. In: Cryptology and Network Security: 13th International Conference, CANS 2014 (2014)
19. El Kaafarani, A., Ghadafi, E.: Attribute-based signatures with user-controlled linkability without random oracles. In: Cryptography and Coding: 16th IMA International Conference, IMACC 2017 (2017)
20. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: CRYPTO' 86 (1987)
21. Fiore, D., Garms, L., Kolonelos, D., Soriente, C., Tucker, I.: Ring signatures with user-controlled linkability. In: European Symposium on Research in Computer Security (2022)
22. Fraser, A., Garms, L., Lehmann, A.: Selectively linkable group signatures—stronger security and preserved verifiability. In: International Conference on Cryptology and Network Security (2021)

23. Fujisaki, E., Suzuki, K.: Traceable ring signature. In: International Workshop on Public Key Cryptography (2007)
24. Garms, L., Lehmann, A.: Group signatures with selective linkability. In: Public-Key Cryptography–PKC 2019: 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography (2019)
25. Hui, X., Chau, S.C.K.: Llring: Logarithmic linkable ring signatures with transparent setup. Cryptology ePrint Archive, Paper 2024/421 (2024)
26. Liu, J.K., Au, M.H., Susilo, W., Zhou, J.: Linkable ring signature with unconditional anonymity. IEEE Transactions on Knowledge and Data Engineering (2013)
27. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable spontaneous anonymous group signature for ad hoc groups. In: Information Security and Privacy: 9th Australasian Conference, ACISP (2004)
28. Liu, J.K., Wong, D.S.: Linkable ring signatures: Security models and new schemes. In: International Conference on Computational Science and Its Applications–ICCSA 2005 (2005)
29. Liu, Z., Nguyen, K., Yang, G., Wang, H., Wong, D.S.: A lattice-based linkable ring signature supporting stealth addresses. In: Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security (2019)
30. Lu, X., Au, M.H., Zhang, Z.: Raptor: a practical lattice-based (linkable) ring signature. In: Applied Cryptography and Network Security: 17th International Conference, ACNS 2019, Bogota, Colombia, 2019. pp. 110–130. Springer (2019)
31. Park, S., Sealfon, A.: It wasn't me! In: Annual International Cryptology Conference (2019)
32. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Annual international cryptology conference (1991)
33. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: International conference on the theory and application of cryptology and information security (2001)
34. Shamir, A.: How to share a secret. Communications of the ACM (1979)
35. Tsang, P.P., Wei, V.K.: Short linkable ring signatures for e-voting, e-cash and attestation. In: International Conference on Information Security Practice and Experience (2005)
36. Tsang, P.P., Wei, V.K., Chan, T.K., Au, M.H., Liu, J.K., Wong, D.S.: Separable linkable threshold ring signatures. In: Progress in Cryptology-INDOCRYPT 2004: 5th International Conference on Cryptology in India (2005)
37. Valimised: Internet voting in estonia (2024), `https://www.valimised.ee/en/internet-voting-estonia`, last access 06/19/2024
38. Van Saberhagen, N.: Cryptonote v 2.0 (2013)
39. Xue, Y., Lu, X., Au, M.H., Zhang, C.: Efficient linkable ring signatures: New framework and post-quantum instantiations. Cryptology ePrint Archive, Paper 2024/553 (2024)
40. Yuen, T.H., Liu, J.K., Au, M.H., Susilo, W., Zhou, J.: Efficient linkable and/or threshold ring signature without random oracles. The Computer Journal (2013)
41. Zhang, L., Li, H., Li, Y., Yu, Y., Au, M.H., Wang, B.: An efficient linkable group signature for payer tracing in anonymous cryptocurrencies. Future Generation Computer Systems (2019)
42. Zhang, X., Liu, J.K., Steinfeld, R., Kuchta, V., Yu, J.: Revocable and linkable ring signature. In: Information Security and Cryptology: 15th International Conference, Inscrypt 2019 (2020)

A Anonymity in the Honest-keys Model

The security properties of ring signatures were formalised in a work by Bender *et al.* [7]. In particular, unforgeability and anonymity of ring signatures were extensively studied. Their models encompass three levels of corruptions. The honest key model is the most considered one for linkable ring signature and always with the flawed one-time anonymity experiments. Only two works [3,8] stand out and consider linkable ring signatures in the adversarially-chosen keys model that we will introduce later in Section 4. Moreover, their definition of anonymity, that of the second [8] resulting from the first [3], is the only one in the literature to consider a natural and stronger formalisation of anonymity for linkable ring signatures. They take advantage of what is sometimes called a *Left-or-Right* ($\mathcal{L}\mathsf{o}\mathcal{R}$) oracle. It acts as a challenge oracle providing signatures to the adversary for consistent unknown *left* and *right* signers. The adversary must uncover how the identity of the two signers are distributed in between the two challenger signers. The $\mathcal{L}\mathsf{o}\mathcal{R}^{\mathsf{HK}}$ oracles is defined in a context in which two key pairs $(\mathsf{pk}_{i_0}, \mathsf{sk}_{i_0})$ and $(\mathsf{pk}_{i_1}, \mathsf{sk}_{i_1})$ are known by the challenger, which also holds a bit $b \in \{0, 1\}$. The oracle is defined as follows:

$\mathcal{L}\mathsf{o}\mathcal{R}^{\mathsf{HK}}$. The *Left-or-Right* oracle $\mathcal{L}\mathsf{o}\mathcal{R}_b^{\mathsf{HK}}(\cdot,\cdot)$ is such that for a call $\mathcal{L}\mathsf{o}\mathcal{R}_b^{\mathsf{HK}}(m, \{\mathsf{pk}_i\}_{i\in\mathcal{R}})$, it checks that all the public keys $\{\mathsf{pk}_i\}_{i\in\mathcal{R}}$ were honestly generated, hence belongs to $\mathcal{JO}$, and if so, it returns a signature $\mathsf{Sign}_{\mathsf{LRS}}(\mathsf{sk}_{i_b}, m, \{\mathsf{pk}_i\}_{i\in\mathcal{R}} \cup \{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\})$.

The $\mathcal{L}\mathsf{o}\mathcal{R}^{\mathsf{HK}}$ oracle can be queried for any arbitrary set of registered keys $\{pk_i\}_{i\in\mathcal{R}}$. This set is always supplemented by the key of the two challengers, pk_{i_0} and pk_{i_1}, in order to avoid trivial identification attacks based on the failure of the oracles.

We introduce the definition of anonymity for linkable ring signatures as per [3] in the *honest-key model.* For the anonymity under the honest key model to hold against a PPT adversary $\mathcal{A}$, it should be computationally difficult to guess the public key corresponding to the secret key used during the production of the signatures of a signer. Formally, the experiment $\mathsf{Exp}^{\mathsf{ano}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n)$ should have a negligible probability $\mathsf{Adv}^{\mathsf{ano}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n)$ given by:

$$\mathsf{Adv}^{\mathsf{ano}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n) = |\Pr[\mathsf{Exp}^{\mathsf{ano\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n) = 1] - 1/2| \le \epsilon(1^\lambda).$$

This bound must hold for every $n \in \mathbb{N}$ and the following experiment.
$\mathsf{Exp}^{\mathsf{ano\text{-}HK}}_{\mathcal{A},\mathsf{LRS}}(1^\lambda, n)$ - (Anonymity in the honest keys model)

```
$\mathsf{p} \leftarrow \mathsf{Setup}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i=1}^n \leftarrow \mathsf{Gen}_{\mathsf{LRS}}(1^\lambda)$
$(m^*, i_0, i_1) \leftarrow \mathcal{A}^{\mathcal{SO}}(\mathsf{p}, \{\mathsf{pk}_i\}_{i=1}^n)$   // Requests $\mathcal{SO}$ must be made using the provided keys.
$b \xleftarrow{\$} \{0, 1\}$
$b^* \leftarrow \mathcal{A}^{\mathcal{SO}, \mathcal{L}\mathsf{o}\mathcal{R}_b^{\mathsf{HK}}}(1^\lambda)$
if $\{\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}\} \cap \mathcal{SO} \neq \emptyset$ : return $b$
  // The $\mathcal{SO}$ oracle did not output a signature for the signer $\mathsf{pk}_{i_b}$.
if $\mathcal{SO}$ was queried for a ring $\mathcal{R}$ with a public key which is not in $\{\mathsf{pk}_i\}_{i=1}^n$ :
  return $b$
if $\mathcal{L}\mathsf{o}\mathcal{R}^{\mathsf{HK}}$ was queried for a ring $\mathcal{R}$ with a public key which is not in $\{\mathsf{pk}_i\}_{i=1}^n$ :
  return $b$
return $b = b^*$
```

In this experiment, the challenge is not directly sent to the adversary, but is deported to the answers of the $\mathcal{L}\mathsf{o}\mathcal{R}^{\mathsf{HK}}$ oracle which provides challenges as output when called by the adversary. Therefore, when proving the anonymity of LRS under this model, every execution of the oracle $\mathcal{L}\mathsf{o}\mathcal{R}^{\mathsf{HK}}$ would have to be considered by the reduction instead of just the first signature, which could lead to less tight reductions when these reductions are not unconditional. However, it does more accurately formalise the anonymity of the linkable ring signature than has previously been achieved in the literature.

Definition 7 (Linkable Ring Signature in the Honest-key Model). *A* Linkable Ring Signature *scheme is defined with algorithms described in Definition 1 and achieves security in the* honest-key model *if it achieves the properties of* Unforgeability $\mathsf{unf\text{-}HK}$*,* Linkability $\mathsf{link\text{-}HK}$ *and* Non-slanderability $\mathsf{slan\text{-}HK}$ *as described in Section 2 and* Anonymity $\mathsf{ano\text{-}HK}$ *as described above in this Section.*

This model with anonymity formalised in the honest key model can only be used when key generation is fully trusted. The use cases are then either (1) when it is possible to prove the honesty of the key generations, or (2) when all the members of the ring are honest. While this assumption may be realistic for some threat models, ring signatures are, by their nature, intended for use in contexts where there is no central authority responsible for verifying the validity of public keys, otherwise linkable group signatures could be used [41]. As a result, this definition does not always reflect the actual security requirements for linkable ring signatures, especially when used in decentralised scenarios such as blockchains [1]. This model leaves open possible attack scenarios in which (1) an adversary arbitrarily generates public keys (which may possibly depend on the public keys of honest users), and then (2) a legitimate signer generates a signature for a ring containing some of these adversary-generated public keys. Definition 7 offers no protection in these scenarios. This motivates the use of a stronger definition in the adversary-selected key model.

B k-Times Full Traceable Ring Signatures Model

This section recalls the model for *k-Times Full Traceable Ring Signature* originally introduced by Bultel and Lafourcade [13]. Their construction is a linkable ring signature that can be traced back to the signer when it produces more than k authorised signatures. We define it here as it is used in Section 5 to show that the 1-time full traceable ring signature presented in [13] can be demonstrated secure under the model of linkable ring signature with one-time anonymity $1\text{-}\mathsf{ano}$ ilustrated in Section 2 despite the fact that it explicitly discloses the identity of the signer on the second signature. We chose to present this construction, we could also have presented the same arguments for the traceable ring signature in [23].

Definition 8 (k-Times Full Traceable Ring Signature ($\mathsf{k\text{-}FTRS}$)). *A k-Times Full Traceable Ring Signature scheme is composed of five algorithms defined as follows:*

$\mathsf{Setup}_{\mathsf{k\text{-}FTRS}}(1^\lambda)$**:** *is a* PPT *algorithm takes a security parameter λ and produces the* public parameters p.

We assume these parameters p *as common input to all the following algorithms.*

$\mathsf{Gen}_{\mathsf{k\text{-}FTRS}}(1^\lambda, k)$**:** *is a* PPT *algorithm that takes the security parameter λ and a* threshold value k *denoting the maximum number of anonymous signatures authorised, it returns a pair of keys* $(\mathsf{pk}, \mathsf{sk})$*.*

$\mathsf{Sign}_{\mathsf{k\text{-}FTRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j\in\mathcal{R}}, l)$**:** *is a* PPT *algorithm that takes a* vector $\{\mathsf{pk}_i\}_{i\in\mathcal{R}}$ *of public keys for a ring $\mathcal{R}$, a signer secret key sk_i, a the witness $l \in \{1, \dots, k\}$ and a message m. It outputs a ring signature σ.*

$\mathsf{Verif}_{\mathsf{k\text{-}FTRS}}(m, \sigma, \{\mathsf{pk}_i\}_{i\in\mathcal{R}})$**:** *is a deterministic polynomial-time algorithm that takes a public key vector $\{\mathsf{pk}_i\}_{i\in\mathcal{R}}$, a signature σ, and a message m, if the signature σ is valid, it returns 1, else it returns 0.*

$\mathsf{Link}_{\mathsf{k\text{-}FTRS}}(\sigma, \sigma')$**:** *is a deterministic polynomial-time algorithm that takes two signatures σ and σ', it returns 1, if they are linked, otherwise, it returns 0. Before running this algorithm, signatures must be verified.*

$\mathsf{Match}_{\mathsf{k\text{-}FTRS}}(\sigma, \sigma')$**:** *is a deterministic polynomial-time algorithm that takes two signatures σ and σ', if* $\mathsf{Link}_{\mathsf{k\text{-}FTRS}}(\sigma, \sigma') = 1$*, it returns a public key* pk *and a* tracing element ω*, else it returns $\perp$.*

$\mathsf{Trace}_{\mathsf{k\text{-}FTRS}}(\sigma, \omega)$**:** *is a deterministic polynomial-time algorithm that takes a signature σ and a* tracing element ω*, it returns 1 if the signature σ was produced by the signer associated to ω, else it returns 0.*

A k-times full traceable ring signature $\mathsf{k\text{-}FTRS}$ must satisfy the properties of *Correctness*, *k-Unforgeability*, *k-Anonymity* and *k-Traceability.*

k-Unforgeability: constructing a valid signature without using the secret key should be unfeasible. The probability $\mathsf{Adv}^{\mathsf{k\text{-}unf}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ of a PPT adversary $\mathcal{A}$ winning against the experiment $\mathsf{Exp}^{\mathsf{k\text{-}unf}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ should be negligible for any integer $n \in \mathbb{N}$, any $k \leq n$ and any security parameter λ.

$\mathsf{Exp}^{\mathsf{k\text{-}unf}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ - (Unforgeability experiment for $\mathsf{k\text{-}FTRS}$)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{k\text{-}FTRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{1 \le i \le n} \leftarrow \mathsf{Gen}_{\mathsf{k\text{-}FTRS}}(1^\lambda, k)$
$(m^*, \sigma^*, (\mathsf{pk}_i)_{i \in \mathcal{R}^*}) \leftarrow \mathcal{A}^{\mathsf{k}\mathcal{SO}_1}(\mathsf{p}, (\mathsf{pk}_i)_{1 \le i \le n})$
$\textbf{if } \mathcal{R} \not\subset \{1, \ldots, n\} : \textbf{return } 0$   $/\!\!/$ No corrupted public keys in the ring.
$\textbf{if } \sigma^* \notin \mathsf{k}\mathcal{SO}_1 : \textbf{return } 0$   $/\!\!/$ The signature $\sigma^*$was not output by $\mathsf{k}\mathcal{SO}_1$.
$\textbf{return } \mathsf{Verif}_{\mathsf{k\text{-}FTRS}}(m^*, \sigma^*, \{\mathsf{pk}_i\}_{i \in \mathcal{R}^*}) = 1$
```

In this experiment, $\mathsf{k}\mathcal{SO}_1$ is a signing oracle that takes $(\mathsf{pk}_i, \{\mathsf{pk}_j\}_{j \in \mathcal{R}^*}, m, l)$ as input to sign it, a message m. If $\mathsf{pk}_i \notin \{\mathsf{pk}_i, \mathsf{sk}_i\}_{1 \le i \le n}$, it returns $\perp$, else it computes $\sigma \leftarrow \mathsf{Sign}_{\mathsf{k\text{-}FTRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, l)$ and returns σ.

k-Anonymity: guessing the public key corresponding to the secret key used to produce less than $(k+1)$ signatures should be hard. Any PPT adversary $\mathcal{A}$ should have a negligible advantage to win the the experiment $\mathsf{Exp}^{\mathsf{k\text{-}ano}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$:

$$\mathsf{Adv}^{\mathsf{k\text{-}ano}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n) = |\Pr[\mathsf{Exp}^{\mathsf{k\text{-}ano}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n) = 1] - 1/2| \le \epsilon(1^\lambda),$$

for any integer $n \in \mathbb{N}$, any $k \le n$ and any security parameter λ.

$\mathsf{Exp}^{\mathsf{k\text{-}ano}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ - (Anonymity experiment for $\mathsf{k\text{-}FTRS}$)

```
$b \xleftarrow{\$} \{0, 1\}$
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{k\text{-}FTRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{i=1}^n \leftarrow \mathsf{Gen}_{\mathsf{k\text{-}FTRS}}(1^\lambda, k)$
$(m^*, i_0, i_1) \leftarrow \mathcal{A}^{\mathsf{k}\mathcal{SO}_2}(\mathsf{p}, \{\mathsf{pk}_i\}_{i=1}^n)$
$\sigma_0 \leftarrow \mathsf{k}\mathcal{SO}_2(m, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, \mathsf{sk}_{i_0}, l)$
$\sigma_1 \leftarrow \mathsf{k}\mathcal{SO}_2(m, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, \mathsf{sk}_{i_1}, l)$
$b^* \leftarrow \mathcal{A}^{\mathsf{k}\mathcal{SO}_2}(\sigma_b)$
$\textbf{return } b = b^*$
```

In this experiment $\mathsf{k}\mathcal{SO}_2$ is a signing oracle that takes $(\mathsf{pk}_i, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, m, l)$ in input to sign the message m. If $l > k$ or $\mathsf{pk}_i \notin \{\mathsf{pk}_j, \mathsf{sk}_j\}_{j=1}^n$ then it returns $\perp$ and aborts. If $l \in \{1, \ldots, k\}$ was already queried for pk_i, it also returns $\perp$. Else, it computes $\sigma \leftarrow \mathsf{Sign}_{\mathsf{k\text{-}FTRS}}(\mathsf{sk}_i, m, \{\mathsf{pk}_j\}_{j \in \mathcal{R}}, l)$ and returns σ.

k-Traceability: more than k signatures from the same signer are always (linkable and then) traceable. The probability $\mathsf{Adv}^{\mathsf{k\text{-}trace}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ of a PPT adversary $\mathcal{A}$ winning against the experiment $\mathsf{Exp}^{\mathsf{k\text{-}trace}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ should be negligible for any integer $n \in \mathbb{N}$, any $k \le n$ and any security parameter λ.

$\mathsf{Exp}^{\mathsf{k\text{-}trace}}_{\mathcal{A},\mathsf{k\text{-}FTRS}}(1^\lambda, k, n)$ - (Traceability experiment for $\mathsf{k\text{-}FTRS}$)

```
$\mathsf{p} \leftarrow \mathsf{Setup}_{\mathsf{k\text{-}FTRS}}(1^\lambda)$
$\{\mathsf{pk}_i, \mathsf{sk}_i\}_{1 \le i \le n} \leftarrow \mathsf{Gen}_{\mathsf{k\text{-}FTRS}}(1^\lambda, k)$
$i^* \leftarrow \mathcal{A}^{\mathsf{k}\mathcal{SO}_1}(\mathsf{p}, \{\mathsf{pk}_i\}_{1 \le i \le n})$
$(\{\mathsf{pk}_j\}_{j \in \mathcal{R}_i^*}, m_i^*, \sigma_i^*)_{1 \le i \le l} \leftarrow \mathcal{A}^{\mathsf{k}\mathcal{SO}_1}(\mathsf{sk}_{i*})$
$\textbf{if } l \ge k \wedge (\forall i \in \{1, \ldots, k\}, \mathsf{Verif}_{\mathsf{k\text{-}FTRS}}(m_i^*, \sigma_i^*, \{\mathsf{pk}_j\}_{j \in \mathcal{R}_i^*}) = 1$
    $\wedge (\{\mathsf{pk}_j\}_{j \in \mathcal{R}_i^*}, m_i^*, \sigma_i^*) \notin \mathsf{k}\mathcal{SO}_1) \wedge \big((\forall 1 \le a < b \le k, \mathsf{Link}_{\mathsf{k\text{-}FTRS}}(\sigma_a, \sigma_b) \ne 1)$
      $\vee (\exists a, b, i, \mathsf{Match}_{\mathsf{k\text{-}FTRS}}(\sigma_a, \sigma_b) = (\mathsf{pk}, \omega), \mathsf{pk} \ne \mathsf{pk}_{i*} \vee \mathsf{Trace}_{\mathsf{k\text{-}FTRS}}(\sigma_i, \omega_i) \ne 1)\big)$
        $\textbf{return } 1$
$\textbf{return } 0$
```